Informatica Proactive Monitoring for PowerCenter Governance (Version 3.0)

Solutions Guide
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/cdlo1.0.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.

This Software is protected by U.S. Patent Numbers 5,794,246; 6,014,670; 6,016,501; 6,029,178; 6,032,158; 6,035,307; 6,044,374; 6,092,086; 6,208,990; 6,399,775; 6,400,226; 6,789,096; 6,823,373; 6,850,947; 6,895,471; 7,117,215; 7,162,643; 7,243,110; 7,254,590; 7,281,001; 7,421,458; 7,496,588; 7,523,121; 7,584,422; 7,676,516; 7,720,842; 7,721,270; 7,774,791; 8,065,266; 8,150,803; 8,166,048; 8,166,071; 8,200,622; 8,224,873; 8,271,477; 8,327,419; 8,386,435; 8,392,460; 8,453,159; 8,458,230; and RE44,478, International Patents and other Patents Pending.

DISCLAIMER: Informatica Corporation 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 Corporation 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 NONINFRINGEMENT.

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.

Part Number: PMPG-SLG-30000-0004
# Table of Contents

**Preface** .......................................................... 9
- Informatica Resources........................................ 9
  - Informatica My Support Portal............................ 9
  - Informatica Documentation................................ 9
  - Informatica Web Site........................................ 9
  - Informatica How-To Library............................... 10
  - Informatica Knowledge Base............................. 10
  - Informatica Support YouTube Channel.................. 10
  - Informatica Marketplace.................................. 10
  - Informatica Velocity....................................... 10
  - Informatica Global Customer Support................. 10

**Chapter 1: Proactive Monitoring for PowerCenter Governance Overview**........ 11
- Introduction.................................................. 11
- Solution Components........................................ 13
  - Informatica RulePoint..................................... 14
  - Informatica Real-Time Alert Manager................ 15
  - Proactive Monitoring Repository....................... 15
  - Proactive Monitoring for PowerCenter Management Console.......................... 16
- Solution Usage................................................ 16

**Chapter 2: Monitoring PowerCenter Governance**................................. 18
- Overview....................................................... 18
- Solution Objects.............................................. 18
  - Proactive Monitoring Objects........................... 18
  - Proactive Monitoring Rules.............................. 20

**Chapter 3: Introduction to Installation and Configuration**....................... 22
- Installation and Configuration Overview................ 22
- Installation Options......................................... 23

**Chapter 4: First Time Installation**............................................. 24
- First Time Installation Overview........................ 24
- Before You Install........................................... 24
  - Verify System Requirements............................ 25
  - Verify Permissions........................................ 26
  - Set Up the X Window Server............................ 26
- Configure Database Schemas................................ 26
  - Drop Database Schemas................................... 27
- Database Size Requirements.............................. 28
Chapter 5: Installing Governance on Proactive Monitoring for PowerCenter Operations

Installing Governance on Proactive Monitoring for PowerCenter Operations Overview

Before You Install

Installing in Graphical Mode

Installing in Console Mode

Chapter 6: After You Install

Post-Installation Tasks

Post-Installation Checklist

(Optional) Revoke User Permissions from Oracle and IBM DB2

Setting Up Proactive Monitoring for PowerCenter on AIX

Start and Stop the Proactive Monitoring for PowerCenter Instance

Import the Objects for Proactive Monitoring for PowerCenter

Configure Alerts

Configure LDAP for Proactive Monitoring for PowerCenter

Create PowerCenter Read-Only Users

Grant Permissions to PowerCenter Read-Only User

Configure the Proactive Monitoring Solution

Configure the RulePoint Components

Configure Email Connection

Schedule PowerCenter Workflow

Copy the ETL File

Create a Folder in the PowerCenter Repository

Create a Connection Object

Import the ETL File to PowerCenter Repository

Configure Scheduler for Workflow

Validate the Installation

Chapter 7: Upgrading Proactive Monitoring for PowerCenter Governance

Upgrading Proactive Monitoring for PowerCenter Governance Overview

Before You Upgrade

Planning Considerations for Migrating Objects from Version 2.6
Chapter 11: Proactive Monitoring Reports ........................................ 95
  Proactive Monitoring Reports Overview ........................................ 95
  Reports Tab - Filter and Display Options ...................................... 96
  Monitoring Application Services and Hosts in the Domain ................. 96
    Monitoring Alerts for Application Services and Host Statistics for the Current Day ....................... 97
    Monitoring the Alert History for Application Services and Hosts .............................................. 98
  Monitoring PowerCenter Operation Alerts .................................... 98
    Monitoring the PowerCenter Operation Alerts for the Current Day .......... 99
    Monitoring the Alert History for PowerCenter Operations ................ 99
    Export Alerts for PowerCenter Operations .................................. 99
  Monitoring PowerCenter Governance Alerts ................................ 100
    Monitoring the PowerCenter Governance Alerts for the Current Day .......... 100
    Monitoring the PowerCenter Governance Best Practice Violations ........ 101
    Export Alerts for PowerCenter Governance .................................. 101
    Monitoring the PowerCenter Governance Alerts Using On Demand Reports ........ 102

Chapter 12: Proactive Monitoring SNMP Alerts .................................. 105
  Proactive Monitoring SNMP Alerts ............................................. 105

Chapter 13: Proactive Monitoring Watchlists ................................... 107
  Proactive Monitoring Watchlists .............................................. 107

Chapter 14: Proactive Monitoring Topics ........................................ 109
  Proactive Monitoring Topics ..................................................... 109

Chapter 15: Proactive Monitoring Services ..................................... 111
  Sources ...................................................................................... 111
  Analytics .................................................................................... 113
  Responders ................................................................................ 115

Chapter 16: Proactive Monitoring Templates and Rules ....................... 117
  Proactive Monitoring Templates .................................................. 118
  Template Rules .......................................................................... 124
  Advanced Rules .......................................................................... 129

Chapter 17: Proactive Monitoring Responses ................................... 137
  Proactive Monitoring Responses .................................................. 137

Appendix A: Proactive Monitoring Lookup Table for Attribute Values .... 139

Appendix B: Topic Properties ......................................................... 143
| Appendix C: Windows Authentication Mode | 149 |
| Windows Authentication Mode Overview | 149 |
| Enable Windows Authentication Mode | 149 |
| Appendix D: Frequently Asked Questions | 151 |
| Appendix E: Glossary | 154 |
| Index | 157 |
Preface

The Proactive Monitoring for PowerCenter Governance Solutions Guide describes the solution provided for proactively monitoring the PowerCenter development environment. This guide also contains how to install and configure Proactive Monitoring for PowerCenter Governance.

The target audience of this guide is the Informatica domain administrator, who is responsible for installing Proactive Monitoring for PowerCenter Governance. This guide assumes that you have a working knowledge of Informatica PowerCenter, the application server, database server, and other system requirements to install and deploy Proactive Monitoring for PowerCenter Governance.

Informatica Resources

Informatica My Support Portal


The site contains product information, user group information, newsletters, access to the Informatica customer support case management system (ATLAS), the Informatica How-To Library, the Informatica Knowledge Base, Informatica Product Documentation, and access to the Informatica user community.

Informatica Documentation

The Informatica Documentation team takes every effort to create accurate, usable documentation. If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com. We will use your feedback to improve our documentation. Let us know if we can contact you regarding your comments.

The Documentation team updates documentation as needed. To get the latest documentation for your product, navigate to Product Documentation from http://mysupport.informatica.com.

Informatica Web Site

You can access the Informatica corporate web site at http://www.informatica.com. The site contains information about Informatica, its background, upcoming events, and sales offices. You will also find product and partner information. The services area of the site includes important information about technical support, training and education, and implementation services.
Informatica How-To Library

As an Informatica customer, you can access the Informatica How-To Library at http://mysupport.informatica.com. The How-To Library is a collection of resources to help you learn more about Informatica products and features. It includes articles and interactive demonstrations that provide solutions to common problems, compare features and behaviors, and guide you through performing specific real-world tasks.

Informatica Knowledge Base

As an Informatica customer, you can access the Informatica Knowledge Base at http://mysupport.informatica.com. Use the Knowledge Base to search for documented solutions to known technical issues about Informatica products. You can also find answers to frequently asked questions, technical white papers, and technical tips. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team through email at KB.Feedback@informatica.com.

Informatica Support YouTube Channel

You can access the Informatica Support YouTube channel at http://www.youtube.com/user/INFASupport. The Informatica Support YouTube channel includes videos about solutions that guide you through performing specific tasks. If you have questions, comments, or ideas about the Informatica Support YouTube channel, contact the Support YouTube team through email at supportvideos@informatica.com or send a tweet to @INFASupport.

Informatica Marketplace

The Informatica Marketplace is a forum where developers and partners can share solutions that augment, extend, or enhance data integration implementations. By leveraging any of the hundreds of solutions available on the Marketplace, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at http://www.informaticamarketplace.com.

Informatica Velocity

You can access Informatica Velocity at http://mysupport.informatica.com. 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 have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Global Customer Support

You can contact a Customer Support Center by telephone or through the Online Support.

Online Support requires a user name and password. You can request a user name and password at http://mysupport.informatica.com.

Proactive Monitoring for PowerCenter Governance
Overview

This chapter includes the following topics:

- **Introduction, 11**
- **Solution Components, 13**
- **Solution Usage, 16**

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.

The built-in rules are classified into the following categories:

**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.

In addition to the built-in rules that detect the mentioned deviations, the Proactive Monitoring solution allows you to 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 illustration gives an overview of the various components of the Proactive Monitoring solution and their purpose in the Proactive Monitoring solution context:
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.

RELATED TOPICS:
• “Proactive Monitoring Configuration” on page 75

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.
This chapter includes the following topics:

- **Overview, 18**
- **Solution Objects, 18**

### 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.

### Solution Objects

The Proactive Monitoring solution uses the RulePoint programming model and includes predefined proactive monitoring objects.

In addition, the solution also includes scripts to perform the following database operations:

- Create read-only permissions on tables and views to access data from the PowerCenter repository databases.
- Create the design, topology, RTAM, topology state, activity, and proactive monitoring schemas.

### 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.

**RELATED TOPICS:**

- "Proactive Monitoring Services" on page 111

Proactive Monitoring Rules

The Proactive Monitoring solution contains a large set of predefined rules that detect anomalies across PowerCenter repository.

The Proactive Monitoring solution provides the following categories of rules based on the types of checks:

- Best practice violations
- Duplicate objects
- Objects that are not valid
- Naming convention violations
- Disabled objects
- Hardcoded values in objects
- Illegal values in objects
- Frequent changes to objects
- Attribute checks for objects

The Proactive Monitoring solution includes the following types of predefined rules:

- Templates
- Advanced rules

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.

RELATED TOPICS:

- "Proactive Monitoring Templates and Rules" on page 117
CHAPTER 3

Introduction to Installation and Configuration

This chapter includes the following topics:

- Installation and Configuration Overview, 22
- Installation Options, 23

Installation and Configuration Overview

You can install the Proactive Monitoring for PowerCenter Governance in graphical or console mode on Windows, Linux, AIX, or Solaris.

Proactive Monitoring for PowerCenter Governance operates in a homogenous database environment for an instance of Proactive Monitoring for PowerCenter and PowerCenter. Therefore, use the same database type for both PowerCenter and Proactive Monitoring for PowerCenter instance. For example, if you create a PowerCenter repository on Oracle, you must create the Proactive Monitoring for PowerCenter repository on Oracle.

**Note:** Do not install Proactive Monitoring for PowerCenter on the same host system where you have installed PowerCenter.

Enhancements in 3.0 Installer

When you install 2.6 and earlier versions of Proactive Monitoring for PowerCenter, you had to install Java, Tomcat, RulePoint, RTAM, and Proactive Monitoring for PowerCenter Governance. You also had to specify the database information for installing RulePoint, RTAM, and Proactive Monitoring for PowerCenter.

The installation of Proactive Monitoring for PowerCenter from 2.6 to 3.0 has been simplified, and the installation effort has been considerably reduced because of the new packaging architecture. The 3.0 installer bundles all the components, and performs the tasks without the need for a user to perform each of the tasks separately. The 3.0 installer installs the files in a new directory and does not interfere with the files from the 2.6 installation. The installer starts the RulePoint and Proactive Monitoring for PowerCenter instances during installation. It also imports the predefined objects for monitoring PowerCenter based on the installer type, Governance or Operations.
Installation Options

When you run the Proactive Monitoring for PowerCenter Governance installer, the installer starts one of the following installation processes based on the options you choose:

- Install Proactive Monitoring for PowerCenter Governance 3.0.
- Install Proactive Monitoring for PowerCenter Governance 3.0 on Proactive Monitoring for PowerCenter Operations 3.0.
- Upgrade from Proactive Monitoring for PowerCenter Governance 2.6.

To upgrade Proactive Monitoring for PowerCenter from versions prior to 2.6, you must first upgrade to 2.6 and then use the 3.0 installer to upgrade to 3.0.

The Proactive Monitoring for PowerCenter 3.0 installer configures a single node configuration by default. The objects are deployed to the default services during the installation process. To create a multi-node setup or to configure high availability for the services, you need to plan accordingly. For more information about planning and instructions, see "Topology Management" in the RulePoint Administrator Guide. Also, for all advanced configurations, see the RulePoint Administrator Guide.
Chapter 4

First Time Installation

This chapter includes the following topics:

- First Time Installation Overview, 24
- Before You Install, 24
- Configure Database Schemas, 26
- Database Size Requirements, 28
- Database Parameter Requirements, 28
- Prerequisites for Typical Installation, 29
- Prerequisites for Custom Installation, 29
- Proactive Monitoring Database User, 32
- Installing in Graphical Mode, 32
- Installing in Console Mode, 36

First Time Installation Overview

You can install Proactive Monitoring for PowerCenter Governance in graphical or console mode on Windows, Linux, AIX, or Solaris. Complete the pre-installation tasks to prepare for the first time installation.

You can install Proactive Monitoring for PowerCenter Governance from a DVD or from the root of the directory where you download the installation files.

When you install, you can choose the typical or custom installation mode. In the typical installation mode, the Proactive Monitoring for PowerCenter installer creates the default schemas during the installation. In the custom installation mode, you configure custom schemas and specify the schema names during the installation.

Before You Install

Before you install Proactive Monitoring for PowerCenter Governance, set up the machine to meet the requirements to install and run the Proactive Monitoring solution.

Complete the following prerequisites before you install Proactive Monitoring for PowerCenter Governance:

- Verify the system requirements.
• Verify permissions.
• Ensure that you use the same database type for the Proactive Monitoring repository as used for PowerCenter.
• Get the name of the Informatica domain that you want to monitor. You can get the name of the Informatica domain name that you would want to monitor from the Administrator tool.
• Set up the X Window server.
• If you install Proactive Monitoring for PowerCenter on UNIX, and if you have both the 32-bit and 64-bit libstdc++ on your machine, make sure that you include libstdc++ 64-bit in the LD_LIBRARY_PATH.
• If you install Proactive Monitoring for PowerCenter on AIX, you must configure umestore and lbmrd on Linux.
• Ensure that the Linux box has 2.6.x kernel with glibc 2.5.x+
• If the schemas are created from a prior installation, you must drop the schemas and then continue with the installation.

Verify System Requirements

Before you install Proactive Monitoring for PowerCenter Governance, ensure to meet the minimum system requirements to install and run the Proactive Monitoring for PowerCenter Governance installer.

The following table lists the platforms supported by Proactive Monitoring for PowerCenter Governance:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Supported Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems</td>
<td>- Windows</td>
</tr>
<tr>
<td></td>
<td>- Linux</td>
</tr>
<tr>
<td></td>
<td>- AIX</td>
</tr>
<tr>
<td></td>
<td>- Solaris</td>
</tr>
<tr>
<td>Database Servers</td>
<td>- Oracle</td>
</tr>
<tr>
<td></td>
<td>- IBM DB2</td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server</td>
</tr>
<tr>
<td>Recommended Hardware Requirements</td>
<td>- 64-bit Intel or AMD-compatible, Xeon equivalent or better, 4 CPU @ 1.7 GHz</td>
</tr>
<tr>
<td></td>
<td>- 16 GB RAM</td>
</tr>
<tr>
<td></td>
<td>- 40 GB application disk space</td>
</tr>
<tr>
<td></td>
<td>- 1 Gbps Network Interface Card</td>
</tr>
<tr>
<td>Informatica PowerCenter</td>
<td>- Informatica PowerCenter 8.6.1</td>
</tr>
<tr>
<td></td>
<td>- Informatica PowerCenter 9.0.1</td>
</tr>
<tr>
<td></td>
<td>- Informatica PowerCenter 9.1.0</td>
</tr>
<tr>
<td></td>
<td>- Informatica PowerCenter 9.5.0</td>
</tr>
<tr>
<td></td>
<td>- Informatica PowerCenter 9.5.1</td>
</tr>
<tr>
<td></td>
<td>- Informatica PowerCenter 9.6.0</td>
</tr>
</tbody>
</table>

For more information about product requirements and supported platforms, see the Product Availability Matrix on the Informatica My Support Portal:

https://mysupport.informatica.com/community/my-support/product-availability-matrices
Verify Permissions

Verify that the user account you use to install Proactive Monitoring for PowerCenter has the following Permissions:

- Read, write, and execute permission on the installation directory.
- Write permissions on the /tmp directory.

On Linux, AIX, or Solaris, the user who runs the installer must have read, write, and execute permissions on the installer and its files directory, and write access to the /tmp directory. The /tmp directory must have a minimum of 200 MB for the installer to perform the install.

Set Up the X Window Server

When you run the installer in graphical mode, you must use a graphics display server. On UNIX, the graphics display server is typically an X Window server. If you do not have the X Window server installed on the machine where you want to install the product, you can run the installer by using an X Window server installed on another machine. Use the DISPLAY variable to redirect output of the X Window server to another UNIX machine.

The following table lists the commands to set the DISPLAY environment variable:

<table>
<thead>
<tr>
<th>Shell</th>
<th>Command</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>setenv DISPLAY &lt;TCP/IP node of XWindow server&gt;:0</td>
<td>setenv DISPLAY 10.1.50.23:0</td>
</tr>
<tr>
<td>Bash/Korn</td>
<td>export DISPLAY=&quot;&lt;TCP/IP node of XWindow server&gt;:0&quot;</td>
<td>export DISPLAY=&quot;10.1.50.23:0&quot;</td>
</tr>
<tr>
<td>Bourne</td>
<td>DISPLAY=&quot;&lt;TCP/IP node of XWindow server&gt;:0&quot;</td>
<td>DISPLAY=&quot;10.1.50.23:0&quot;</td>
</tr>
<tr>
<td></td>
<td>export display</td>
<td>export display</td>
</tr>
</tbody>
</table>

If you do not know the IP address of a UNIX machine where the X Window server is installed, ask your network administrator. For more information about redirecting the DISPLAY variable, see the documentation from the UNIX vendor.

If the X Window server does not support the font that the installer uses, the installer might display incorrect labels on the buttons.

Configure Database Schemas

By default, the Proactive Monitoring for PowerCenter installer creates the schemas during a typical installation. You can, however, configure custom schemas and specify the schema names if you choose the custom installation mode.

If you choose a typical installation, the Proactive Monitoring for PowerCenter installer creates the following schemas during installation:

- **Design schema**
  
  Stores details of design metadata of application projects, objects, and security configurations. The default schema name: RulePoint_Design.
**Topology schema**
Stores details of run-time topology such as host, nodes, run-time components, and run-time configurations. The default schema name is RulePoint_Topology.

**RTAM schema**
Stores responses for the RTAM tool. The default schema name is RulePoint_RTAM.

**Topology State schema**
Stores information about the run-time state of the topology. The default schema name is RulePoint_TopologyState.

**Activity schema**
Stores information about the run-time activity of application objects deployed on the run-time topology. The default schema name is RulePoint_Activity.

**Proactive Monitoring schema**
Stores metadata of the Informatica domain you want to monitor. The schema also stores host statistics and reporting data. The default schema name is Proactive_Monitoring.

---

**Drop Database Schemas**

If you are installing Proactive Monitoring for PowerCenter for the first time, you do not have to drop the schemas.

If schemas exist from a previous Proactive Monitoring for PowerCenter installation or if your installation fails, you need to drop the schemas before you install Proactive Monitoring for PowerCenter. If you install Proactive Monitoring for PowerCenter to upgrade the previous version of Proactive Monitoring for PowerCenter, you do not have to drop the schemas.

Drop the following default schemas or the schemas:

- RulePoint_Design
- RulePoint_RTAM
- RulePoint_Topology
- RulePoint_Activity
- RulePoint_TopologyState
- Proactive_Monitoring

**Dropping Tables from a Database**

To drop existing tables from a database, such as Oracle, perform the following steps:

1. Navigate to the following location:
   `<INSTALLER_HOME>\resources\db\<schema_name>\oracle`
2. Run the following script to drop the database tables:
   `drop_tables.sql`
3. Repeat the steps to drop tables for all schemas.

**Dropping Schemas from a Database**

1. Connect to the database as a database administrative user, and provide the password for the database administrative user.
2. To drop users from a database, for example, Oracle, run the following script:

```sql
drop user RulePoint_Design CASCADE;
drop user RulePoint_RTAM CASCADE;
drop user RulePoint_Technology CASCADE;
drop user RulePoint_Activity CASCADE;
drop user RulePoint_TechnologyState CASCADE;
drop user Proactive_Monitoring CASCADE;
commit;
```

## Database Size Requirements

Before you start the installation process, verify that the database has the required disk space based on your requirements.

The installer writes temporary files to the hard disk. Verify that you have enough available disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space. The installer requires 200 MB of temporary disk space.

The Proactive Monitoring for PowerCenter installation will require 1 GB free space. Other disk space requirements depend on the number of incoming events and generated responses. If the number of incoming events for a topic is high, you need to increase the disk space proportionally. By default, the maximum disk space requirement for each topic is 1 GB. For 40 topics, consider increasing the disk space to 50 GB.

The disk usage for the database schemas of Proactive Monitoring for PowerCenter differs based on the sample sizes.

The following table describes the disk space usage based on a sample sizing:

<table>
<thead>
<tr>
<th>Schema</th>
<th>Disk Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design time (RulePoint_Design)</td>
<td>225 MB for 315 objects.</td>
</tr>
<tr>
<td>Run time (RulePoint_TechnologyState,</td>
<td>351 MB for 315 objects.</td>
</tr>
<tr>
<td>RulePoint_Technology)</td>
<td></td>
</tr>
<tr>
<td>Activity Manager (RulePoint_Activity)</td>
<td>22 GB for 2 M events processed using 117 rules, and</td>
</tr>
<tr>
<td></td>
<td>with a Hit Ratio of 10%.</td>
</tr>
<tr>
<td>RTAM (RulePoint_RTAM)</td>
<td>15 GB for 300 K RTAM responses.</td>
</tr>
<tr>
<td>Proactive Monitoring (Proactive_Monitoring)</td>
<td>500 MB.</td>
</tr>
</tbody>
</table>

Contact Informatica Global Customer Support for specific database size requirements for your use case.

## Database Parameter Requirements

You must adequately tune the connections, memory, and database parameters to optimize Proactive Monitoring for PowerCenter. You need to increase the number of processes and sessions in the database.
For example, if you use the Oracle database, you must set the sessions, processes, and transactions to a minimum value as provided in the following table:

<table>
<thead>
<tr>
<th>Oracle Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions</td>
<td>800</td>
</tr>
<tr>
<td>Processes</td>
<td>500</td>
</tr>
<tr>
<td>Transactions</td>
<td>600</td>
</tr>
</tbody>
</table>

Microsoft SQL Server, by default, allows an unlimited number of concurrent connections. For IBM DB2, the Configuration Parameters Summary displays the connection information for the database. Contact the Database Administrator for any modifications on the default database parameters.

Prerequisites for Typical Installation

If you want the installer to create the default schemas at the time of installation, choose the typical installation mode. Configure the database user and provide the database administrator privileges to this user.

The default schema users are created with the same password as that of the database user used during installation. For example, if the database administrator user used during installation in Oracle is rulepoint and the password is rulepoint, the installer creates the six schemas with the same password, rulepoint. You can change the default password for the database user and the schemas, if required. For more information about changing the password, see the Informatica How-To Library article "Changing the Password of the Proactive Monitoring Database User".

Prerequisites for Custom Installation

If you do not want to use the default schema names or do not want to provide the database administrator privileges, you must choose the custom installation mode during installation.

Before you proceed with the custom installation, you must configure the database user, configure the schemas, and provide the required permissions.

Configure Schemas in Oracle

1. Launch SQL*Plus, log in as the database administrator user, and perform the rest of the tasks as an administrative user.

2. To create the Proactive Monitoring for PowerCenter database user and the required schemas, perform the following tasks:
   a. Navigate to the following directory:
      `<INSTALLER_HOME>\resources\db\schema_creation\oracle`
b. Edit the `create_users_ddl.sql` script. Provide the Proactive Monitoring for PowerCenter user name, password, and schema name in the script.

c. Run `create_users_ddl.sql`.

3. Perform the following tasks for each of the schemas:

   a. Navigate to the following directory:

      ```plaintext
      <INSTALLER_HOME>\resources\db\schema_configuration\<schema_name>\oracle
      ```

      where `schema_name` is the Design, Topology, RTAM, Topology State, Activity or Proactive Monitoring schema.

   b. Replace the schema names with the corresponding schema names that you created.

   c. Run the following script to populate the database tables for the Design, Topology, RTAM, Topology State, Activity schemas:

      ```sql
tables.sql
      ```

   d. Replace `<&DOMAIN_NAME>` with the Informatica domain name in the `pmpc_repository_ddl.sql` script and then run the following scripts to populate the database tables for the Proactive Monitoring schema:

      ```plaintext
      • pmpc_repository_ddl.sql
      • pmpc_aggregate_ddl.sql
      • pmpc_reporting_ddl.sql
      • pmpc_reporting_ddl_index.sql
      ```

4. To grant the required permissions to the Proactive Monitoring for PowerCenter database users, perform the following tasks:

   a. Navigate to the following directory:

      ```plaintext
      <INSTALLER_HOME>\Windows\resources\db\schema_permissions\oracle
      ```

   b. Replace the default schema names with the corresponding schema names that you created.

   c. Run the `grant_permissions_ddl.sql` script.

Configure Schemas in IBM DB2

1. Launch DB2 Command Line Processor, log in as the database administrator user, and perform the rest of the tasks as an administrative user.

2. To create the required schemas, perform the following tasks:

   a. Navigate to the following directory:

      ```plaintext
      <INSTALLER_HOME>\resources\db\schema_creation\db2
      ```

   b. Edit the `create_users_ddl.sql` script. Provide the Proactive Monitoring for PowerCenter user name and the schema names.

   c. Run `create_users_ddl.sql`.

3. Perform the following tasks for each schema:

   a. Navigate to the following location:

      ```plaintext
      <INSTALLER_HOME>\resources\db\schema_configuration\<schema_name>\db2
      ```

      where `schema_name` is the Design, Topology, RTAM, Topology State, Activity, or Proactive Monitoring schema.
b. Replace the schema names with the corresponding schema names that you created.
c. Run the following script to populate the database tables for the Design, Topology, RTAM, Topology State, Activity schemas:

```
tables.sql
```
d. Replace `<&DOMAIN_NAME>` with the Informatica domain name in the `pmc_repository_ddl.sql` script and then run the following scripts to populate the database tables for the Proactive Monitoring schema:

- `pmc_repository_ddl.sql`
- `pmc_aggregate_ddl.sql`
- `pmc_reporting_ddl.sql`
- `pmc_reporting_ddl_index.sql`

4. To grant the required permissions to the Proactive Monitoring for PowerCenter database users, perform the following tasks:
   a. Navigate to the following directory:
      `<INSTALLER_HOME>/resources/db/schema_permissions/db2`
   b. Replace the default schema names with the corresponding schema names that you created.
   c. Run `grant_permissions_ddl.sql`.

### Configure Schemas in Microsoft SQL

1. Launch Microsoft SQL Server Management Studio.
2. Create a database and provide a name for the database.
3. Change the default owner of the database to administrative user.
4. To create the database user, run the following command:

   ```sql
   CREATE LOGIN `<pm_user>` WITH PASSWORD='`<<password>>`',
   DEFAULT_DATABASE=`<<database_name>>`, CHECKExpiration=OFF, CHECK_POLICY=OFF
   USE `<<database_name>>`
   CREATE USER `<pm_user>` FOR LOGIN "`<<pm_user>>""
   GRANT CREATE SCHEMA, CREATE TABLE, CREATE FUNCTION, CREATE PROCEDURE, SELECT,
   INSERT, DELETE, UPDATE TO `<pm_user>`
   ```

   where:
   - `<pm_user>` is the name of the Proactive Monitoring database user.
   - `<password>` is the associated password for the user `<pm_user>`.
   - `<database_name>` is the name of the database that you create.

5. To create the design time, topology, RTAM, topology state, activity, and proactive monitoring schema, run the following command for each schema:

   ```sql
   CREATE SCHEMA `<<schema_name>>` AUTHORIZATION `<pm_user>`
   ```

   where:
   - `<pm_user>` is the name of the Proactive Monitoring for PowerCenter database user.
   - `<schema_name>` is the name of the schemas that you want to configure.
6. Perform the following tasks for each of the schemas:
   a. Click Open File, and navigate to the following location:
      
      ```
      <INSTALLER_HOME>\resources\db\schema_configuration\<schema>\sqlserver.
      ```
      
      where `schema` is the Design, Topology, RTAM, Topology State, Activity, or Proactive Monitoring schema.
   b. Edit the scripts for the Design, Topology, RTAM, Topology State, Activity schemas, or Proactive Monitoring schemas.
   c. Replace the default schema names with the corresponding schema names that you configured.
   d. Run the following script to populate the database tables for the Design, Topology, RTAM, Topology State, Activity schemas:
      
      ```
      tables.sql
      ```
   e. Replace `&&DOMAIN_NAME&&` with the Informatica domain name in the `pmc_repository_ddl.sql` script and then run the following scripts to populate the database tables for the Proactive Monitoring schema:
      
      ```
      pmc_repository_ddl.sql
      pmc_aggregate_ddl.sql
      pmc_reporting_ddl.sql
      pmc_reporting_ddl_index.sql
      ```

### Proactive Monitoring Database User

The Proactive Monitoring database user, pm_user, is used to access all the objects in the six configured schemas and perform all operations in Proactive Monitoring for PowerCenter. The grant scripts ensure that the pm_user has the required select, insert, update, and delete privileges for the objects that belong to the schemas.

Unlike IBM DB2 and Microsoft SQL Server, Oracle database automatically creates a schema when you create a user. So you need to create six different users for each of the schemas. However, the operational model of Proactive Monitoring for PowerCenter uses only the pm_user to access all the objects that are associated with the configured schemas. Hence, the user pm_user is the master user for Proactive Monitoring for PowerCenter and you require this user even after installation.

### Installing in Graphical Mode

You can install Proactive Monitoring for PowerCenter Governance in graphical mode on Windows, Linux, AIX, or Solaris.

1. Run the Proactive Monitoring for PowerCenter Governance installer based on the operating system.
   a. To install on Windows, run `Informatica_PMPC_Governance_3.0.exe` from the root directory.
   b. To install on Linux, AIX, or Solaris, use a shell command line to run `Informatica_PMPC_Governance_3.0.bin` from the root directory with `-gui` option for graphical mode installation. For example, enter `Informatica_PMPC_Governance_3.0.bin`.
2. In the Introduction page, choose the option Install Proactive Monitoring for PowerCenter Governance 3.0, and click Next. The Choose Installation Folder page appears.

3. Specify the location of the installation directory.

The following table shows the default location of the installation directory:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Proactive_Monitoring</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/Proactive_Monitoring</td>
</tr>
</tbody>
</table>

**Note**: Ensure that the directory path does not have spaces.

If the disk space available is not sufficient, a warning message appears. Ensure that you must have 40 GB disk space and then continue with the installation.

4. Click Next.

The License File page appears.

5. Provide the full path of the Proactive Monitoring for PowerCenter license file, and click Next.

The Database Configuration Mode page appears.

6. Specify the database configuration mode:
   - If you want to use the default database schemas that the installer creates, select Typical.
   - If you want to use the database schemas that you created, select Custom.

The Database Configuration page appears.

7. Select the database type from the displayed list:
   - Oracle
   - IBM-DB2
   - MS-SQL

8. Enter the database information where you want to configure Proactive Monitoring for PowerCenter.

You must have database administrator privileges on the database in which you want to configure Proactive Monitoring for PowerCenter.

The following table describes the database properties that you specify for Proactive Monitoring for PowerCenter:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database for Proactive Monitoring for PowerCenter.</td>
</tr>
<tr>
<td>Database User Name</td>
<td>User name for the database user account. The user must have the database administrator privileges on the database and at least 100 connection sessions to the database.</td>
</tr>
<tr>
<td>Database Password</td>
<td>Password for the database user account.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Hostname of the database.</td>
</tr>
</tbody>
</table>
9. Click **Test Connection** to verify that you can connect to the database.

The success message appears if the connection to the database is successful. If you had selected typical database configuration mode, the installer creates the following schemas for Proactive Monitoring for PowerCenter:

- RulePoint_Design
- RulePoint_RTAM
- RulePoint_Topology
- RulePoint_TopologyState
- RulePoint_Activity
- Proactive_Monitoring

If you had selected custom database configuration mode, you must provide the custom schema names that you have created.

**Important:** You must test the database connection parameters before you proceed.

10. Click **Next**.

The **Host and HTTP Configuration** dialog box appears.

11. Enter the Proactive Monitoring for PowerCenter host IP and port details.

The following table describes the Proactive Monitoring for PowerCenter host configuration details:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP</td>
<td>IP address of the host where you install Proactive Monitoring for PowerCenter.</td>
</tr>
<tr>
<td>Tomcat Port</td>
<td>HTTP port number of the Tomcat server. The default port is 8080.</td>
</tr>
</tbody>
</table>

12. If you want to enable a secure connection to access Proactive Monitoring for PowerCenter, perform the following steps, and then click **Next**:

   a. Select **Enable HTTPS for Proactive Monitoring for PowerCenter**.
   
   b. Enter the port number. By default, the port number is 8443.
   
   c. Select either a keystore generated by the installer, or use an existing keystore, and click **Next**.
   
   d. If you use an existing keystore, enter the keystore password and the name of the keystore file.

13. To configure email notifications to receive alerts for process failures in Proactive Monitoring for PowerCenter, click **Advanced Configurations**.
The Advanced Configurations dialog box appears.

- Select Enable Email Notification, configure the following email notification settings, and then click Save:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Host</td>
<td>The fully qualified domain name of the SMTP server that you use to send outbound email from RulePoint. For example, mail.mycompany.com</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the SMTP server.</td>
</tr>
<tr>
<td>From</td>
<td>Sender email address from which you send outbound emails.</td>
</tr>
<tr>
<td>To</td>
<td>Email recipient address to which you send notifications.</td>
</tr>
<tr>
<td>Priority</td>
<td>Email messages with the priority that you want to receive. Select from the following options: - Critical - High - Medium - Low For example, select Critical to receive email messages that have the priority as critical. When the default node fails, you receive an email alert of critical priority with the message that the default node has failed.</td>
</tr>
<tr>
<td>Verbosity</td>
<td>Verbosity of the email notification. Select from the following options: - More - Less For example, select Less to receive email messages with brief information of the alert.</td>
</tr>
<tr>
<td>User Name</td>
<td>Optional. The user account name of the SMTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Optional. The user account password of the SMTP server.</td>
</tr>
</tbody>
</table>

- If you do not want to configure email notifications during installation, click Cancel.

The PowerCenter Configuration page appears.

14. Enter the Informatica domain name.

The domain name is the name of the Informatica domain that you want to monitor. You can get the domain information from the Informatica domain administrator.

**Note:** The installer does not validate the domain name. Enter the correct name for the domain that you want to monitor.

15. To configure Proactive Monitoring reports, select Enable Reporting for Proactive Monitoring.

Proactive Monitoring for PowerCenter uses pre-defined PowerCenter workflows to transform alert data into the format required by Proactive Monitoring for PowerCenter reports. When you configure reports, the installer generates and configures an ETL file that contains the workflows to populate data in reports.
16. Configure the following report settings, and click **Next**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informatica Domain</td>
<td>Name of the Informatica domain in which you want to run the workflows to populate data in reports. <strong>Note:</strong> It is recommended that you do not use the same Informatica domain name that you provided for monitoring.</td>
</tr>
<tr>
<td>PowerCenter Integration Service</td>
<td>Name of the PowerCenter Integration Service to run the workflows.</td>
</tr>
<tr>
<td>Workflow Connection Name</td>
<td>Name of the relational connection used in the reporting workflow. This connection connects to the database where the proactive_monitoring schema is available.</td>
</tr>
</tbody>
</table>

The installer generates and configures the `ETL_ALL_PMPC_v30.xml` with the values you provide. After the installation, the `ETL_ALL_PMPC_v30.xml` file is available in the following location:

```<PMPC Installation folder>/Solutions/PMPC/reporting/et1/<database>```

You must import the `ETL_ALL_PMPC_v30.xml` file in to PowerCenter and run the workflows to transform the alert data.

The **Pre-installation Summary** page appears.

17. Review the pre-installation summary, and click **Install**.

18. Choose whether you want to register services for RulePoint components.
   - To create Windows services for the RulePoint components, click **Yes**. The RulePoint Design Time, RulePoint HostAgent, and RulePoint Topology services are created in the Windows services. You can use these services to start or stop the RulePoint instances after you complete the installation.
   - If you do not want to register Windows services for RulePoint components, click **No**.

After the installation is complete, the **Install Complete** page appears.

19. Review the post-installation tasks, and click **Done** to complete the installation procedure and exit the installer.

**RELATED TOPICS:**

- "Installing in Console Mode" on page 36
- "After You Install" on page 45

## Installing in Console Mode

You can install Proactive Monitoring for PowerCenter Governance in console mode on Windows, Linux, AIX, or Solaris.

**Note:** When you run the installer in console mode, the words Quit and Back are reserved words. You cannot use the reserved words as input text during installation.

1. At the command prompt for Windows or on a shell command line for Linux, AIX, and Solaris, run the Proactive Monitoring for PowerCenter Governance installer located in the root directory.
2. Enter the Proactive Monitoring for PowerCenter Governance executable name with the option -i console.
   - For Windows, enter `Informatica_PMPC_Governance_3.0.exe -i console`.
   - For Linux, AIX, or Solaris, enter `Informatica_PMPC_Governance_3.0.bin -i console`.

3. In the Introduction section, enter 1 to install Proactive Monitoring for PowerCenter Governance 3.0, and press Enter.
   The Choose Installation Folder section appears.

4. Specify the location of the installation folder, and press Enter.
   The following table shows the default location of the installation folder:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Proactive_Monitoring</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/Proactive_Monitoring</td>
</tr>
</tbody>
</table>

Note: Ensure that the directory path does not have spaces.

If the disk space available is not sufficient, a warning message appears. Ensure that you must have 40 GB disk space and then continue with the installation.

5. If you enter a different folder, enter Y to confirm the installation directory path.
   The License File section appears.

6. Enter the full path of the Proactive Monitoring for PowerCenter license file, and press Enter.
   The Database Configuration Mode section appears.

7. Specify the database configuration mode, and then press Enter.
   - To run the Typical mode and create the required database schemas with the default names, enter 1.
   - To run the Custom mode and use the database schemas that you created, enter 2.
   The Database Configuration section appears.

8. Select the database type where you want to configure Proactive Monitoring for PowerCenter, and then press Enter.
   - Enter 1 to select Oracle.
   - Enter 2 to select IBM DB2.
   - Enter 3 to select Microsoft SQL Server.

9. Enter the user name for the database user account, and then press Enter. The user must have the database administrator privileges on the database.

10. Enter the password for the database user account, and then press Enter.

11. Specify an option to use custom JDBC connection string, and then press Enter.
   - To use a custom JDBC connection string to enter the JDBC connection information, press Y.
     Enter the connection string and verify that the connection string contains all the connection parameters.
   - If you do not want to use the custom JDBC connection string to enter the JDBC connection information, press N, and then enter the database connection information.
The following table describes the connection properties that you specify for Proactive Monitoring for PowerCenter:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database for Proactive Monitoring for PowerCenter.</td>
</tr>
<tr>
<td>Database User Name</td>
<td>User name for the database user account. The user must have the database administrator privileges on the database and at least 100 connection sessions to the database.</td>
</tr>
<tr>
<td>Database Password</td>
<td>Password for the database user account.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Host name of the database.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Port number of the database.</td>
</tr>
<tr>
<td>Service Name/SID Name</td>
<td>Service name or SID name for Oracle, IBM DB2, or Microsoft SQL Server database.</td>
</tr>
<tr>
<td>JDBC Parameters</td>
<td>Optional. JDBC parameters to include in the JDBC URL. Optionally, you can specify additional JDBC parameters to include in the JDBC URL.</td>
</tr>
<tr>
<td>Custom Connection String for DataDirect driver</td>
<td>Optional. Connection string to connect to the database. To provide a customized connection string, select this option and enter the custom connection string.</td>
</tr>
</tbody>
</table>

If you had selected typical database configuration mode, the installer creates the following schemas for Proactive Monitoring for PowerCenter:

- RulePoint_Design
- RulePoint_RTAM
- RulePoint_Topology
- RulePoint_TopologyState
- RulePoint_Activity
- Proactive_Monitoring

If you had selected custom database configuration mode, you must provide the custom schema names that you have created.

The Host and HTTP Configuration section appears.

12. Enter the Proactive Monitoring for PowerCenter host IP and port details, and then press Enter.

The following table describes the Proactive Monitoring for PowerCenter host configuration details:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP</td>
<td>IP address of the server where you install Proactive Monitoring for PowerCenter.</td>
</tr>
<tr>
<td>Tomcat Port</td>
<td>HTTP port number of the Tomcat server. The default port number is 8080.</td>
</tr>
</tbody>
</table>

13. Select whether to set up a secure connection for Proactive Monitoring for PowerCenter:
The following table describes the options available to create or disable a secure connection:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y - Enable HTTPS for Proactive Monitoring for PowerCenter</td>
<td>Set up a secure connection for Proactive Monitoring for PowerCenter.</td>
</tr>
<tr>
<td>N - Disable HTTPS</td>
<td>Do not set up a secure connection for Proactive Monitoring for PowerCenter.</td>
</tr>
</tbody>
</table>

a. If you are enabling HTTPS, enter the configuration details, and then press Enter.

The following table describes the HTTPS connection information you must enter if you enable HTTPS:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number for the HTTPS connection.</td>
</tr>
<tr>
<td>Keystore file</td>
<td>Select the following option to use a keystore file generated by the installer or a keystore file you create:</td>
</tr>
<tr>
<td></td>
<td>1 - Use a keystore generated by the installer.</td>
</tr>
<tr>
<td></td>
<td>2 - Use an existing keystore</td>
</tr>
</tbody>
</table>

b. If you use an existing keystore, enter the password and location of the keystore file.

14. To configure email notifications to receive alerts for process failures in Proactive Monitoring for PowerCenter, enter Y to choose Advanced Configuration, and then press Enter.

- The following tables describes the email notification settings:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Host</td>
<td>The fully qualified domain name of the SMTP server that you use to send outbound email from RulePoint. For example: mail.mycompany.com</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the SMTP server.</td>
</tr>
<tr>
<td>From</td>
<td>Sender email address from which you send outbound emails.</td>
</tr>
<tr>
<td>To</td>
<td>Email recipient address to which you send notifications.</td>
</tr>
</tbody>
</table>
Property | Description
---|---
Priority | Email messages with the priority that you want to receive. Select from the following options:
1 - Critical
2 - High
3 - Medium
4 - Low
For example, enter 1 to receive email messages that have the priority as critical. When the default node fails, you receive an email alert of critical priority with the message that the default node has failed.

Verbosity | Verbosity of the email notification. Select from the following options:
1 - More
2 - Less
For example, enter 1 to receive email messages with detailed alert information.

User Name | Optional. The user account name of the SMTP server.
Password | Optional. The user account password of the SMTP server.

- If you do not want to configure email notifications during installation, enter No.

The **PowerCenter Configuration** section appears.

15. Enter the Informatica domain name.

The domain name is the name of the Informatica domain that you want to monitor. You can get the domain information from Informatica domain administrator.

**Note**: The installer does not validate the domain name. Enter the correct name for the domain that you want to monitor.

16. Select whether to configure Proactive Monitoring for PowerCenter reports.

The Proactive Monitoring for PowerCenter solution uses pre-defined PowerCenter workflows to transform alert data into the format required by PMPC reports. When you configure reports, the installer generates and configures an ETL file that contains the workflows to populate data in reports.

- To configure Proactive Monitoring for PowerCenter reports, enter Y and then configure the following report settings:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Informatica Domain | Name of the Informatica domain in which you want to run the workflows to populate data in reports.  
**Note**: It is recommended that you do not use the same Informatica domain name that you provided for monitoring. |
| PowerCenter Integration Service | Name of the PowerCenter Integration Service to run the workflows. |
| Workflow Connection Name | Name of the relational connection used in the reporting workflow. This connection connects to the database where the proactive_monitoring schema is available. |
The installer generates and configures the ETL_ALL_PMPC_v30.xml with the values you provide. After the installation, the ETL_ALL_PMPC_v30.xml file is available in the following location:

<PMPC Installation folder>/Solutions/PMPC/reporting/etl/<database>

You must import the ETL_ALL_PMPC_v30.xml file into PowerCenter and run the workflows to transform the alert data.

- If you do not want to configure Proactive Monitoring for PowerCenter reports, click N.

The Pre-installation Summary section appears.

17. Review the pre-installation summary, and then press Enter.

18. If you are using Windows, you can choose to register services for RulePoint components.
   - To register Windows services for the RulePoint components, enter 2.
     The RulePoint Design Time, RulePoint HostAgent, and RulePoint Topology services are created in the Windows services. You can use these services to start or stop the RulePoint instances after you complete the installation.
   - If you do not want to register Windows services for RulePoint components, enter 1.
     After the installation is complete, the Install Complete section appears.

19. Review the post-installation tasks, and press Enter to complete the installation and exit the installer.

Related Topics:

- "Installing in Graphical Mode" on page 32
- "After You Install" on page 45
CHAPTER 5

Installing Governance on Proactive Monitoring for PowerCenter Operations

This chapter includes the following topics:

- Installing Governance on Proactive Monitoring for PowerCenter Operations Overview, 42
- Before You Install, 42
- Installing in Graphical Mode, 43
- Installing in Console Mode, 44

Installing Governance on Proactive Monitoring for PowerCenter Operations Overview

You can install Proactive Monitoring for PowerCenter Governance 3.0 on Proactive Monitoring for PowerCenter Operations 3.0. You can run the installer in graphical or console mode on Windows, Linux, AIX, or Solaris. Complete the pre-installation tasks to prepare for the installation.

You can install Proactive Monitoring for PowerCenter Governance 3.0 from a DVD or from the root of the directory where you download the installation files.

Before You Install

Complete the following prerequisite before you install Proactive Monitoring for PowerCenter Governance 3.0 on an instance of Proactive Monitoring for PowerCenter Operations 3.0:

On Linux, the user who runs the installer must have read, write, and execute permissions on the installer and its files directory, and write access to the /tmp directory. The /tmp directory must have sufficient space, a minimum of 200 MB, for the installer to perform the installation.
Installing in Graphical Mode

You can install Proactive Monitoring for PowerCenter Governance 3.0 on an instance of Proactive Monitoring for PowerCenter Operations 3.0 in graphical mode on Windows, Linux, AIX, or Solaris.

1. Run the Proactive Monitoring for PowerCenter Governance installer based on the operating system.
   - To install on Windows, run Informatica_PMPC_Governance_3.0.exe from the root directory.
   - To install on Linux, AIX, or Solaris, use a shell command line to run Informatica_PMPC_Governance_3.0.bin from the root directory with -i gui option for graphical mode installation. For example, enter Informatica_PMPC_Governance_3.0.bin -i.

2. In the Introduction page, click Install Proactive Monitoring for PowerCenter Governance 3.0, and then click Next.
   The Choose Installation Folder page appears.

3. Specify the location where you installed the Proactive Monitoring for PowerCenter Operations solution.
   The following table shows the default location of the installation folder:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Proactive_Monitoring</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/Proactive_Monitoring</td>
</tr>
</tbody>
</table>

4. Click Next.
   The Installation Type page appears, indicating that Proactive Monitoring for PowerCenter Operations 3.0 is installed on RulePoint, for example at, C:\Proactive_Monitoring. Proactive Monitoring for PowerCenter Governance 3.0 will be configured on the existing installation.

5. Click Next.
   The Pre_Installation Summary dialog box appears.

6. Review the pre-installation summary, and click Install.

7. Select whether to start RulePoint and import Governance_3.0 solution.
   - To start RulePoint and import the Governance_3.0 solution, click Yes.
   - If you do not want to start RulePoint and import the Governance_3.0 solution, click No.
   After the installation is complete, the Install Complete page appears.

8. Review the post-installation tasks, and click Done to complete the installation procedure and exit the installer.
Installing in Console Mode

You can install Proactive Monitoring for PowerCenter Governance 3.0 on an instance of Proactive Monitoring for PowerCenter Operations 3.0 in console mode on Windows, Linux, AIX, or Solaris.

**Note:** When you run the installer in console mode, the words Quit and Back are reserved words. You cannot use the reserved words as input text during installation.

1. At the command prompt for Windows or on a shell command line for Linux, AIX, and Solaris, run the Proactive Monitoring for PowerCenter Governance installer located in the root directory.
2. Enter the Proactive Monitoring for PowerCenter Governance executable name with the option `-i console`.
   - For Windows, enter `Informatica_PMPC_Operations_3.0.exe -i console`.
   - For Linux, AIX, or Solaris, enter `Informatica_PMPC_Operations_3.0.exe -i console`.
3. In the **Introduction** section, enter **1** to install **Proactive Monitoring for PowerCenter Governance 3.0**, and then press **Enter**.
   The **Choose Installation Folder** section appears.
4. Specify the location where you installed the Proactive Monitoring for PowerCenter Operations solution. The following table shows the default location of the installation folder:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Proactive_Monitoring</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/Proactive_Monitoring</td>
</tr>
</tbody>
</table>

5. Press **Enter**.
   The **Installation Type** page appears, indicating that Proactive Monitoring for PowerCenter Operations 3.0 is installed on RulePoint, for example at, `C:\Proactive_Monitoring`. Proactive Monitoring for PowerCenter Governance 3.0 will be configured on the existing installation.
6. Press **Enter**.
   The **Pre_Installation Summary** section appears.
7. Review the pre-installation summary, and then press **Enter**.
8. Select whether to start RulePoint and import **Operations_3.0 solution**.
   - To start RulePoint and import the **Operations_3.0 solution**, enter **1**.
   - If you do not want to start RulePoint and import the **Operations_3.0 solution**, enter **2**.
   After the installation is complete, the **Install Complete** section appears.
9. Review the post-installation tasks, and press **Enter** to complete the installation and exit the installer.
CHAPTER 6

After You Install

This chapter includes the following topics:

- Post-Installation Tasks, 45
- Post-Installation Checklist, 46
- (Optional) Revoke User Permissions from Oracle and IBM DB2, 48
- Setting Up Proactive Monitoring for PowerCenter on AIX, 48
- Start and Stop the Proactive Monitoring for PowerCenter Instance, 49
- Import the Objects for Proactive Monitoring for PowerCenter, 50
- Configure Alerts, 50
- Configure LDAP for Proactive Monitoring for PowerCenter, 51
- Create PowerCenter Read-Only Users, 52
- Grant Permissions to PowerCenter Read-Only User, 52
- Configure the Proactive Monitoring Solution, 53
- Configure the RulePoint Components, 53
- Schedule PowerCenter Workflow, 53
- Validate the Installation, 56

Post-Installation Tasks

After installation, perform the post-installation tasks to ensure that Proactive Monitoring for PowerCenter Governance runs properly.
Post-Installation Checklist

The post-installation checklist provides a high-level overview of the tasks that you need to complete after you complete the installation. For detailed instructions, see appropriate sections in this chapter.

Windows and Linux

1. Verify that the following processes are running on the Linux or Windows machine on which you installed RulePoint:
   - java process for design time
   - java process for host agent that runs on the corresponding host and associates with port 19000
   - java process for grid manager that runs on the corresponding host and associates with port 19010
   - java process for node that runs on the corresponding node and associates with port 19020
   - lbmrd
   - umestored

2. If the processes are not running, navigate to <INSTALLER_HOME>/Proactive_Monitoring/bin, and start the Proactive Monitoring for PowerCenter instance, solutions.bat start for Windows or solutions.sh start for Linux. For more information, see “Start and Stop the Proactive Monitoring for PowerCenter Instance” on page 49.

3. If only some of the services are running, perform the following tasks:
   a. Verify that there is sufficient system CPU, memory, and hard disk space available.
   b. Stop the Proactive Monitoring for PowerCenter services using the script solutions.bat stop for Windows and solutions.sh stop for Linux. For more information, see “Start and Stop the Proactive Monitoring for PowerCenter Instance” on page 49.
   c. Start the Proactive Monitoring for PowerCenter instance, solutions.bat start for Windows or solutions.sh start for Linux. For more information, see “Start and Stop the Proactive Monitoring for PowerCenter Instance” on page 49.

4. To verify whether the import of Proactive Monitoring for PowerCenter objects is successful, perform one of the following tasks:
   a. Log in to the RulePoint Console, and navigate to the Import view of the Administrator tab to view the imported xml files. The Governance pack must contain the common.xml, governance.xml, and govCommon.xml files.
      The Operations and Governance pack must contain the common.xml, opsCommon.xml, operations.xml,govCommon.xml, governance.xml, and govCommon.xml files.
   b. Log in to the Proactive Monitoring for PowerCenter Management Console, and click the Manage Objects tab. View the corresponding views in the navigator and verify that the listed objects are in Deployed state. For a list of objects in deployed state, see the .
   c. Verify that the objects are in the Deployed state in RulePoint. Log on to the RulePoint Console, and click the PMPC project in the navigator. Select the corresponding object views and verify that the objects are in the deployed state.
      For example, for a list of topics that are in the deployed state, see “Proactive Monitoring Topics” on page 109.
5. If the import of objects for Proactive Monitoring for PowerCenter is not successful, perform the following tasks:
   a. Import the Proactive Monitoring for PowerCenter Governance 3.0 XML. Run the script from the location `Proactive_Monitoring/bin`.
      For Windows, run the script `pmpc.bat import Governance`.
      For Unix, run the script `pmpc.sh import Governance`.

6. Complete all the steps to configure the Proactive Monitoring solution to connect to the Informatica domain that you want to monitor. For more information, see "Proactive Monitoring Configuration Overview" on page 75, or Proactive Monitoring for PowerCenter Getting Started Guide.

Solaris

If the installer fails to start Proactive Monitoring for PowerCenter services and import objects:

1. Verify that you set the LD library path properly. If you have both the 32-bit and 64-bit libstdc++ on your machine, make sure that you include libstdc++ 64-bit in the `LD_LIBRARY_PATH`.

2. Start the Proactive Monitoring for PowerCenter instance, `solutions.bat start` for Windows and `solutions.sh start` for Linux. For more information, see "Start and Stop the Proactive Monitoring for PowerCenter Instance" on page 49.

3. Import the Proactive Monitoring for PowerCenter objects.

4. Verify that all the objects are deployed in RulePoint. Perform the following tasks:
   a. Log in to the Proactive Monitoring for PowerCenter Management Console.
   b. Navigate to the Manage Objects tab, and verify that the objects are in Deployed state. For example, for a list of advanced rules that are in Deployed state, see "Advanced Rules" on page 129.

5. Complete all the steps to configure the Proactive Monitoring solution to connect to the Informatica domain that you want to monitor. For more information, see "Proactive Monitoring Configuration Overview" on page 75, or the Proactive Monitoring for PowerCenter Getting Started Guide.

AIX

The installer will not start the Proactive Monitoring for PowerCenter services. Perform the following tasks:

1. Start the RulePoint design-time instance manually.
   Note: You must have set RULEPOINT_HOME environment variable to `<PROACTIVE_MONITORING_HOME>/rulepoint`.

2. Edit the configurations to reflect the IP of the host where the UM service is running.
   a. Navigate to the Topology View on the Administrator tab.
   b. Edit the configurations to reflect the IP of the host where the UM service is running.

3. Start the run-time instance.
   For instructions to perform steps 1-3, see "Setting Up Proactive Monitoring for PowerCenter on AIX" on page 48.

4. Import the Proactive Monitoring for PowerCenter objects.

5. Verify that all the objects are deployed in RulePoint. Perform the following tasks:
   a. Log in to the Proactive Monitoring for PowerCenter Management Console.
   b. Navigate to the Manage Objects tab, and verify that the objects are in Deployed state. For example, for a list of template rules that are in Deployed state, see "Advanced Rules" on page 129.
6. Complete all the steps to configure the Proactive Monitoring solution to connect to the Informatica domain that you want to monitor. For more information, see “Proactive Monitoring Configuration Overview” on page 75, or the Proactive Monitoring for PowerCenter Getting Started Guide.

(Optional) Revoke User Permissions from Oracle and IBM DB2

For security or other reasons, you might want to revoke some of the Proactive Monitoring for PowerCenter user permissions on Oracle and IBM DB2 after installation.

1. To revoke the create table permissions for users on Oracle, run the following scripts in the Oracle database:
   
   REVOKE CREATE TABLE FROM RULEPOINT_DESIGN
   REVOKE CREATE TABLE FROM RULEPOINT_TOPOLOGY
   REVOKE CREATE TABLE FROM RULEPOINT_ACTIVITY
   REVOKE CREATE TABLE FROM RULEPOINT_TOPOLOGYSTATE
   REVOKE CREATE TABLE FROM RULEPOINT_RTAM
   REVOKE CREATE TABLE FROM PROACTIVE_MONITORING

2. To revoke the create, drop, and alter permissions for the Proactive Monitoring for PowerCenter users on IBM DB2, run the following scripts in the IBM DB2 database:
   
   Revoke CREATEIN,DROPIN,ALTERIN on SCHEMA RULEPOINT_DESIGN from <<pm_user>>
   Revoke CREATEIN,DROPIN,ALTERIN on SCHEMA PROACTIVE_MONITORING from <<pm_user>>
   Revoke CREATEIN,DROPIN,ALTERIN on SCHEMA RULEPOINT_TOPOLOGY from <<pm_user>>
   Revoke CREATEIN,DROPIN,ALTERIN on SCHEMA RULEPOINT_ACTIVITY from <<pm_user>>
   Revoke CREATEIN,DROPIN,ALTERIN on SCHEMA RULEPOINT_TOPOLOGYSTATE from <<pm_user>>
   Revoke CREATEIN,DROPIN,ALTERIN on SCHEMA RULEPOINT_RTAM from <<pm_user>>

Setting Up Proactive Monitoring for PowerCenter on AIX

If you install Proactive Monitoring for PowerCenter on AIX, you must set the user home path, configure the umestore and lbmd on Linux, and copy the required jars.

1. Set up the RULEPOINT_HOME environment variable to the following path:
   
   userhome/Proactive_Monitoring/rulepoint

2. Copy the Proactive Monitoring installation directory to Linux where you want to configure umestore and lbmd.

3. Provide the IP address of the AIX box in the um.multicast.interface property of the rtam-config.properties file located at the following directory:
   
   userhome/Proactive_Monitoring/rulepoint/design/webapps/RTAM/WEB-INF/classes

4. To configure the UM store, unzip the UM related files, Linux.zip, from the following location:
   
   <INSTALLER_HOME>/resources/rulepoint/extras/UM

5. Delete the contents of the UM folder from the following location:
   
   userhome/Proactive_Monitoring/rulepoint/system/UM
6. Copy the unzipped files to the following location on Linux where you copied the Proactive Monitoring directory:
   
   /userhome/Proactive_Monitoring/rulepoint/system/UM

7. To configure java, unzip the java related files, Linux.zip, from the following location:

   <INSTALLER_HOME>/resources/rulepoint/extras/Java

8. Create a file named java, and copy the unzipped files to the following location on Linux where you copied the Proactive Monitoring directory:

   /userhome/Proactive_Monitoring/rulepoint/system/java

9. Give execute permissions to the Proactive Monitoring directory.

10. Start the host agent on the Linux box. Run the following command:

    </userhome/Proactive_Monitoring/rulepoint/bin/startHostAgent.sh -h <Host IP address> -p <port>

11. ON AIX machine, copy the jars for the webservices from /userhome/Proactive_Monitoring/rulepoint/extras to the following locations:

    - /userhome/Proactive_Monitoring/rulepoint/lib
    - /userhome/Proactive_Monitoring/rulepoint/design/webapps/rulepoint/WEB-INF/lib
    - /userhome/Proactive_Monitoring/rulepoint/design/webapps/pmcp/WEB-INF/lib

12. Start the design-time instance, and log in to RulePoint.

13. In the Administration view of the Topology tab, add a host with the IP address of the Linux machine where you want to configure UM store.

14. Edit the UM store and UM lbmrld services to point to the Linux host.

15. Start the RulePoint Host Agent instance and then start the RulePoint Topology instance.

16. Import the solution XML.

---

**Start and Stop the Proactive Monitoring for PowerCenter Instance**

If the Proactive Monitoring for PowerCenter Governance installer fails to start the instance during installation, you can use the solutions.bat command to start the instance on Windows. Use the solutions.sh command to start the instance on UNIX.

The Proactive Monitoring for PowerCenter installer installs the script in the following directory by default:

<INSTALLER_HOME>/Proactive_Monitoring/bin

1. Go to the directory where the script is located.

2. To start the Proactive Monitoring for PowerCenter instance on Windows or UNIX, run the script from the command prompt.

    - On Windows, enter the following command:
      
      solutions.bat start

    - On UNIX, enter the following command:
      
      solutions.sh start
3. To stop the Proactive Monitoring for PowerCenter instance on Windows or UNIX, run the script from the command prompt.
   - On Windows, enter the following command:
     ```
solutions.bat stop
```
   - On UNIX, enter the following command:
     ```
solutions.sh stop
```

Import the Objects for Proactive Monitoring for PowerCenter

If the import of Proactive Monitoring for PowerCenter Governance 3.0 objects fails during installation, you can use the `pmpc.bat` command to import the objects on Windows. Use the `pmpc.sh` command to import the XML on UNIX.

The Proactive Monitoring for PowerCenter installer installs the script in the following directory by default:

`<INSTALLER_HOME>/Proactive_Monitoring/bin`

1. Go to the directory, where the script is located.
2. To import the Proactive Monitoring for PowerCenter Governance 3.0 XML, enter the following command at the command prompt on Windows or UNIX:
   - On Windows, enter the following command:
     ```
     pmpc.bat import Governance
     ```
   - On UNIX, enter the following command:
     ```
     pmpc.sh import Governance
     ```

   **Note:** You can view the imported objects in the RulePoint console. The imported objects are located in the project `PMPC`. Do not change the name of the project.

Configure Alerts

Configure the users or personas to receive alerts through email, Real-Time Alert Manager, or both.

1. Configure Real-Time Alert Manager to receive alerts for the users.

   Log in to Real-Time Alert Manager with each of the following five user IDs. You log in with the IDs to configure Real-Time Alert Manager to receive alerts for each of the users.

   The following table provides the list of user IDs and passwords to log in to RTAM:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>pcmonitor</td>
<td>pcmonitor123</td>
</tr>
<tr>
<td>pcadmin</td>
<td>pcadmin123</td>
</tr>
</tbody>
</table>
2. Configure the alert recipients for personas.

You can configure the delivery of alerts to personas using the Alert Recipients settings tab in the Proactive Monitoring for PowerCenter Management Console. Edit the alerts recipients for each repository, workflow, or folder to monitor.

For more information, see "Alert Recipients Parameters" on page 81.

3. To configure LDAP users to receive Proactive Monitoring for PowerCenter alerts, you must configure LDAP for Proactive Monitoring for PowerCenter from the Administrator tab in the RulePoint user interface, and make the necessary changes for the Proactive Monitoring for PowerCenter alerts recipients in the Proactive Monitoring for PowerCenter Management Console. For instructions to create an LDAP user, see the RulePoint Administrator Guide.

### Configure LDAP for Proactive Monitoring for PowerCenter

Configure LDAP users to receive Proactive Monitoring for PowerCenter alerts.

1. Configure the LDAP server information and create the default LDAP users in RulePoint.

   The role that you assign to the users must have the ROLE_USER and ROLE_ADMIN privileges to log into the Proactive Monitoring for PowerCenter Management Console. For instructions, see the "LDAP Authentication" section in the "User Management" chapter of the RulePoint Administrator Guide.

2. To enable Proactive Monitoring for PowerCenter alerts to the LDAP users, configure the Alert Recipients information and add the users to the appropriate personas. Perform the following tasks:
   a. Log on to the Proactive Monitoring for PowerCenter Management Console.
   b. Click the Settings tab.
   c. Click Alert Recipients in the Navigator, select the domain, and then select Edit from the Actions menu.

      The Alert Recipients Configuration dialog box appears.
   d. In the RTAM List field, replace the RTAM user with the LDAP users that you created in RulePoint for each of the five users.
   e. Click Save.

3. Log on to RTAM as each of the five users created.

**Example**

For the persona, apparchitect, the default associated users are apparchitect and pcmonitor. The users, apparchitect and pcmonitor, receive the Proactive Monitoring for PowerCenter alerts associated with the persona apparchitect. If you want to use LDAP users instead of apparchitect and pcmonitor, you must modify the Proactive Monitoring for PowerCenter alerts recipients table and replace the RTAM users list with the list of required LDAP users, for example, LDAP user1;user2.
Create PowerCenter Read-Only Users

Create the database user, pcrs_readonly, with read-only permissions to access each PowerCenter repository database.

Important: You must create the PowerCenter read-only user to enable the Proactive Monitoring solution to monitor the PowerCenter Repository Service.

The installer saves the required files to the installation directory. The files contain the database scripts and instructions to create the PowerCenter read-only user with required privileges for the databases.

You can find the database scripts in the following path of the installation directory:

- **Oracle.** `<PROACTIVE_MONITORING_HOME>\Solutions\PMPC\ddls\powercenter\oracle\create_pc_user.txt`
  1. Log in as sys. Run the SQL commands in the `create_pc_user.txt` file to create the PowerCenter repository read-only user.
  2. Log in as the PowerCenter repository read-only user and run the `pcrs_readonly.dd1.sql` script.

- **Microsoft SQL Server.** `<PROACTIVE_MONITORING_HOME>\Solutions\PMPC\ddls\powercenter\mssql\create_pc_user.txt`
  1. Follow the steps in the `create_pc_user.txt` file to create the PowerCenter repository read-only user. Grant SELECT permission to `pcrs_readonly` on table, `sys.database_files`.
  2. Log in as the PowerCenter repository read-only user and follow the instructions in the `pcrs_readonly.dd1.sql` script.

- **IBM DB2.** `<PROACTIVE_MONITORING_HOME>\Solutions\PMPC\ddls\powercenter\db2\create_pc_user.txt`
  1. Follow the steps in the `create_pc_user.txt` file to create the PowerCenter repository read-only user.
  2. Log in as the PowerCenter repository read-only user and follow the instructions in the `pcrs_readonly.dd1.sql` script.

Grant Permissions to PowerCenter Read-Only User

In Microsoft SQL Server, grant execute permissions to the PowerCenter read-only user on the functions, `TO_DATE_MMDDYYYYHHMM` and `TO_DATE_MMDDYYYYHHMMSS`.

Detailed instructions on how to grant permissions to `pcrs_readonly` are available in the `create_pc_user.txt` file in the following directory of the installer:

`..\resources\dbscripts\powercenter\sqlserver`
Configure the Proactive Monitoring Solution

Log on to the Proactive Monitoring for PowerCenter Management Console, and provide details of the nodes, hosts, files and folders on the host, the PowerCenter Repository Services, Integration Services, Web Services Hub that you want to monitor.

Use the Proactive Monitoring Management Console to configure the global settings, alert recipients, and the source timestamp parameters.

You can access the Proactive Monitoring for PowerCenter Management Console through a web browser.

http://<host>:<port>/pmpc

Replace <host> with the host name or IP address of the server where you install Proactive Monitoring for PowerCenter. Replace <port> with the HTTP port number of the Apache Tomcat server. Default is 8080.

**RELATED TOPICS:**

- "Proactive Monitoring Configuration Overview" on page 75

Configure the RulePoint Components

Configure the RulePoint components to work with the rules and services of Proactive Monitoring for PowerCenter Governance.

Configure Email Connection

In RulePoint, edit *email_connection* to add information about the email host server and its authentication credentials for the organization.

1. On the **Design** tab of the RulePoint Console, click the **PMPC** project in the Navigator.
2. In the **Connections** view, select **email_connection** from the list in the contents panel.
3. Select **Edit** from the **Actions** menu.
4. Enter the email server, port number, and the required details for the email service.
5. To test that the connection details are correct, click **Test Connection**.
6. Click **Save**.
   - If you edit a deployed connection, click **Save and Update** to deploy the connection and the associated objects. The state of the connection changes to Deployed.

Schedule PowerCenter Workflow

Schedule a workflow in PowerCenter to populate data in PMPC reports. Reporting uses the PowerCenter workflow to transform PMPC alert data to reporting specific format.

During PMPC installation, the PMPC installer creates the wf_pmpc_reports workflow to populate PMPC reports. You must import the workflow into PowerCenter and define schedule for the workflow. You can set the schedule based on the time interval at which you want to refresh data in the PMPC reports dashboard.
It is recommended that you schedule the workflow such that it has less interference with the PowerCenter environment.

Complete the following tasks to populate PMPC reports:

1. Copy the ETL file that contains the workflow to populate reports data. The PMPC installer creates the ETL_ALL_PMPC_v30.xml file during PMPC installation.
2. Create a folder in the PowerCenter repository to store the workflow and mappings in the ETL_ALL_PMPC_v30.xml file.
3. Create a connection object in the PowerCenter Workflow Manager. Use the connection that you specified in the Reports Configuration section while installing PMPC.
4. Import the ETL file to the PowerCenter repository.
5. Create schedule for the wf_pmpc_reports workflow to populate data in the PMPC reports. The default schedule for the wf_pmpc_reports workflow is 4 hours. Depending on the database workload, you might want to at schedule the workflow at different times during the off peak hours of the day.

If you have not specified the report configuration settings during installation, replace occurrences of the following names in the ETL_ALL_PMPC_v30.xml file:

- **REPORTING_DOMAIN**: Replace with the name of the Informatica domain.
- **REPORTING_IS_NAME**: Replace with the name of the Integration Service to run these workflows.
- **REPORTING_CONNECTION_NAME**: Replace with the connection name for the PowerCenter repository.
- **PM_SCHEMA**: Replace with the Proactive Monitoring schema name.

**Note**: Ensure that at least 30 connections to the PowerCenter repository are available to run the workflow.

**Copy the ETL File**

Copy the ETL file that contains the workflow to populate reports data from the PMPC installation folder. During PMPC installation, you specify the domain, Integration Service, and connection information to use with the workflow to populate data in PMPC reports. Configure the connection to the Proactive Monitoring Database in PowerCenter Workflow Manager.

The PMPC Installer creates the ETL_ALL_PMPC_v30.xml file with these values in the following location:

\<PROACTIVE_MONITORING_HOME\>\Solutions\PMPC\reporting\etl\<database>\|

Copy the ETL_ALL_PMPC_v30.xml file from the PMPC installation location to a folder in the system in which the PowerCenter clients are installed.

**Create a Folder in the PowerCenter Repository**

Create a folder in the PowerCenter Repository Manager to store the workflow in the ETL file.

1. In the Repository Manager, connect to the repository.
2. Click *Folder > Create*.
   - The Create Folder dialog box appears.
3. Enter the information for folder properties.
4. Click *OK*. 

54 Chapter 6: After You Install
Create a Connection Object

Before you import and schedule the workflow, you must configure connections in the Workflow Manager. Configure the connection to the PMPC repository in the PowerCenter Workflow Manager.

1. In the Workflow Manager, click Connections and select Relational connection type.
   The Relational Connection Browser dialog box appears.
2. Click New.
   The Select Subtype dialog box appear.
3. Select the database and click OK.
   The Relational Connection Editor dialog box appears.
4. Specify the relational connection properties. For connection name, enter the connection name that you provided for reports configuration during PMPC installation as the connection name.
   The following table describes the relational connection properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the connection that you specified for reports configuration during PMPC installation.</td>
</tr>
<tr>
<td>User Name</td>
<td>Database user name with the appropriate read and write database permissions to access the database.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the database user name.</td>
</tr>
<tr>
<td>Server name</td>
<td>Database server name. Use to configure the workflow.</td>
</tr>
</tbody>
</table>
5. Click OK.
   The database connection appears in the Connection Browser list.

Import the ETL File to PowerCenter Repository

Use the Import Wizard in the Repository Manager to import the workflow from the ETL file.

1. Open the folder into which you want to import an object.
2. Click Repository > Import Objects.
   The Import Wizard appears.
3. In the Import Wizard, click Browse to locate the ETL XML file that you copied to the PowerCenter client system. Navigate to the directory where the ETL XML file is located. Select the ETL XML file and click OK.
4. Click Next.
   The Select objects to import step of the Import Wizard appears.
5. Click Add All and then click Next.
   The Match Folders step of the Import Wizard appears.
6. In the Destination folder, select the folder that you created in the PowerCenter repository to store the workflow and click OK.
7. Click Next.
   The Choose Options step of the Import Wizard appears.
8. Click **Next**.
   The **Specify rules for conflict resolutions** step of the Import Wizard appears.

9. Click **Next**.

10. Click **Import**.
    The **Conflict Resolutions** Wizard appears.

11. To resolve the default_session_config in the Session Configuration, select **Rename** and **Click Apply this resolution to**.

12. Click **Close** when you resolve all the conflicts for this folder.
    The **Import** Wizard appears.

13. Click **Import** to import the objects into the repository.

14. Click **Finish**.

15. Click **Done**.

**Configure Scheduler for Workflow**

Configure scheduler settings to set run options, schedule options, start options, and end options for the schedule. The Integration Services runs the workflow at the scheduled time.

To configure scheduler settings for a workflow:

1. In the Workflow Manager, click **Workflows > Schedulers**.
2. In the **Scheduler Browser** dialog box, select the scheduler for the workflow and click **Edit**.
3. In the **Schedule** tab of the **Edit Scheduler** screen, configure the scheduler settings for the workflow.
4. Click **OK**.

Configure scheduler for the *wf_pmpc_reports* workflows to populate data in PMPC reports:

The default schedule for the workflow is 4 hours. Depending on the database workload, you might want to at schedule the workflow at different times during the off peak hours of the day. If you add hosts, nodes, Repository Services, or Integration Services, rerun the *wf_pmpc_reports* workflow.

**Note:** Ensure to clear the browser cache and refresh or reload the browser after you run the workflow to populate data in reports.

**Validate the Installation**

After you complete installation, log into the Proactive Monitoring for PowerCenter Management Console and validate the installation.

You can validate the installation by viewing alerts and reports for events in the following dashboards:

- **Real-Time Alert Manager** dashboard. You receive alerts in the Real-Time Alert Manager dashboard or through the configured email. Log in to Real-Time Alert Manager to check alert generation.
- **Reports** dashboard. You can view alerts and usage statistics from the Reports dashboard.
  For example, create a mapping in PowerCenter Designer. When you save the mapping, you get an email or Real-Time Alert manager alert if the mapping is not valid.
- **RulePoint** dashboard. You can view the events generated for a PMPC topic from the **Events** view on the **Dashboard** tab.
**RELATED TOPICS:**

- "Proactive Monitoring Configuration" on page 75
Upgrading Proactive Monitoring for PowerCenter Governance Overview

You can upgrade Proactive Monitoring for PowerCenter Governance version 2.6 to 3.0 on Windows, Linux, AIX, or Solaris. To upgrade earlier versions of 2.6, you must first upgrade to 2.6 and then upgrade to 3.0.

Before you upgrade, consider the version that you want to upgrade:

- **Upgrade Versions Prior to 2.6**
  To upgrade from Proactive Monitoring for PowerCenter Governance versions prior to 2.6, you must first upgrade to version 2.6 and then upgrade to version 3.0.

- **Upgrade Version 2.6 to 3.0**
  You can upgrade Proactive Monitoring for PowerCenter Governance version 2.6 to 3.0.

  Run the upgrade installer in graphical or console mode. Complete the pre-upgrade tasks to prepare for the upgrade. You can upgrade to Proactive Monitoring for PowerCenter Governance 2.6 to 3.0 from a DVD or from the root of the directory where you download the installation files. When you run the installer for upgrade, provide the correct location for RP_HOME. After the upgrade, the installer copies the configurations that you set up in version 2.6 to 3.0. You cannot, however, see the alert history and reports from the previous version.
If you have installed both Proactive Monitoring for PowerCenter Operations and Proactive Monitoring for PowerCenter Governance 2.6, you must first complete the upgrade for both Operations and Governance and then run the migration tool.

After you upgrade from 2.6 to 3.0, use the migration tool to migrate objects from version 2.6. The migration tool creates an XML file containing the 2.6 objects that you can import into the PMPC project in version 3.0.

If you had configured LDAP users for Proactive Monitoring for PowerCenter 2.6, the LDAP settings are not migrated to 3.0. You must configure the LDAP users explicitly after installing Proactive Monitoring for PowerCenter 3.0. For more information about setting LDAP, see the "LDAP Authentication" section in the "User Management" chapter of the RulePoint Administrator Guide.

Before You Upgrade

Before you upgrade Proactive Monitoring for PowerCenter Governance, set up the machine to meet the requirements to install and run the Proactive Monitoring solution.

Complete the following prerequisites before you upgrade to Proactive Monitoring for PowerCenter Governance 3.0:

1. Ensure that Proactive Monitoring for PowerCenter Governance 2.6 is installed on the system where you want to upgrade to 3.0.
2. On Linux, the user who runs the installer must have read, write, and execute permissions on the installer and its files directory, and write access to the /tmp directory. The /tmp directory must have a minimum of 200 MB for the installer to perform the upgrade.
3. Back up the essential alert history and PowerCenter Monitored Folders watchlist. The upgrade installer clears all alert history and PowerCenter Monitored Folders watchlist contents.
4. Shut down the instance of Apache Tomcat application server on which you have set up Proactive Monitoring for PowerCenter Governance 2.6.
5. Shut down the 2.6 Node Agent instance on all the PowerCenter hosts where it is running.
6. Verify the minimum system requirements.
7. Create a database user with administrator privileges. The installer creates the following schemas when you choose typical installation:
   - RulePoint_Design
   - RulePoint_RTAM
   - RulePoint_Topology
   - RulePoint_Activity
   - RulePoint_TopologyState
   - Proactive_Monitoring
   If you do not want to grant the database administrator privileges, you can use the custom mode of installation for which you must configure the schemas and provide the database user the required permissions.
8. You require the correct location for RP_HOME where you installed Proactive Monitoring for PowerCenter 2.6. RP_HOME is the path of the RulePoint directory in the Apache Tomcat server. For example, c:\tomcat\webapps\rulepoint.
Planning Considerations for Migrating Objects from Version 2.6

The installer installs the 3.0 objects when you upgrade Proactive Monitoring for PowerCenter Operations 2.6 to 3.0. The default objects available in the Proactive Monitoring for PowerCenter Operations or Governance 2.6 installation are also available in 3.0. After the upgrade, the configurations that you set up in the Proactive Monitoring for PowerCenter Management Console version 2.6 appear in version 3.0. Use the migration tool to migrate objects, other than the default objects, that you created or customized in 2.6 to 3.0.

You do not have to configure the setup in the Proactive Monitoring for PowerCenter Management Console. For example, the domain, alert, recipient, PowerCenter Repository Service, nodes, PowerCenter Integration Service, and PowerCenter Web Service Hub configurations on the Management Console are migrated as part of the upgrade. However, the reporting configurations, alerts, and alert history are not migrated.

You cannot migrate all objects between 2.6 and 3.0. The following list helps you understand which objects you can migrate from 2.6 to 3.0:

**Topics**

The following table provides information about topics that you can migrate from 2.6 to 3.0:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Migration from 2.6 to 3.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default topics created as part of Proactive Monitoring for PowerCenter 2.6 installation. The topics do not involve an edit, rename, or change in content in 2.6.</td>
<td>No</td>
<td>Migration is not applicable. The upgrade from 2.6 to 3.0 installs the topics.</td>
</tr>
<tr>
<td>Renamed default topics.</td>
<td>Yes</td>
<td>Migrates renamed topics.</td>
</tr>
<tr>
<td>Default topics are edited, but the topic name remains the same.</td>
<td>No</td>
<td>Does not migrate the edited topics. The migration tool generates a report that lists the topics that are not migrated.</td>
</tr>
</tbody>
</table>

**Rules**

The following table provides information about rules that you can migrate from 2.6 to 3.0:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Migration from 2.6 to 3.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default rules created as part of Proactive Monitoring for PowerCenter 2.6 installation. The rules do not involve an edit, rename, or change in content.</td>
<td>No</td>
<td>Migration is not applicable. The upgrade from 2.6 to 3.0 installs the rules.</td>
</tr>
<tr>
<td>New advanced rules created in 2.6.</td>
<td>Yes</td>
<td>Migrates new advanced rules.</td>
</tr>
<tr>
<td>New template rules created in 2.6.</td>
<td>Yes</td>
<td>Migrates template rules. <strong>Note:</strong> You can migrate template rules only if you include the associated templates in the migration.</td>
</tr>
<tr>
<td>Scenario</td>
<td>Migration from 2.6 to 3.0</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Default rule names renamed in 2.6.</td>
<td>Yes</td>
<td>Migrates the renamed rules.</td>
</tr>
<tr>
<td>Content in default rules updated, but the name of the rule does not involve a change.</td>
<td>No</td>
<td>Does not migrate the rules. A report is generated that lists the rules that are not migrated.</td>
</tr>
<tr>
<td>New wizard rules.</td>
<td>No</td>
<td>You must convert the wizard rule to an advanced rule in 2.6 and then migrate.</td>
</tr>
</tbody>
</table>
### Scenario Migration from 2.6 to 3.0 Comments

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Migration from 2.6 to 3.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default sources edited in 2.6, but not renamed.</td>
<td>No</td>
<td>Does not migrate edited sources if you do not rename those sources.</td>
</tr>
<tr>
<td>Renamed default sources.</td>
<td>Yes</td>
<td>Migrates renamed sources.</td>
</tr>
</tbody>
</table>

**Responses**

The following table provides information about responses that you can migrate from 2.6 to 3.0:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Migration from 2.6 to 3.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default responses.</td>
<td></td>
<td>Migration not applicable. The upgrade from 2.6 to 3.0 installs the responses.</td>
</tr>
<tr>
<td>Renamed default responses.</td>
<td>Yes</td>
<td>Migrates renamed responses.</td>
</tr>
<tr>
<td>Edited responses, but do not involve rename.</td>
<td>No</td>
<td>Does not migrate the responses. The migration tool generates a report that lists the topics that are not migrated.</td>
</tr>
</tbody>
</table>

**Templates**

The following table provides information about templates that you can migrate from 2.6 to 3.0:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Migration from 2.6 to 3.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default templates created as part of 2.6 installation. The templates do not involve an edit, rename, or change in content.</td>
<td>No</td>
<td>Migration is not applicable.</td>
</tr>
<tr>
<td>New templates created in 2.6.</td>
<td>Yes</td>
<td>Migrates the templates.</td>
</tr>
<tr>
<td>Renamed default templates.</td>
<td>Yes</td>
<td>Migrates the renamed templates.</td>
</tr>
<tr>
<td>Default templates that involve a content update but the template name remains the same.</td>
<td>No</td>
<td>Does not migrate. A report is generated when you upgrade that lists the templates that are not migrated.</td>
</tr>
</tbody>
</table>
Users

The following table provides information about users that you can migrate from 2.6 to 3.0:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Migration from 2.6 to 3.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users created in 2.6 other than the default users created during installation.</td>
<td>Yes</td>
<td>By default, input.read_users in the properties file is set to false. You need to change the setting to true to migrate any users created in 2.6. The 3.0 installer creates the default users for Proactive Monitoring for PowerCenter. Note: The migration tool does not migrate the LDAP users from 2.6.</td>
</tr>
</tbody>
</table>

Upgrading in Graphical Mode

You can upgrade in graphical mode on Windows, Linux, AIX, or Solaris.

1. Run the Proactive Monitoring for PowerCenter Governance installer based on the operating system.
   - To install on Windows, run Informatica_PMPC_Governance_3.0.exe from the root directory.
   - To install on Linux, AIX, or Solaris, use a shell command line to run Informatica_PMPC_Governance_3.0.bin from the root directory with -i gui option for graphical mode installation. For example, enter Informatica_PMPC_Governance_3.0.bin -i gui.

2. In the Introduction page, choose the option Upgrade Proactive Monitoring for PowerCenter Governance 3.0, and click Next.

3. Specify the path to RP_HOME where you have installed the previous version, and press Next.
   The following table shows the location of the installation folder where you installed the previous version:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>c:\tomcat\webapps\rulepoint</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/tomcat/webapps/rulepoint</td>
</tr>
</tbody>
</table>

   The Choose Installation Folder page appears.

4. Specify the location of the installation directory.
   The following table shows the default location of the installation directory:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Proactive_Monitoring</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/Proactive_Monitoring</td>
</tr>
</tbody>
</table>

   Note: Do not use the same path as 2.6 RP_HOME.
5. Click **Next**. The **License File** page appears.

6. Provide the full path of the Proactive Monitoring for PowerCenter license file, and click **Next**. The **Database Configuration Mode** page appears.

7. Specify the database configuration mode:
   - If you want to use the default database schemas that the installer creates, select **Typical**.
   - If you want to use the database schemas that you created, select **Custom**.
     For instructions to configure the custom schemas, see "Prerequisites for Custom Installation" on page 29.

The **Database Configuration** page appears.

8. Enter the database information where you want to configure Proactive Monitoring for PowerCenter. You must have database administrator privileges on the database in which you want to configure Proactive Monitoring for PowerCenter.

The following table describes the database properties that you specify for Proactive Monitoring for PowerCenter:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database of Proactive Monitoring for PowerCenter 2.6.</td>
</tr>
<tr>
<td>Database User Name</td>
<td>User name for the database user account. The user must have the database administrator privileges on the database and at least 100 connection sessions to the database.</td>
</tr>
<tr>
<td>Database Password</td>
<td>Password for the database user account.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Hostname of the database.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Port number of the database.</td>
</tr>
<tr>
<td>Service Name/SID Name</td>
<td>Service name or SID name for Oracle, IBM DB2, or Microsoft SQL Server database.</td>
</tr>
<tr>
<td>JDBC Parameters</td>
<td>Optional. JDBC parameters to include in the JDBC URL. Optionally, you can specify additional JDBC parameters to include in the JDBC URL.</td>
</tr>
<tr>
<td>Custom Connection String for DataDirect driver</td>
<td>Optional. Connection string to connect to the database. To provide a customized connection string, select this option and enter the custom connection string.</td>
</tr>
</tbody>
</table>

9. Click **Test Connection** to verify that you can connect to the database.

The success message appears if the connection to the database is successful. If you had selected typical database configuration mode, the installer creates the following schemas for Proactive Monitoring for PowerCenter:

- RulePoint_Design
- RulePoint_RTAM
- RulePoint_Topology
- RulePoint_TopologyState
• RulePoint_Activity
• Proactive_Monitoring

If you had selected custom database configuration mode, you must provide the custom schema names that you have created.

10. Click **Next**.

    The **Host and HTTP Configuration** dialog box appears.

11. Enter the Proactive Monitoring for PowerCenter host IP and port details.

    The following table describes the Proactive Monitoring for PowerCenter host configuration details:

    | Property   | Description                                                                 |
    |------------|-----------------------------------------------------------------------------|
    | Host IP    | IP address of the host where you install Proactive Monitoring for PowerCenter. |
    | Tomcat Port| HTTP port number of the Tomcat server. The default port is 8080.            |

12. If you want to enable a secure connection to access Proactive Monitoring for PowerCenter, perform the following steps, and then click **Next**:

    a. Select **Enable HTTPS for Proactive Monitoring for PowerCenter**.
    b. Enter the port number. By default, the port number is 8443.
    c. Select either a keystore generated by the installer, or use an existing keystore, and click **Next**.
    d. If you use an existing keystore, enter the keystore password and the name of the keystore file.

13. To configure email notifications to receive alerts for process failures in Proactive Monitoring for PowerCenter, click **Advanced Configurations**.

    The **Advanced Configurations** dialog box appears.

    • Select **Enable Email Notification**, configure the following email notification settings, and then click **Save**:

<pre><code>| Property | Description                                                                 |
|----------|-----------------------------------------------------------------------------|
| SMTP Host| The fully qualified domain name of the SMTP server that you use to send outbound email from RulePoint. For example, mail.mycompany.com |
| Port     | Port number of the SMTP server.                                             |
| From     | Sender email address from which you send outbound emails.                   |
| To       | Email recipient address to which you send notifications.                    |
</code></pre>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Priority       | Email messages with the priority that you want to receive. Select from the following options:  
- Critical  
- High  
- Medium  
- Low  
For example, select **Critical** to receive email messages that have the priority as critical. When the default node fails, you receive an email alert of critical priority with the message that the default node has failed. |
| Verbosity      | Verbosity of the email notification. Select from the following options:  
- More  
- Less  
For example, select **Less** to receive email messages with brief information of the alert. |
| User Name      | Optional. The user account name of the SMTP server.                                                                                          |
| Password       | Optional. The user account password of the SMTP server.                                                                                       |

- If you do not want to configure email notifications during installation, click **Cancel**.

The **PowerCenter Configuration** page appears.

14. Enter the Informatica domain name.

The domain name is the name of the Informatica domain that you want to monitor. You can get the domain information from the Informatica domain administrator.

**Note:** The installer does not validate the domain name. Enter the correct name for the domain that you want to monitor.

15. To configure Proactive Monitoring reports, select **Enable Reporting for Proactive Monitoring**.

Proactive Monitoring for PowerCenter uses pre-defined PowerCenter workflows to transform alert data into the format required by Proactive Monitoring for PowerCenter reports. When you configure reports, the installer generates and configures an ETL file that contains the workflows to populate data in reports.

16. Configure the following report settings, and click **Next**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Informatica Domain        | Name of the Informatica domain in which you want to run the workflows to populate data in reports.  
**Note:** It is recommended that you do not use the same Informatica domain name that you provided for monitoring. |
| PowerCenter Integration Service | Name of the PowerCenter Integration Service to run the workflows.  
**Note:** Name of the relational connection used in the reporting workflow. This connection connects to the database where the proactive_monitoring schema is available. |

The installer generates and configures the `ETL_ALL_PMPC_v30.xm1` with the values you provide. After the installation, the `ETL_ALL_PMPC_v30.xm1` file is available in the following location:  
`<PMPC Installation folder>/Solutions/PMPC/reporting/etl/<database>`
You must import the ETL_ALL_PMPC_v30.xml file in to PowerCenter and run the workflows to transform the alert data.

The Proactive Monitoring 2.6 Configuration section appears that displays the database details.

17. Enter the password for the Proactive Monitoring database user account.

The Pre-installation Summary section appears.

18. Review the pre-installation summary, and click Install.

If you are using Windows, a message appears prompting you to register for Windows services.

19. Choose whether you want to register services for RulePoint components.
   - To create Windows services for the RulePoint components, click Yes. The RulePoint Design Time, RulePoint HostAgent, and RulePoint Topology services are created in the Windows services. You can use these services to start or stop the RulePoint instances after you complete the installation.
   - If you do not want to register Windows services for RulePoint components, click No.

After the installation is complete, the Install Complete page appears.

20. Review the post-installation tasks, and click Done to complete the installation procedure and exit the installer.

Upgrading in Console Mode

You can upgrade in console mode on Windows, Linux, AIX, or Solaris.

**Note:** When you run the installer in console mode, the words Quit and Back are reserved words. You cannot use the reserved words as input text during installation.

1. At the command prompt for Windows or on a shell command line for Linux, AIX, and Solaris, run the Proactive Monitoring for PowerCenter Governance installer located in the root directory.

2. Enter the Proactive Monitoring for PowerCenter Governance executable name with the option -i console.
   - For Windows, enter zs.informatica_PMPC_Governance_3.0.exe -i console.
   - For Linux, AIX, or Solaris, enter Informatica_PMPC_Governance_3.0.bin -i console.

3. In the Introduction section, enter 2 to upgrade Proactive Monitoring for PowerCenter Governance 3.0, and press Enter.

4. Specify the path to RP_HOME where you have installed the previous version, and press Enter.

The following table shows the location of the installation folder where you installed the previous version:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>c:\tomcat\webapps\rulepoint</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/tomcat/webapps/rulepoint</td>
</tr>
</tbody>
</table>

The Choose Installation Folder page appears.

5. Specify the location of the installation directory.
The following table shows the default location of the installation directory:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Proactive_Monitoring</td>
</tr>
<tr>
<td>Linux, AIX, and Solaris</td>
<td>/home/Proactive_Monitoring</td>
</tr>
</tbody>
</table>

**Note:** Do not use the same path as 2.6 RP_HOME.

6. If you enter a different folder, enter Y to confirm the installation directory path.

   The **License File** section appears.

7. Enter the full path of the Proactive Monitoring for PowerCenter license file, and press **Enter**.

   The **Database Configuration Mode** section appears.

8. Specify the database configuration mode, and then press **Enter**.

   - To run the Typical mode and create the required database schemas with the default names, enter 1.
   - To run the Custom mode and use the database schemas that you created, enter 2.

     For instructions to configure the custom schemas, see “Prerequisites for Custom Installation” on page 29.

   The **Database Configuration** section appears.

9. Enter the user name for the database user account, and then press **Enter**. The user must have the database administrator privileges on the database and at least 100 connection sessions to the database.

10. Enter the password for the database user account, and then press **Enter**.

11. Specify an option to use custom JDBC connection string, and then press **Enter**.

    - To use a custom JDBC connection string to enter the JDBC connection information, press Y.
      Enter the connection string and verify that the connection string contains all the connection parameters.
    - If you do not want to use the custom JDBC connection string to enter the JDBC connection information, press N, and then enter the database connection information.

The following table describes the connection properties that you specify for Proactive Monitoring for PowerCenter:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database of Proactive Monitoring for PowerCenter 2.6.</td>
</tr>
<tr>
<td>Database User Name</td>
<td>User name for the database user account. The user must have the database administrator privileges on the database and at least 100 connection sessions to the database.</td>
</tr>
<tr>
<td>Database Password</td>
<td>Password for the database user account.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Host name of the database.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Port number of the database.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Name/SID Name</td>
<td>Service name or SID name for Oracle, IBM DB2, or Microsoft SQL Server database.</td>
</tr>
<tr>
<td>JDBC Parameters</td>
<td>Optional. JDBC parameters to include in the JDBC URL. Optionally, you can specify additional JDBC parameters to include in the JDBC URL.</td>
</tr>
<tr>
<td>Custom Connection String for DataDirect driver</td>
<td>Optional. Connection string to connect to the database. To provide a customized connection string, select this option and enter the custom connection string.</td>
</tr>
</tbody>
</table>

If you had selected typical database configuration mode, the installer creates the following schemas for Proactive Monitoring for PowerCenter:

- RulePoint_Design
- RulePoint_RTAM
- RulePoint_Topology
- RulePoint_TopologyState
- RulePoint_Activity
- Proactive_Monitoring

If you had selected custom database configuration mode, you must provide the custom schema names that you have created.

The **Host and HTTP Configuration** section appears.

12. Enter the Proactive Monitoring for PowerCenter host IP and port details, and then press **Enter**.

The following table describes the Proactive Monitoring for PowerCenter host configuration details:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP</td>
<td>IP address of the server where you install Proactive Monitoring for PowerCenter.</td>
</tr>
<tr>
<td>Tomcat Port</td>
<td>HTTP port number of the Tomcat server. The default port number is 8080.</td>
</tr>
</tbody>
</table>

13. Select whether to set up a secure connection for Proactive Monitoring for PowerCenter:

The following table describes the options available to create or disable a secure connection:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y - Enable HTTPS for Proactive Monitoring for PowerCenter</td>
<td>Set up a secure connection for Proactive Monitoring for PowerCenter.</td>
</tr>
<tr>
<td>N - Disable HTTPS</td>
<td>Do not set up a secure connection for Proactive Monitoring for PowerCenter.</td>
</tr>
</tbody>
</table>

a. If you are enabling HTTPS, enter the configuration details, and then press **Enter**.
The following table describes the HTTPS connection information you must enter if you enable HTTPS:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number for the HTTPS connection.</td>
</tr>
</tbody>
</table>
| Keystore file | Select the following option to use a keystore file generated by the installer or a keystore file you create:  
1 - Use a keystore generated by the installer.  
2 - Use an existing keystore |

b. If you use an existing keystore, enter the password and location of the keystore file.

14. To configure email notifications to receive alerts for process failures in Proactive Monitoring for PowerCenter, enter **Y** to choose **Advanced Configuration**, and then press **Enter**.
   - The following tables describes the email notification settings:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| SMTP Host        | The fully qualified domain name of the SMTP server that you use to send outbound email from RulePoint.  
For example: mail.mycompany.com |
| Port             | Port number of the SMTP server.                                             |
| From             | Sender email address from which you send outbound emails.                  |
| To               | Email recipient address to which you send notifications.                    |
| Priority         | Email messages with the priority that you want to receive. Select from the following options:  
1 - Critical  
2 - High  
3 - Medium  
4 - Low  
For example, enter 1 to receive email messages that have the priority as critical. When the default node fails, you receive an email alert of critical priority with the message that the default node has failed. |
| Verbosity        | Verbosity of the email notification. Select from the following options:  
1 - More  
2 - Less  
For example, enter 1 to receive email messages with detailed alert information. |
| User Name        | Optional. The user account name of the SMTP server.                         |
| Password         | Optional. The user account password of the SMTP server.                     |

- If you do not want to configure email notifications during installation, enter **No**.

The **PowerCenter Configuration** section appears that displays the domain name.
15. Select whether to configure Proactive Monitoring for PowerCenter reports.

The Proactive Monitoring for PowerCenter solution uses pre-defined PowerCenter workflows to transform alert data into the format required by PMPC reports. When you configure reports, the installer generates and configures an ETL file that contains the workflows to populate data in reports.

- To configure Proactive Monitoring for PowerCenter reports, enter **Y** and then configure the following report settings:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informatica Domain</td>
<td>Name of the Informatica domain in which you want to run the workflows to populate data in reports. <strong>Note:</strong> It is recommended that you do not use the same Informatica domain name that you provided for monitoring.</td>
</tr>
<tr>
<td>PowerCenter Integration Service</td>
<td>Name of the PowerCenter Integration Service to run the workflows.</td>
</tr>
<tr>
<td>Workflow Connection Name</td>
<td>Name of the relational connection used in the reporting workflow. This connection connects to the database where the proactive_monitoring schema is available.</td>
</tr>
</tbody>
</table>

The installer generates and configures the **ETL_ALL_PMPC_v30.xml** with the values you provide. After the installation, the **ETL_ALL_PMPC_v30.xml** file is available in the following location: `<PMPC Installation folder>/Solutions/PMPC/reporting/etl/<database>`

You must import the **ETL_ALL_PMPC_v30.xml** file in to PowerCenter and run the workflows to transform the alert data.

- If you do not want to configure Proactive Monitoring for PowerCenter reports, click **N**.

The **Proactive Monitoring 2.6 Configuration** section appears that displays the database details.

16. Enter the password for the Proactive Monitoring database user account.

The **Pre-installation Summary** section appears.

17. Review the pre-installation summary, and then press Enter.

18. If you are using Windows, you can choose to register services for RulePoint components.

- To register Windows services for the RulePoint components, enter **2**.

  The RulePoint Design Time, RulePoint HostAgent, and RulePoint Topology services are created in the Windows services. You can use these services to start or stop the RulePoint instances after you complete the installation.

- If you do not want to register Windows services for RulePoint components, enter **1**.

After the installation is complete, the **Install Complete** section appears.

19. Review the post-installation tasks, and press **Enter** to complete the installation procedure and exit the installer.
Migrating Objects from Proactive Monitoring for PowerCenter Version 2.6 to 3.0

After you upgrade Proactive Monitoring for PowerCenter Governance from version 2.6 to 3.0, run the migration tool to migrate all the objects from 2.6 to 3.0. If you have installed both Proactive Monitoring for PowerCenter Operations and Proactive Monitoring for PowerCenter Governance 2.6, you must first complete the upgrade for both Operations and Governance and then run the migration tool. The migration tool exports the sources, rules, topics, responders, responses, watchlists, analytics, and templates from 2.6 to 3.0. To migrate sources, responders, or analytics, the migration tool first creates the corresponding connections that are supported by 3.0 and then migrates these objects along with the connections.

1. Navigate to the following directory:
   <INSTALLER_HOME>\resources\ppmc\tools

2. Extract the contents of the migration-tool-6.1.zip file, and copy it to the location where you have installed Proactive Monitoring for PowerCenter.

3. Navigate to the \conf directory, and perform the following tasks:
   a. Edit the input.property file with the required values:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input.artifacts_type_list</td>
<td>The list of objects that you want to migrate. You can migrate sources, responders, topics, rules, templates, watchlists, analytics, and responses.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: When you migrate, ensure that you include the required dependencies in the list. To migrate topics, include the required source. To migrate responses, include the required responders. To migrate template rules, include the required templates. To migrate wizard rules, first convert the wizard rules to advanced rules before migration.</td>
</tr>
<tr>
<td>input.read_users</td>
<td>The list of users created in Proactive Monitoring for PowerCenter 2.6. The default users will not be overwritten.</td>
</tr>
<tr>
<td></td>
<td><strong>By default, input.read_users=false. Change the setting to true to migrate any users created in 2.6.</strong></td>
</tr>
<tr>
<td>input.xml.path</td>
<td>The full absolute path of the input XML file that contains the exported 2.6 objects.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You must export the Proactive Monitoring for PowerCenter 2.6 objects that you want to migrate from the RulePoint 5.2 Console. From the Administration view, click Export All to export objects to a local folder.</td>
</tr>
</tbody>
</table>
b. Edit the `output.property` file with the required values:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output.xml_filepath</td>
<td>The location where you want to place the output file containing the migrated objects. Set the property <code>output.xml_filepath</code> to an accessible path for the output.xml file. After you run the migration tool, the output file will contain the migrated objects. The migration tool creates a directory <code>ImportExport</code> at the specified path and the file contains the migrated objects in the <code>ImportExport</code> directory. For example, for the specified path <code>/export/home/john/dir/output.xml</code>, the migration tool creates a directory <code>ImportExport</code> at <code>/export/home/john/dir</code>. The migration tool creates the <code>output.xml</code> file in the <code>ImportExport</code> directory. <strong>Note:</strong> Make sure that you use escape characters for colons and backslashes in the Windows paths. For example, <code>C:\\export\\export.3.0.xml</code>.</td>
</tr>
<tr>
<td>output.rusername</td>
<td>The user name to log into Proactive Monitoring for PowerCenter 3.0. The user name to log into Proactive Monitoring for PowerCenter 3.0.</td>
</tr>
<tr>
<td>output.rpassword</td>
<td>The password for the user to log into Proactive Monitoring for PowerCenter 3.0.</td>
</tr>
</tbody>
</table>

4. To migrate the objects from Proactive Monitoring for PowerCenter version 2.6 to 3.0, run the script from the command prompt from the following location:

```
<INSTALLER_HOME>/resources/pmpc/tools/migration-tool-6.1/bin
```

- On Windows, enter the following command:
  ```
migrate.bat
  ```

- On Unix, enter the following command:
  ```
migrate.sh
  ```

  **Note:** If you run the `migrate.sh` script on Solaris, replace `$JAVA_EXE -cp .:..:/lib/*:.../...` with the following value:

  ```
  $JAVA_EXE -cp .:..:/lib/*:...:/conf:$RULEPOINT_HOME/custom/*:$RULEPOINT_HOME/design/webapps/rulepoint/WEB-INF/classes:$RULEPOINT_HOME/design/lib/*:$RULEPOINT_HOME/design/webapps/rulepoint/WEB-INF/lib/ehcache-2.7.0.jar:$RULEPOINT_HOME/design/webapps/rulepoint/WEB-INF/lib/*
  ```

  The tool returns a list that displays the details of the objects that are migrated. The list also displays details of the objects or users in 2.6 that already exist in Proactive Monitoring for PowerCenter 3.0 installation and will not be exported into version 3.0. A report `migrate.log` is generated at `<INSTALLER_HOME>/resources/pmpc/tools/migration-tool-6.1/logs` that contains the migration details.

5. A message prompts you to confirm whether you want to continue to import the objects into version 3.0.

- Type **Yes** to import the objects to Proactive Monitoring for PowerCenter 3.0.
- Type **No** to import the XML file later. You can import the xml file generated from the location that you have specified in the `output.properties` file.
Running the Migration Tool on AIX

You need to complete the prerequisites before you run the migration tool on AIX.

Choose one of the following options:

- In the migrate.sh file located at `<INSTALLER_HOME>/resources/pmpc/tools/migration-tool-6.1/bin`, replace `<JAVA_EXE>` with `JAVA_HOME/bin/java` of the AIX host.
  For example, edit `<JAVA_EXE>` -cp `.../lib/*:/conf:<RULEPOINT_HOME>/*` with `JAVA_HOME/bin/java -cp `.../lib/*:/conf:<RULEPOINT_HOME>`.
- Copy the updated migration-tool-6.1 folder and the exported 2.6 xml file from the Linux host.

After You Upgrade

After you upgrade, perform the post-installation tasks to ensure that the services for Proactive Monitoring for PowerCenter Governance run properly.

1. If you perform a migration, complete the following tasks:
   - The migration tool does not create schedules for migrated sources. Create a schedule for the sources in 3.0 using the RulePoint User Interface. For instructions to create schedules, see the `RulePoint User Guide`.
   - The import might cause a change in state of objects to Needs_Deployment. You need to redeploy these objects. For instructions to deploy the objects, see the `RulePoint User Guide`.
   - Delete the templates: PC_OT5 PowerCenter statistics when memory consumption of the integration service node exceeds threshold and PC_OT4 PowerCenter statistics when integration service node CPU consumption exceeds threshold that are not used for Proactive Monitoring for PowerCenter 3.0.
   - Edit and save the monitored folder from Manage Objects > Monitored Folders. Click Update Runtime for the changes to reflect.

2. Grant permissions to the PowerCenter read-only users for the PowerCenter repositories. If the database type is Oracle, perform the following tasks:
   - Log in as the PowerCenter repository owner and run the following script:
     ```bash
     GRANT SELECT ON <<repo_owner>>.OPB_WIDGET_FIELD TO pcsr_readonly;
     ```
     where `<<repo_owner>>` is the owner of the PowerCenter repository.
   - Log in as pcsr_readonly user, and create the following synonym:
     ```sql
     CREATE OR REPLACE SYNONYM OPB_WIDGET_FIELD FOR <<repo_owner>>.OPB_WIDGET_FIELD;
     ```
     where `<<repo_owner>>` is the owner of the PowerCenter repository.

3. If the database type is IBM DB2, perform the following tasks:
   - Log in as the PowerCenter repository owner and run the following script:
     ```bash
     GRANT SELECT ON <<repo_owner>>.OPB_WIDGET_FIELD TO pcsr_readonly;
     ```
     where `<<repo_owner>>` is the owner of the PowerCenter repository.
   - Log in as pcsr_readonly user, and create the following synonym:
     ```sql
     CREATE SYNONYM OPB_WIDGET_FIELD FOR <<repo_owner>>.OPB_WIDGET_FIELD;
     ```
     where `<<repo_owner>>` is the owner of the PowerCenter repository.

4. Schedule and run workflows in PowerCenter to populate data in the Reports dashboard.
Proactive Monitoring Configuration Overview

Configure the Proactive Monitoring solution to connect to the Informatica domain that you want to monitor.

The Informatica domain can contain multiple repository services, repository databases, PowerCenter Integration Service, and Web Services Hub running on multiple physical or virtual machines.

To monitor PowerCenter best practices, the Proactive Monitoring solution collects data from the PowerCenter repository databases at regular intervals. The Proactive Monitoring solution uses the collected information to check for anomalies in the metadata of PowerCenter objects, and alert appropriate users. The alert messages contain required contextual information, such as the PowerCenter object name and the cause of the alert.

You can use the Proactive Monitoring for PowerCenter Management Console to configure the Proactive Monitoring solution.
Proactive Monitoring for PowerCenter Management Console

The Proactive Monitoring for PowerCenter Management Console is a web application that you can use to configure the Proactive Monitoring solution to monitor the PowerCenter domain.

You can use the Management Console to add details of PowerCenter hosts, nodes, grids, and the application services that you want to monitor. The application services include the PowerCenter Repository Service, the PowerCenter Integration Service, and the Web Services Hub. You can use the Management Console to change the monitoring solution settings and the mode of alert delivery, whether to use email or RTAM.

A single installation of the Proactive Monitoring solution can monitor a single domain, with its multiple PowerCenter repository databases, application services, and hosts.

Proactive Monitoring for PowerCenter Governance connects to the PowerCenter repository to monitor the coding violations. You can connect the Proactive Monitoring solution to the PowerCenter Repository Service through the Management console.

Proactive Monitoring for PowerCenter Management Console

The Proactive Monitoring for PowerCenter Management Console includes the Setup, Reports, Settings, and Manage Objects tab.

The following illustration shows the Proactive Monitoring for PowerCenter Management Console:

![Proactive Monitoring for PowerCenter Management Console](image)

**Setup Tab**

You can use the Setup tab to configure the Informatica domain to monitor. You can provide details about the hosts, nodes, and the application services of the domain in the Setup tab.

**Reports Tab**

You can use the Reports tab to monitor the Repository Services, Integration Services, and hosts within a single Informatica domain. You can also analyze alerts and drill down into the current and historical alerts.
Settings Tab
You can use the Settings tab to configure the default global settings to receive alerts and the default alert recipients. You can also configure the source timestamp for each workflow from its startup time.

Manage Objects Tab
You can use the Manage Objects tab to manage the list of PowerCenter folders, topics, rules, watchlists, and sources that you use to monitor PowerCenter.

Logging In to the Proactive Monitoring for PowerCenter Management Console
To log in to the Proactive Monitoring for PowerCenter Management Console, you must have a RulePoint administrator account.

1. Open Microsoft Internet Explorer, Mozilla Firefox, or Chrome.
2. In the address field, enter the following URL for the Informatica Proactive Monitoring login page:
   http://<host>:<port>/pmpc
   Replace <host> with the host name or IP address of the server where you install the Proactive Monitoring solution. Replace <port> with the HTTP port number of the Apache Tomcat server. Default is 8080.
   If you configure the Apache Tomcat server with SSL, enter the following URL for the Informatica Proactive Monitoring login page:
   https://<host>:<port>/pmpc
   The Informatica Proactive Monitoring login page appears.
3. Enter the user name and password.
   Use the RulePoint default user name and password credentials, Administrator/Administrator1.
4. Click Log In.

Setup Configuration
You can use the Proactive Monitoring for PowerCenter Management Console to provide details about the hosts, nodes, and the application services that you want to monitor in the Informatica domain.

1. In the navigator, select the type of object that you want to add to the Management Console.
2. From the Actions menu, click New.
   You can edit and delete an existing configuration.
3. Configure the object properties.
Steps to configure the Proactive Monitoring solution to monitor the Informatica domain

1. Provide details of hosts that you want to monitor.
   See "Host Properties" on page 78.
2. Provide details of nodes that you want to monitor.
   See "Node Properties" on page 79.
3. Provide details of PowerCenter Repository Services that you want to monitor.
   See "Monitoring a PowerCenter Repository Service" on page 79.
   See "Global Settings Parameters" on page 80.
5. Configure alert recipients.
   See "Alert Recipients Parameters" on page 81.
6. Configure source timestamps.
   See "Source Timestamp Configuration" on page 83.

Host Properties

The following table describes the host properties that you need to enter:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Host name of the machine that you want to monitor. The host name must be the same that you specify when you define a PowerCenter node.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the host. The description cannot exceed 200 characters.</td>
</tr>
<tr>
<td>Top CPU stats</td>
<td>Number of the highest CPU consumers that you want to record from the host.</td>
</tr>
<tr>
<td></td>
<td>Use this property for Proactive Monitoring for PowerCenter Operations. Retain the default value for Proactive Monitoring for PowerCenter Governance.</td>
</tr>
<tr>
<td>Top Memory stats</td>
<td>Number of the highest memory consumers that you want to record from the host.</td>
</tr>
<tr>
<td></td>
<td>Use this property for Proactive Monitoring for PowerCenter Operations. Retain the default value for Proactive Monitoring for PowerCenter Governance.</td>
</tr>
<tr>
<td>Frequency</td>
<td>The time interval at which the node agent collects the memory and CPU statistics from the host.</td>
</tr>
<tr>
<td></td>
<td>Use this property for Proactive Monitoring for PowerCenter Operations. Retain the default value for Proactive Monitoring for PowerCenter Governance.</td>
</tr>
<tr>
<td>Processes</td>
<td>List of specified process names that you want to monitor. Enter the process names separated by comma.</td>
</tr>
<tr>
<td></td>
<td>You can monitor any process running in the host. For example, you can monitor PowerCenter processes, such as pmdtm, pmrepagent, or pmserver.</td>
</tr>
<tr>
<td></td>
<td>Use this property for Proactive Monitoring for PowerCenter Operations. Retain the default value for Proactive Monitoring for PowerCenter Governance.</td>
</tr>
</tbody>
</table>
**Node Properties**

The following table describes the node properties that you need to enter:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the node associated with the host.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the node. The description cannot exceed 200 characters.</td>
</tr>
<tr>
<td>Host</td>
<td>Host name of the node.</td>
</tr>
</tbody>
</table>

**Monitoring a PowerCenter Repository Service**

You can use the Proactive Monitoring for PowerCenter Management Console to provide details of the PowerCenter Repository Service that you want to monitor.

The following table describes the PowerCenter Repository Service properties that you need to enter:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Monitor Option | You can choose from the following options:  
  - Operations. You want to monitor the run-time environment.  
  - Governance. You want to monitor the design-time environment.  
  - Both. You want to monitor the run-time and design-time environments.  
| Name         | Name of the PowerCenter Repository Service. |
| Description  | Description of the PowerCenter Repository Service. The description cannot exceed 200 characters. |
| Deploy Type  | You can choose one of the following options:  
  - Standalone. You want to monitor the PowerCenter Repository Service that runs on a single node.  
  - High Availability. You want to monitor the PowerCenter Integration Service that runs on primary and backup nodes configured for high availability. |
| Primary Node | The primary node on which the PowerCenter Repository Service runs on. |
| Backup Node  | The backup nodes configured for the PowerCenter Repository Service in a highly available domain. |
| Connection URL | The DataDirect JDBC connection string used to connect to the repository database.  
  The following list shows the sample connection string for the databases:  
  - Oracle. oracle.database.url=jdbc:informatica:oracle://<host>:<port>;databaseName=<SID>  
  - IBM DB2. db2.database.url=jdbc:informatica:db2://<host>:<port>;databaseName=<SID>  
  - Microsoft SQL Server. mssql.database.url=jdbc:informatica:sqlservlet://<host>:<port>;databaseName=<SID>  
  **Note:** The connection URL validates the database connectivity while saving the configuration. Provide valid connection information to save the PowerCenter Repository Service configuration. |

---

Node Properties  79
**Property** | **Description** |
---|---
Read-Only User Name | Database user name with read-only permissions to access PowerCenter repository. You create the PowerCenter read-only user with the required privileges as part of the post-installation tasks. The scripts and instructions are located at `<PROACTIVE_MONITORING_HOME>\Solutions\PMP\dls\powercenter\<database>`. |
Read-Only Password | Password for the PowerCenter read-only user. |
State | Option to enable or disable monitoring of the PowerCenter Repository Service. You can choose one of the following options:  
- Enabled. You want to monitor the PowerCenter Repository Service and receive alerts.  
- Disabled. You do not want to monitor the PowerCenter Repository Service. |

**Settings Configuration**

You can use the Proactive Monitoring for PowerCenter Management Console to configure the global settings, alert recipients, and the source timestamp parameters.

1. In the navigator, select the type of object that you want to configure in the Management Console.
2. From the **Actions** menu, click **New** or **Edit**.  
   You can edit the global settings and the source timestamp configurations. You can add, edit, and delete the alert recipients configurations.
3. Provide details of the object properties.

**Global Settings Parameters**

You can change the default response delivery method for alerts. Use the **Global Settings** option in the Management Console to change the global settings for response delivery, configure the notification framework and shadow table framework.

Every template and advanced rule in the Proactive Monitoring solution that is responsible for sending alerts uses a single response, PowerCenter Notification Response. The predefined response uses Real-Time Alert Manager alerts as the default delivery mechanism.

The Proactive Monitoring for PowerCenter Management Console contains the default values of the global setting parameters. You can edit the parameters based on the requirements.
The following table lists the attributes that you can configure using the Global Settings option:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Disturb</td>
<td>Settings to temporarily stop alerts. For example, set this value to Yes if the monitored PowerCenter instance is down for maintenance. Proactive Monitoring does not send out alerts during the maintenance period. After the maintenance is over, you can reset the value to No. Default is No.</td>
</tr>
<tr>
<td>Alert Purge Frequency</td>
<td>Alert history purge duration specifies the time to retain alert history. The Proactive Monitoring solution database tables contains the alert history. These tables grow with time, and it is a good practice to archive and purge these tables. This attribute specifies the time, in days, to retain the history. All alerts older than this time are archived and purged. Default is 60 days.</td>
</tr>
<tr>
<td>Default Notification</td>
<td>Default notification method. You can set the default notification method to RTAM or email, or both. Default is RTAM.</td>
</tr>
<tr>
<td>Alert Hyperlink</td>
<td>Alert hyperlink URL included in each Real-Time Alert Manager alert or email alert that the Proactive Monitoring solution sends. You can set this URL to an intranet web page, email ID, or a distribution list. The Proactive Monitoring solution includes a default hyperlink with every notification that points to a landing page. This landing page contains information about the PowerCenter Monitoring project of the organization with contact information. Default is <a href="https://community.informatica.com/solutions/1514">https://community.informatica.com/solutions/1514</a>.</td>
</tr>
<tr>
<td>Workflows and Sessions</td>
<td>Sets the number of records to persist in the shadow table. The number of records persisted is twice the number of the value entered for this attribute. For example, if the number of workflows and sessions persisted is five, the Proactive Monitoring solution retains the last 10 records in the shadow tables. The shadow tables of pc_completed_workflows and pc_completed_sessions retains these last 10 records. Default is 5. Note: This setting is not applicable for Proactive Monitoring for PowerCenter Governance.</td>
</tr>
</tbody>
</table>

**Alert Recipients Parameters**

You can use the Alert Recipients option of the Proactive Monitoring for PowerCenter Management Console to configure the default alert recipients.

When an event occurs, the alert recipients get alerts through email, Real-Time Alert Manager, or both. The alert recipients get the alerts based on the value specified in the default notification global setting.
The following table lists the attributes that you can configure for the Alert Recipients:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Domain name of the PowerCenter Repository Service.</td>
</tr>
<tr>
<td>Repository Service</td>
<td>Name of the PowerCenter Repository Service for which you want to receive alerts. Leave it blank if you want to use the configuration for all PowerCenter Repository Services in the domain.</td>
</tr>
<tr>
<td>Folder</td>
<td>Name of the folder for which you want to receive alerts. Leave it blank if you want to use the configuration for all the folders of the PowerCenter repository. The configuration for the folder name will not be used if the PowerCenter Repository Service name is blank.</td>
</tr>
<tr>
<td>Workflow</td>
<td>Name of the workflow for which you want to receive alerts. Leave it blank if you want to use the configuration for all the workflows of the PowerCenter Repository Service. The configuration for the folder name will not be used if the Repository Service name or the Folder name is blank.</td>
</tr>
<tr>
<td>pcmonitor RTAM List</td>
<td>Real-Time Alert Manager IDs of the users that you want to associate with the pcmonitor persona. Enter the IDs separated by semicolon.</td>
</tr>
<tr>
<td>pcmonitor Email List</td>
<td>Email IDs of the users that you want to associate with pcmonitor persona list. Enter the IDs separated by comma.</td>
</tr>
<tr>
<td>pcadmin RTAM List</td>
<td>Real-Time Alert Manager IDs of the users that you want to associate with pcadmin persona list. Enter the IDs separated by semicolon.</td>
</tr>
<tr>
<td>pcadmin Email List</td>
<td>Email IDs of the users that you want to associate with pcadmin persona list. Enter the IDs separated by comma.</td>
</tr>
<tr>
<td>apparchitect RTAM List</td>
<td>Real-Time Alert Manager IDs of the users that you want to associate with apparchitect persona list. Enter the IDs separated by semicolon.</td>
</tr>
<tr>
<td>apparchitect Email List</td>
<td>Email IDs of the users that you want to associate with apparchitect persona list. Enter the IDs separated by comma. To configure email alert recipients, update the email connection information in RulePoint.</td>
</tr>
<tr>
<td>dataarchitect RTAM List</td>
<td>Real-Time Alert Manager IDs of the users that you want to associate with dataarchitect persona list. Enter the IDs separated by semicolon.</td>
</tr>
<tr>
<td>dataarchitect Email List</td>
<td>Email IDs of the users that you want to associate with dataarchitect persona list. Enter the IDs separated by comma.</td>
</tr>
<tr>
<td>itsecurity RTAM List</td>
<td>Real-Time Alert Manager IDs of the users that you want to associate with itsecurity persona list. Enter the IDs separated by semicolon.</td>
</tr>
<tr>
<td>itsecurity Email List</td>
<td>Email IDs of the users that you want to associate with itsecurity persona list. Enter the IDs separated by comma.</td>
</tr>
</tbody>
</table>

**Note:** The Management Console does not validate the configuration information provided for alert recipients. Provide valid values for every field before you save the configuration.

After you save the alert recipient configuration, you cannot change the values in the Repository Service, Folder, and Workflow fields. You can change the email and RTAM values. To change the values for Repository Service, Folder, or Workflow, you must delete the existing alert recipient configuration and create again.
Source Timestamp Configuration

The Proactive Monitoring installer updates the value of the tstamp parameter for source services to that of the system time. You can leave this value as it is, the monitoring of the PowerCenter objects will start from the time defined in the tstamp parameter. The PMPC SQL source service updates the tstamp each time the service runs.

You can update the tstamp parameter to have the PMPC SQL Source fetch older events. The tstamp parameter value must not be too old or a future value. If you set the tstamp to a past time that is too old, you might receive unwanted alerts. If you set the tstamp to a future time, you will not receive any alerts.

The installer updates the following services with the tstamp value:
- PowerCenter Command Tasks
- PowerCenter Mappings Modified Incremental
- PowerCenter Mapplets Modified Incremental
- PowerCenter Sessions Modified Incremental
- PowerCenter Transforms Modified Incremental
- PowerCenter Workflows Modified Incremental
- PowerCenter Worklets Modified Incremental

Configuring Source Timestamp

You can use the Proactive Monitoring for PowerCenter Management Console to change the source timestamp.

1. On the **Settings** tab, click **Source Timestamp**.
2. Select a source for an appropriate repository service.
3. From the **Actions** menu, click **Edit**.
   The **Source Timestamp Configuration** page appears.
4. Enter the timestamp parameter values for the source.
   Do not change default time format.
5. Click **Save**.

Adding or Removing Folders to the Watchlist for Monitoring

Watchlists contains the items that you store as a single object with a unique name that you define. You can reference this name in a rule so that it can use the data stored in the object.

Watchlists are useful because you can change the items within the watchlist at any time, and any rule referencing that watchlist automatically uses those new items. Start modifying a small watchlist, and progressively add to it after you have a good understanding of the solution and the various configuration options.
PowerCenter monitored folders is a predefined watchlist that is available in the Proactive Monitoring solution. You can manage the monitored folders from the Manage Objects tab in the Proactive Monitoring for PowerCenter Management Console.

1. In the Proactive Monitoring for PowerCenter Management Console, click the Manage Objects view.
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, select Add/Remove from the Actions menu.
   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 will take a few minutes to update.
8. Click OK.
   A message appears that indicates that the runtime is successfully updated.
Troubleshooting the Proactive Monitoring Installation

This chapter includes the following topic:

- Troubleshooting Real-Time Alert Manager to Receive Alerts, 85

Troubleshooting Real-Time Alert Manager to Receive Alerts

Alerts do not show up in the Real-Time Alert Manager dashboard even when you start all the services after installation.

1. Log in to Real-Time Alert Manager as each of the five users.
   The following table provides the user names and passwords for the five users:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>pcmonitor</td>
<td>pcmonitor123</td>
</tr>
<tr>
<td>pcadmin</td>
<td>pcadmin123</td>
</tr>
<tr>
<td>apparchitect</td>
<td>apparchitect123</td>
</tr>
<tr>
<td>dataarchitect</td>
<td>dataarchitect123</td>
</tr>
<tr>
<td>itsecurity</td>
<td>itsecurity123</td>
</tr>
</tbody>
</table>

2. Check the Proactive Monitoring for PowerCenter Management Console for the correct details of Informatica domain, PowerCenter repository service, personas, email, and Real-Time Alert Manager users.

3. Check the global settings for the Proactive Monitoring user through the Proactive Monitoring for PowerCenter Management Console. Ensure that the default entries for Real-Time Alert Manager are available.

4. Ensure that you update the monitored folders and check whether the source services are deployed.

5. Ensure that all the responders are deployed.
6. Check the pc_notification events created under Monitored Events in the Manage Objects tab of the Proactive Monitoring for PowerCenter Management Console.

7. Ensure that you schedule and run the workflows in PowerCenter to populate data in the Reports dashboard.

8. Review the solutions.log file located at <PROACTIVE_MONITORING_HOME>/bin/logs and resolve any exceptions.
Chapter 10

Manage Objects

This chapter includes the following topics:

- Manage Objects Overview, 87
- Managing PMPC SQL Source Services, 89
- Monitored Event Management, 90
- Monitored Objects Management, 91
- Managing Templates Rules, 92

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 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.
   b. Click OK.
   - You can deploy an object that is in the Drafts state.
   - A message appears that indicates that the source is deployed successfully.
   - 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.
   b. Click OK.
   - 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.
   - 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.
   b. Click OK.
   - 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.
   - The status of the source service changes from Needs_Deployed to Deployed.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>Lists the predefined topics that are available by default after you install Proactive Monitoring for PowerCenter Operations.</td>
</tr>
<tr>
<td>Common</td>
<td>Lists the predefined topics that are common to both Operations and Governance.</td>
</tr>
<tr>
<td>Custom</td>
<td>Lists the topics that you create in RulePoint.</td>
</tr>
</tbody>
</table>

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.

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 11

Proactive Monitoring Reports

This chapter includes the following topics:

- Proactive Monitoring Reports Overview, 95
- Monitoring Application Services and Hosts in the Domain, 96
- Monitoring PowerCenter Operation Alerts, 98
- Monitoring PowerCenter Governance Alerts, 100

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:

![Reports tab in 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. You 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.
   - For more information on attribute types and values, see [Proactive Monitoring Lookup Table for Attribute Values](#).
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:

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

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the responder.</td>
</tr>
<tr>
<td>NMS Host</td>
<td>IP address of the host on which NMS is available.</td>
</tr>
<tr>
<td>NMS Port</td>
<td>Port number on which NMS will receive traps. The default value is 162.</td>
</tr>
<tr>
<td>Community String</td>
<td>Community string for SNMPv2. The default value is public.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout value for trap in milliseconds. The default value is 0.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Retry count for trap. The default value is 0.</td>
</tr>
<tr>
<td>Trap OID</td>
<td>OID of the trap.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the responder. Change the status of the responder to active to reactivate the responder.</td>
</tr>
</tbody>
</table>

**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 13

Proactive Monitoring Watchlists

This chapter includes the following topic:
- Proactive Monitoring Watchlists, 107

Proactive Monitoring Watchlists

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

<table>
<thead>
<tr>
<th>Watchlists Name</th>
<th>Description</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerCenter Workflow Attributes</td>
<td>The list of PowerCenter workflow attributes. This watchlist is referenced in the template, PC_GWT2 Compare workflow attributes.</td>
<td>Draft</td>
</tr>
<tr>
<td>PowerCenter Transformation Attributes</td>
<td>The list of PowerCenter transformation attributes. This watchlist is referenced in the template, PC_GTT1 Compare transformation attributes.</td>
<td>Draft</td>
</tr>
<tr>
<td>PowerCenter Monitored Folders</td>
<td>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.</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Session Attributes</td>
<td>The list of PowerCenter session attributes. This watchlist is referenced in the template, PC_GST1 Compare session attributes.</td>
<td>Draft</td>
</tr>
<tr>
<td>Watchlists Name</td>
<td>Description</td>
<td>State</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>PowerCenter Default Transformation Names</td>
<td>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.</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter CLI commands Watchlists</td>
<td>The list of CLI commands which should not be used in PowerCenter tasks of type Command.</td>
<td>Deployed</td>
</tr>
</tbody>
</table>

Chapter 13: Proactive Monitoring Watchlists
This chapter includes the following topic:

- **Proactive Monitoring Topics, 109**

## Proactive Monitoring Topics

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

<table>
<thead>
<tr>
<th>Topic Name</th>
<th>Description</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>pc_notifications</td>
<td>This topic contains event properties associated with the proactive monitoring notification framework.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_alert_history_purge_request</td>
<td>This topic contains event properties associated with the alert history purge request. Source: PowerCenter Daily Alert History Purge Requestor</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_pmpc_global_settings</td>
<td>This topic contains event properties associated with global settings framework. Source: PowerCenter Load PMPC Global Settings from Database</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_sessions</td>
<td>This topic contains event properties associated with PowerCenter sessions. Source: PowerCenter Sessions Modified Incremental</td>
<td>Deployed</td>
</tr>
<tr>
<td>Topic Name</td>
<td>Description</td>
<td>State</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>pc_mapplets</td>
<td>This topic contains event properties associated with PowerCenter mapplets.</td>
<td>Deployed</td>
</tr>
<tr>
<td></td>
<td>Source: PowerCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mapplets Modified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incremental</td>
<td></td>
</tr>
<tr>
<td>pc_worklets</td>
<td>This topic contains event properties associated with the PowerCenter worklets.</td>
<td>Deployed</td>
</tr>
<tr>
<td></td>
<td>Source: PowerCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Worklets Modified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incremental</td>
<td></td>
</tr>
<tr>
<td>pc_transforms</td>
<td>This topic contains event properties associated with PowerCenter transformations.</td>
<td>Deployed</td>
</tr>
<tr>
<td></td>
<td>Source: PowerCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transforms Modified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incremental</td>
<td></td>
</tr>
<tr>
<td>pc_mappings</td>
<td>This topic contains event properties associated with PowerCenter mappings.</td>
<td>Deployed</td>
</tr>
<tr>
<td></td>
<td>Source: PowerCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mappings Modified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incremental</td>
<td></td>
</tr>
<tr>
<td>pc_workflows</td>
<td>This topic contains event properties associated with the PowerCenter workflows.</td>
<td>Deployed</td>
</tr>
<tr>
<td></td>
<td>Source: PowerCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workflows Modified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incremental</td>
<td></td>
</tr>
<tr>
<td>pc_command_tasks</td>
<td>This topic contains event properties associated with Command task type used in PowerCenter workflows.</td>
<td>Deployed</td>
</tr>
<tr>
<td></td>
<td>Source: PowerCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Command Tasks</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 15

Proactive Monitoring Services

This chapter includes the following topics:

- **Sources**, 111
- **Analytics**, 113
- **Responders**, 115

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:

<table>
<thead>
<tr>
<th>Source Service Name</th>
<th>Description</th>
<th>Properties</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerCenter Command Tasks</td>
<td>Retrieve the details of <em>Command</em> task type used in PowerCenter workflows.</td>
<td>- Type: PMPC SQL Source&lt;br&gt;- Topic: pc_command_tasks&lt;br&gt;- Connected to: PowerCenter Repository (pcrs_readonly)&lt;br&gt;- Default interval: 21600 seconds</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Daily Alert History Purge Requestor</td>
<td>Retrieve alert history purge frequency from the global settings framework. The frequency is used for purging the alert history.</td>
<td>- Type: SQL&lt;br&gt;- Topic: pc_alert_history_purge_request&lt;br&gt;- Connected to: Rulepoint Repository (pc_rp)&lt;br&gt;- Default interval: Daily</td>
<td>Deployed</td>
</tr>
<tr>
<td>Source Service Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 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 |
| 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 |
<table>
<thead>
<tr>
<th>Source Service Name</th>
<th>Description</th>
<th>Properties</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerCenter Workflows Modified Incremental</td>
<td>Retrieve the details of PowerCenter workflows modified since the last run.</td>
<td>- Type: PMPC SQL Source&lt;br&gt;- Topic: pc_workflows&lt;br&gt;- Connected to: PowerCenter Repository (pcrs_readonly)&lt;br&gt;- Default interval: 21600 seconds</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Worklets Modified Incremental</td>
<td>Retrieve the details of PowerCenter worklets modified since the last run.</td>
<td>- Type: PMPC SQL Source&lt;br&gt;- Topic: pc_worklets&lt;br&gt;- Connected to: PowerCenter Repository (pcrs_readonly)&lt;br&gt;- Default interval: 21600 seconds</td>
<td>Deployed</td>
</tr>
</tbody>
</table>

## 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Connects to...</th>
<th>Analytic Type</th>
<th>Description</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>pc_get_alert_history_csv</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>Obtain alert history for the previous N days for reporting purposes.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_alert_history_purge_count</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>Obtain the count of alert history records to be purged.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_email</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>Obtain the email address for a specified recipient of an alert.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_rtam</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>Obtain the Real-Time Alert Manager target for a specified recipient of an alert.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_global_setting</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>Obtain value from the global settings framework for a specified attribute name.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_purge_cutoff_date</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>Obtain the text string for the cutoff date. The cutoff date will be specified in the alerts.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_recent_alert</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>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.</td>
<td>Deployed</td>
</tr>
<tr>
<td>Name</td>
<td>Connects to...</td>
<td>Analytic Type</td>
<td>Description</td>
<td>State</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>pc_is_mapping_duplicate</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the duplicates of a specified mapping in all other folders.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_is_session_duplicate</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the duplicates of a specified session in all other folders.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_is_workflow_duplicate</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the duplicates of a specified workflow in all other folders.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_session_details_for_mapping</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain PowerCenter session details corresponding to the specified mapping.</td>
<td>Draft</td>
</tr>
<tr>
<td>pc_get_session_attribute</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the value for a specified session attribute name.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_session_attribute_count</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain count for a specified session attribute name and value.</td>
<td>Draft</td>
</tr>
<tr>
<td>pc_get_workflow_attribute</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the workflow attribute for a specified workflow.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_workflow_attribute_count</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the number of workflows for a specified attribute value.</td>
<td>Draft</td>
</tr>
<tr>
<td>pc_get_transform_attribute</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the value for a specified transformation attribute.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_transform_attribute_count</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the number of transformations for a specified attribute value.</td>
<td>Draft</td>
</tr>
<tr>
<td>pc_get_session_mapping_attribute</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the mapping attributes for a specified session.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_get_task_parent_failure_options</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Obtain the value of failed parent task option for a specified session.</td>
<td>Deployed</td>
</tr>
<tr>
<td>pc_is_session_on_test_load</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Check if a session has the Enable Test Load attribute set.</td>
<td>Draft</td>
</tr>
<tr>
<td>rs_formatter</td>
<td>RulePoint Repository</td>
<td>SQL</td>
<td>This formats the rs value in the notification response.</td>
<td>Deployed</td>
</tr>
<tr>
<td>Name</td>
<td>Connects to...</td>
<td>Analytic Type</td>
<td>Description</td>
<td>State</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>get_mapping_ports</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Return all the transformation ports that do not meet the port naming criteria within a mapping.</td>
<td>Draft</td>
</tr>
<tr>
<td>get_session_hardcoded_paths</td>
<td>PowerCenter Repository</td>
<td>PMPC SQL Analytic</td>
<td>Return all hardcoded paths configured for sources and targets within a session.</td>
<td>Draft</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Responder Service Name</th>
<th>Description</th>
<th>Properties</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerCenter Alert History Purge Responder</td>
<td>Responds to events by purging alert history older than the specified number of days.</td>
<td>- Type: SQL Responder - Topic: - - Connected to: Rulepoint Repository (pc_rp)</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Alert Recorder</td>
<td>The alert recorder stores details of alerts in the RulePoint database.</td>
<td>- Type: SQL Responder - Topic: - - Connected to: Rulepoint Repository (pc_rp)</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Email Responder</td>
<td>Responds to events by sending email alerts.</td>
<td>- Type: Email - Topic: - - Connected to: Email server</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Notification Responder</td>
<td>Responds to events by transforming them as notification events.</td>
<td>- Type: Event Transformer - Topic: pc_notifications - Connected to: -</td>
<td>Deployed</td>
</tr>
<tr>
<td>Responder Service Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| 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 16

Proactive Monitoring Templates and Rules

This chapter includes the following topics:

- Proactive Monitoring Templates, 118
**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.

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

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Properties</th>
<th>Template Parameters</th>
<th>State</th>
</tr>
</thead>
</table>
| PC_GST1                     | Notify if the session attribute contains a specified value. | - Topic: pc_sessions  
- Analytics: pc_get_session_attribute  
- Source: PowerCenter Sessions Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | - <<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). | Draft  |
| PC_GST2                     | Notify if the session name does not start with the specified prefix. | - Topic: pc_sessions  
- Analytics: -  
- Source: PowerCenter Sessions Modified Incremental  
- Notification: PowerCenter Notification Response  
- Persona: apparchitect | <<prefix>> Check prefix for naming convention of session. | Draft  |
<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Properties</th>
<th>Template Parameters</th>
<th>State</th>
</tr>
</thead>
</table>
| 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. | - Topic: pc_sessions  
- Analytics: -  
- Source: PowerCenter Sessions Modified Incremental  
- Notification: PowerCenter Notification Response  
- Persona: apparchitect | - <<p_times>>  
Number of times a session is modified.  
- <<p_minutes>>  
Time range within which the session is modified the specified number of times. | Draft |
| PC_GMT1 Naming Convention Violation for Mapping Name prefix | Notify if the mapping name does not start with the specified prefix. | - Topic: pc_mappings  
- Analytics: -  
- Source: PowerCenter Mappings Modified Incremental  
- Notification: PowerCenter Notification Response  
- Persona: apparchitect | <<prefix>>  
Check prefix for naming convention of mapping. | Draft |
| 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. | - Topic: pc_mappings  
- Analytics: -  
- Source: PowerCenter Mappings Modified Incremental  
- Notification: PowerCenter Notification Response  
- Persona: apparchitect | - <<p_times>>  
Number of times the mapping is modified.  
- <<p_minutes>>  
Time range within which the mapping is modified the specified number of times. | Draft |
<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Properties</th>
<th>Template Parameters</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC_GTT1</td>
<td>Compare transformation attributes</td>
<td>- Topic: pc_transforms&lt;br&gt;- Analytics: pc_get_transform_attribute&lt;br&gt;- Source: PowerCenter Transforms Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>- &lt;&lt;transform_attribute&gt;&gt;&lt;br&gt;Select the transformation attribute from the drop down menu.&lt;br&gt;- &lt;&lt;operator&gt;&gt;&lt;br&gt;Enter comparison operator.&lt;br&gt;- &lt;&lt;attr_value&gt;&gt;&lt;br&gt;Enter the attribute value.&lt;br&gt;- &lt;&lt;alert_cause&gt;&gt;&lt;br&gt;Enter text to explain the cause of the alert.&lt;br&gt;- &lt;&lt;priority&gt;&gt;&lt;br&gt;Select a priority level (0=Least critical to 5=Most Critical).</td>
<td>Draft</td>
</tr>
<tr>
<td>PC_GWT1</td>
<td>Naming Convention Violation for Workflow Name prefix</td>
<td>- Topic: pc_workflows&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Workflows Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>&lt;&lt;prefix&gt;&gt;&lt;br&gt;Check prefix for naming convention of mapping.</td>
<td>Draft</td>
</tr>
<tr>
<td><strong>Template Name</strong></td>
<td><strong>Description</strong></td>
<td><strong>Properties</strong></td>
<td><strong>Template Parameters</strong></td>
<td><strong>State</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>----------------</td>
<td>-------------------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| PC_GWT2          | Compare workflow attributes | Notify if the workflow attribute contains a specified value. | - Topic: pc_workflows  
- Analytics: pc_get_workflow_attribute  
- Source: PowerCenter Workflows Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | - <<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). | Draft |
| PC_GWT3          | Windows pathname is hardcoded with a drive letter | Notify if the command tasks contains the specified drive letter, such as "C:". | - Topic: pc_command_tasks  
- Analytics: -  
- Source: PowerCenter Command Tasks  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | <<drive>> Check for the drive letter in the command tasks. | Draft |
| PC_GWT5          | Naming Convention Violation for Workflow Name suffix | Notify if the workflow name does not end with the specified suffix. | - Topic: pc_workflows  
- Analytics: -  
- Source: PowerCenter Workflows Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | <<suffix>> Check suffix for naming convention of workflow. | Draft |
<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Properties</th>
<th>Template Parameters</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC_GWKT2</td>
<td>Notify if the worklet name does not end with the specified suffix.</td>
<td>- Topic: pc_worklets - Analytics: - - Source: PowerCenter Worklets Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>&lt;&lt;suffix&gt;&gt; Check suffix for naming convention of worklet.</td>
<td>Draft</td>
</tr>
<tr>
<td>PC_GST5</td>
<td>Notify if the session name does not end with the specified suffix.</td>
<td>- Topic: pc_sessions - Analytics: - - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>&lt;&lt;suffix&gt;&gt; Check suffix for naming convention of session.</td>
<td>Draft</td>
</tr>
<tr>
<td>PC_GMT4</td>
<td>Notify if the mapping name does not end with the specified suffix.</td>
<td>- Topic: pc_mappings - Analytics: - - Source: PowerCenter Mappings Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>&lt;&lt;suffix&gt;&gt; Check suffix for naming convention of mapping.</td>
<td>Draft</td>
</tr>
<tr>
<td>PC_GMPT2</td>
<td>Notify if the mapplet name does not end with the specified suffix.</td>
<td>- Topic: pc_mapplets - Analytics: - - Source: PowerCenter Mapplets Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>&lt;&lt;suffix&gt;&gt; Check suffix for naming convention of mapplet.</td>
<td>Draft</td>
</tr>
<tr>
<td>Template Name</td>
<td>Description</td>
<td>Properties</td>
<td>Template Parameters</td>
<td>State</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| PC_GMT5 Naming Convention Violation for Mapping Transformation Port prefix | Notify if transformation ports in a mapping do not start with the specified prefix. | - Topic: pc_mappings  
- Analytics: get_mapping_ports  
- Source: PowerCenter Mappings Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | <<prefix>> Check prefix for naming convention of the mapping transformation port. | Draft  |
| PC_GTT2 Naming Convention Violation for Transformation Name prefix | Notify if transformation name does not start with the specified prefix. | - Topic: pc_transforms  
- Analytics: -  
- Source: PowerCenter Transforms Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | <<prefix>> Check prefix for naming convention of transformation name. | Draft  |
## Template Rules

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

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

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>Properties</th>
<th>State</th>
</tr>
</thead>
</table>
| PC_GM5 Mapping name should begin with m_ | Notify if the mapping name does not begin with m_. | - Topic: pc_mappings  
- Analytics: -  
- Source: PowerCenter Mappings Modified Incremental  
- Notification: PowerCenter Notification Response  
- Persona: apparchitect | Deployed |
| 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. | - Topic: pc_mappings  
- Analytics: -  
- Source: PowerCenter Mappings Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | Deployed |
| PC_GS3 Session name should begin with s_ | Notify if the session name does not begin with s_. | - Topic: pc_sessions  
- Analytics: -  
- Source: PowerCenter Sessions Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | Deployed |
| 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. | - Topic: pc_sessions  
- Analytics: pc_get_session_attribute  
- Source: PowerCenter Sessions Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | Deployed |
| 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. | - Topic: pc_sessions  
- Analytics: -  
- Source: PowerCenter Sessions Modified Incremental  
- Response: PowerCenter Notification Response  
- Persona: apparchitect | Deployed |
<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>Properties</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC_GS12 Check whether save session log for these runs uses the global variable PMSessionLogCount</td>
<td>Notify if <code>Save session log for these runs</code> attribute does not use the global variable <code>$PMSessionLogCount</code>.</td>
<td>- Topic: pc_sessions - Analytics: pc_get_session_attrib - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS13 Check whether stop on errors uses the global variable PMSessionErrorThreshold</td>
<td>Notify if <code>Stop on errors</code> attribute does not use the global variable <code>$PMSessionErrorThreshold</code>.</td>
<td>- Topic: pc_workflows - Analytics: pc_get_session_attribute - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS14 Check whether write backward compatible session log file is set</td>
<td>Notify whether a session does not have <code>Write Backward Compatible Session Log File</code> set.</td>
<td>- Topic: pc_sessions - Analytics: pc_get_session_attribute - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS16 Check for session where commit interval exceeds 1000 seconds</td>
<td>Notify if <code>Commit Interval</code> greater than equal to 1000 seconds for a session.</td>
<td>- Topic: pc_sessions - Analytics: pc_get_task_parent_failure_options - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GT3 Check for transformations with lookup SQL override</td>
<td>Notify if the <code>Lookup SQL Override</code> for a transformation is not <code>NULL</code>.</td>
<td>- Topic: pc_transforms - Analytics: - - Source: PowerCenter Transforms Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>PC_GT4 Check for transformations with source SQL override</td>
<td>Notify if SQL Query for a transformation is not NULL.</td>
<td>- Topic: pc_transforms - Analytics: - - Source: PowerCenter Transforms Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GT5 Check for transformations with tracing level higher than terse</td>
<td>Notify if a transformation has Tracing Level higher than terse.</td>
<td>- Topic: pc_transforms - Analytics: pc_get_transform_attribute - Source: PowerCenter Transforms Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GT7 Check if sequence generator reset option is set</td>
<td>Notify if the sequence generator Reset option is set.</td>
<td>- Topic: pc_transforms - Analytics: pc_get_transform_attribute - Source: PowerCenter Transforms Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW3 Workflow name should begin with wf_</td>
<td>Notify if a workflow name does not begin with wf_.</td>
<td>- Topic: pc_workflows - Analytics: - - Source: PowerCenter Workflows Incremental - Notification: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW6 Check whether save workflow log for these runs used the global variable PMWorkflowLogCount</td>
<td>Notify if Save workflow log for these runs attribute does not use the global variable $PMWorkflowLogCount.</td>
<td>- Topic: pc_workflows - Analytics: pc_get_workflow_attribute - Source: PowerCenter Workflows Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>PC_GW8 Check whether backward write compatible workflow log option is set</td>
<td>Notify whether a workflow does not have <em>Write Backward Compatible Workflow Log File</em> set.</td>
<td>- Topic: pc_workflows - Analytics: pc_get_workflow_attribute - Source: PowerCenter Workflows Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW9 Check if Windows path name is hardcoded with drive letter C</td>
<td>Notify if the command task contains a hardcoded Microsoft Windows drive letter C:.</td>
<td>- Topic: pc_command_tasks - Analytics: - - Source: PowerCenter Command Tasks - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW13 Workflow Name should end with _DEV</td>
<td>Notify if the workflow name does not end with _DEV.</td>
<td>- Topic: pc_workflows - Analytics: - - Source: PowerCenter Workflows Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GWK3 Worklet Name should end with _DEV</td>
<td>Notify if the worklet name does not end with _DEV.</td>
<td>- Topic: pc_worklets - Analytics: - - Source: PowerCenter Worklets Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS20 Session Name should end with _DEV</td>
<td>Notify if the session name does not end with _DEV.</td>
<td>- Topic: pc_sessions - Analytics: - - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>PC_GM8 Mapping Name should end with _DEV</td>
<td>Notify if the mapping name does not end with _DEV.</td>
<td>- Topic: pc_mappings - Analytics: - - Source: PowerCenter Mappings Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GMP3 Mapplet Name should end with _DEV</td>
<td>Notify if the mapplet name does not end with _DEV.</td>
<td>- Topic: pc_mapplets - Analytics: - - Source: PowerCenter Mappings Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GM9 Mapping Transformation Input Port must begin with in_</td>
<td>Notify if transformation ports in a mapping do not start with the specified prefix. You need to deploy this rule to receive the notifications.</td>
<td>- Topic: pc_mappings - Analytics: - - Source: PowerCenter Mappings Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Draft</td>
</tr>
<tr>
<td>PC_GT8 Aggregator Transformation Name should start with AGG_</td>
<td>Notify if the aggregator transformation name does not start with AGG_. You need to deploy this rule to receive the notifications.</td>
<td>- Topic: pc_transforms - Analytics: - - Source: PowerCenter Transforms Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Draft</td>
</tr>
</tbody>
</table>
Advanced rules do not have parameters. You can extend these rules once you are comfortable with the functioning of these rules.

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

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>Properties</th>
<th>State</th>
</tr>
</thead>
</table>
| PC_GM1 Check for mappings without description | Notify if the description for a mapping is NULL. | - Topic: pc_mappings  
- Analytics:  
  - Source: PowerCenter Mappings Modified Incremental  
  - Notification: PowerCenter Notification Response  
  - Persona: apparchitect | Deployed |
| PC_GM2 Check for duplicate mappings           | Notify if the name of the mapping is duplicated. | - Topic: pc_mappings  
- Analytics: pc_is_mapping_duplicate  
  - Source: PowerCenter Mappings Modified Incremental  
  - Notification: PowerCenter Notification Response  
  - Persona: apparchitect | Deployed |
| PC_GM3 Check whether the mappings is not valid | Notify if a mapping is not valid. | - Topic: pc_mappings  
- Analytics:  
  - Source: PowerCenter Mappings Modified Incremental  
  - Response: PowerCenter Notification Response  
  - Persona: apparchitect | Deployed |
| PC_GM4 Check for mapping names with spaces    | Notify if the mapping name has spaces. | - Topic: pc_mappings  
- Analytics:  
  - Source: PowerCenter Mappings Modified Incremental  
  - Response: PowerCenter Notification Response  
  - Persona: apparchitect | Deployed |
<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>Properties</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC_GS1 Check whether the session is not valid</td>
<td>Notify if the session is not valid.</td>
<td>- Topic: pc_sessions - Analytics: - - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS2 Check for sessions without description</td>
<td>Notify if the description for a session is NULL.</td>
<td>- Topic: pc_sessions - Analytics: - - Source: PowerCenter Sessions Modified Incremental - Notification: PowerCenter Sessions Modified Incremental - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS4 Check for duplicate sessions</td>
<td>Notify if a session name is repeated.</td>
<td>- Topic: pc_sessions - Analytics: pc_is_session_duplicate - Source: PowerCenter Sessions Incremental - Notification: PowerCenter Sessions Modified Incremental - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS5 Check whether a sessions is not reusable</td>
<td>Notify if a session is not reusable.</td>
<td>- Topic: pc_sessions - Analytics: - - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS6 Check if session log file name is not derived from the session name</td>
<td>Notify if the session log file name does not contain the session name.</td>
<td>- Topic: pc_sessions - Analytics: pc_get_session_attribute - Source: PowerCenter Sessions Modified Incremental - Response: PowerCenter Notification Response - Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>PC_GS7 Check</td>
<td>Whether the truncate table option is set</td>
<td>- Topic: pc_sessions&lt;br&gt;- Analytic: pc_get_session_mapping_attribute&lt;br&gt;- Source: PowerCenter Sessions Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS10 Check for disabled sessions</td>
<td>Notify if a session is disabled.</td>
<td>- Topic: pc_sessions&lt;br&gt;- Analytic: pc_get_session_mapping_attribute&lt;br&gt;- Source: PowerCenter Sessions Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS11 Check for hardcoded source connection</td>
<td>Notify if the source connection value of a session does not begin with $.</td>
<td>- Topic: pc_sessions&lt;br&gt;- Analytic: pc_get_session_attribute&lt;br&gt;- Source: PowerCenter Sessions Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS15 Check</td>
<td>Whether both the parent fail options are not set</td>
<td>- Topic: pc_sessions&lt;br&gt;- Analytic: task_parent_failure_options&lt;br&gt;- Source: Sessions Modified Incremental&lt;br&gt;- Response: Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GS17 Check</td>
<td>Notify if a session has the option &quot;fail parent if this task does not run&quot; not set</td>
<td>- Topic: pc_sessions&lt;br&gt;- Analytic: pc_get_task_parent_failure_options&lt;br&gt;- Source: PowerCenter Sessions Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>PC_GS18 Check whether target connection value is empty</td>
<td>Notify if a Target connection value is empty for a session.</td>
<td>- Topic: pc_sessions&lt;br&gt;- Analytic: pc_get_session_attribute&lt;br&gt;- Source: PowerCenter Sessions Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GT1 Check for transformations without description</td>
<td>Notify if the description for a transformation is NULL.</td>
<td>- Topic: pc_transforms&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Transforms Modified Incremental&lt;br&gt;- Notification: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GT2 Check for transformations with default names</td>
<td>Notify if the transformation are saved with default names.</td>
<td>- Topic: pc_transforms&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Transforms Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GT6 Check whether connection information option is set</td>
<td>Notify if the Connection Information option is not set.</td>
<td>- Topic: pc_transforms&lt;br&gt;- Analytics: pc_get_transform_attribute&lt;br&gt;- Source: PowerCenter Transforms Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GMP2 Check whether the mapplet is not valid</td>
<td>Notify if a mapplet is not valid.</td>
<td>- Topic: pc_mapplets&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Mapplets Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PC_GWK2 Check</td>
<td>Notify if a worklet is not valid.</td>
<td>- Topic: pc_worklets&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Worklets Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW1 Check for workflows without description</td>
<td>Notify if the description for a workflow is NULL.</td>
<td>- Topic: pc_workflows&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Mappings Modified Incremental&lt;br&gt;- Notification: PowerCenter Sessions Modified Incremental&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW2 Check for duplicate workflows</td>
<td>Notify if a workflow name is repeated.</td>
<td>- Topic: pc_workflows&lt;br&gt;- Analytics: pc_is_workflow_duplicate&lt;br&gt;- Source: PowerCenter Workflows Incremental&lt;br&gt;- Notification: PowerCenter Sessions Modified Incremental&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW4 Check for workflows that are not valid</td>
<td>Notify if the workflow is not valid.</td>
<td>- Topic: pc_workflows&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Workflows Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW5 Check if the workflow is a web service</td>
<td>Notify if the workflow is a web service.</td>
<td>- Topic: pc_workflows&lt;br&gt;- Analytic: -&lt;br&gt;- Source: PowerCenter Mappings Modified Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PC_GW7 Check if workflow log file name is not derived from workflow name</td>
<td>Notify if the Workflow Log File name does not contain the workflow name.</td>
<td>- Topic: pc_workflows&lt;br&gt;- Analytics: pc_get_workflow_attribute&lt;br&gt;- Source: PowerCenter Workflows Incremental&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW10 Check for hardcoded UNIX path</td>
<td>Notify if the command tasks contain hardcoded UNIX path names.</td>
<td>- Topic: pc_command_tasks&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Command Tasks&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_GW11 Check for illegal command tasks</td>
<td>Notify if the workflow contains illegal command tasks listed in the PowerCenter CLI command watchlist.</td>
<td>- Topic: pc_command_tasks&lt;br&gt;- Analytics: -&lt;br&gt;- Source: PowerCenter Command Tasks&lt;br&gt;- Response: PowerCenter Notification Response&lt;br&gt;- Persona: apparchitect</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_S1 RTAM Notification</td>
<td>Generate Real-Time Alert Manager notification.</td>
<td>Do not edit. For internal use.</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_S2 Email Notification</td>
<td>Generate email notification.</td>
<td>Do not edit. For internal use.</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_S3 Daily alert history report</td>
<td>Send a daily report of the alert history.</td>
<td>- Topic: pc_alert_history_purge_request&lt;br&gt;- Analytics: pc_get_alert_history_csv&lt;br&gt;pc_get_purge_cutoff_date&lt;br&gt;- Source: PowerCenter Daily Alert History Purge Requestor&lt;br&gt;- Response: PowerCenter Real-Time Alert Manager Alert&lt;br&gt;- Persona: pcmonitor</td>
<td>Deployed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>PC_S4 Zero records purged from alert history</td>
<td>Send a daily report when zero records are purged.</td>
<td>- Topic: pc_alert_history_purge_request&lt;br&gt;- Analytics: pc_get_alert_history_purge_count, pc_get_purge_cutoff_date&lt;br&gt;- Source: PowerCenter Daily Alert History Purge Requestor&lt;br&gt;- Response: PowerCenter Real-Time Alert Manager Alert&lt;br&gt;- Persona: pcmonitor</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_S5 Purge alert history</td>
<td>Notify when alert history is purged.</td>
<td>- Topic: pc_alert_history_purge_request&lt;br&gt;- Analytics: pc_get_alert_history_purge_count, pc_get_purge_cutoff_date&lt;br&gt;- Source: PowerCenter Daily Alert History Purge Requestor&lt;br&gt;- Response: PowerCenter Real-Time Alert Manager Alert&lt;br&gt;- Persona: pcmonitor</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_S6 Load Global Settings from Database</td>
<td>Generate Real-Time Alert Manager alert when global settings are loaded from the database.</td>
<td>- Topic: pc_pmpc_global_settings&lt;br&gt;- Analytics: pc_get_rtam&lt;br&gt;- Source: PowerCenter Load PMPC Global Settings from Database&lt;br&gt;- Response: PowerCenter Real-Time Alert Manager Alert&lt;br&gt;- Persona: pcmonitor</td>
<td>Deployed</td>
</tr>
<tr>
<td>PC_S7 SNMP Notification Response</td>
<td>Generate SNMP trap for alerts. To enable sending notifications as SNMP traps, deploy this rule.</td>
<td>- Topic: pc_notifications&lt;br&gt;- Response: SNMP v2 Response</td>
<td>Draft</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Properties</td>
<td>State</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>PC_S8 RTAM and Email Notification</td>
<td>Generate RTAM and Email Notification</td>
<td>Do not edit. For internal use.</td>
<td>Deployed</td>
</tr>
</tbody>
</table>
| PC_GS21 Check whether the session Target Load Type is Bulk | Notify if the session "Target Load Type" is set to "Bulk". | - Topic: pc Sessions
- Analytics: pc_get_session_mapping_attribute
- Source: PowerCenter Sessions Modified Incremental
- Response: PowerCenter Notification Response
- Persona: apparchitect | Draft    |
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Response Type</th>
<th>Description</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerCenter Alert Recorder Response</td>
<td>SQL</td>
<td>Records alerts to the RulePoint database.</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Email Response</td>
<td>Email</td>
<td>Sends email to the specified users with content based on the response properties.</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter Notification Response</td>
<td>Event Transformer</td>
<td>Transforms events to notification events.</td>
<td>Deployed</td>
</tr>
<tr>
<td>PowerCenter RTAM Alert</td>
<td>RTAM</td>
<td>Sends alerts to Real-Time Alert Manager.</td>
<td>Deployed</td>
</tr>
<tr>
<td>Name</td>
<td>Response Type</td>
<td>Description</td>
<td>State</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>PowerCenter Alert History Purge Response</td>
<td>SQL</td>
<td>Purges alert history older than the specified number of days.</td>
<td>Deployed</td>
</tr>
<tr>
<td>SNMP v2 Response</td>
<td>SNMP Response</td>
<td>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.</td>
<td>Draft</td>
</tr>
</tbody>
</table>
The look up table for proactive monitoring contains the attribute values that you can use in the on-demand reports.

The **PCPM_DROPDOWN** table or proactive monitoring lookup table is created while you install Proactive Monitoring for PowerCenter Governance. Based on the attribute name and the decoded attribute value, you can use the attribute value in the on-demand reports. For example, if the attribute name is *Commit Type*, and the decoded attribute value is *Source*, then use the attribute value as 0.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
<th>Decoded Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commit Type</td>
<td>0</td>
<td>Source</td>
</tr>
<tr>
<td>Commit Type</td>
<td>1</td>
<td>Target</td>
</tr>
<tr>
<td>Commit Type</td>
<td>2</td>
<td>User Defined</td>
</tr>
<tr>
<td>Decimal Separator</td>
<td>1</td>
<td>.</td>
</tr>
<tr>
<td>Decimal Separator</td>
<td>2</td>
<td>.</td>
</tr>
<tr>
<td>Dynamic Partitioning</td>
<td>0</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dynamic Partitioning</td>
<td>1</td>
<td>Based on number of partitions</td>
</tr>
<tr>
<td>Dynamic Partitioning</td>
<td>2</td>
<td>Based on number of nodes in grid</td>
</tr>
<tr>
<td>Dynamic Partitioning</td>
<td>3</td>
<td>Based on source partitioning</td>
</tr>
<tr>
<td>Dynamic Partitioning</td>
<td>4</td>
<td>Based on number of CPUs</td>
</tr>
<tr>
<td>Error Log Type</td>
<td>0</td>
<td>None</td>
</tr>
<tr>
<td>Error Log Type</td>
<td>1</td>
<td>Relational Database</td>
</tr>
<tr>
<td>Error Log Type</td>
<td>2</td>
<td>Flat File</td>
</tr>
<tr>
<td>Is Partitionable</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Is Partitionable</td>
<td>1</td>
<td>Locally</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Attribute Value</td>
<td>Decoded Attribute Value</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Is Partitionable</td>
<td>2</td>
<td>Across Grid</td>
</tr>
<tr>
<td>Join Type</td>
<td>1</td>
<td>Normal Join</td>
</tr>
<tr>
<td>Join Type</td>
<td>2</td>
<td>Master Outer Join</td>
</tr>
<tr>
<td>Join Type</td>
<td>3</td>
<td>Detail Outer Join</td>
</tr>
<tr>
<td>Join Type</td>
<td>4</td>
<td>Full Outer Join</td>
</tr>
<tr>
<td>Lookup Policy on Multiple Match</td>
<td>1</td>
<td>Use First Value</td>
</tr>
<tr>
<td>Lookup Policy on Multiple Match</td>
<td>2</td>
<td>Use Last Value</td>
</tr>
<tr>
<td>Lookup Policy on Multiple Match</td>
<td>3</td>
<td>Report Error</td>
</tr>
<tr>
<td>Lookup Policy on Multiple Match</td>
<td>4</td>
<td>Use Any Value</td>
</tr>
<tr>
<td>Master Sort Order</td>
<td>0</td>
<td>Ascending</td>
</tr>
<tr>
<td>Master Sort Order</td>
<td>1</td>
<td>Auto</td>
</tr>
<tr>
<td>Null Ordering</td>
<td>0</td>
<td>Null Is Highest Value</td>
</tr>
<tr>
<td>Null Ordering</td>
<td>1</td>
<td>Null Is Lowest Value</td>
</tr>
<tr>
<td>Null Ordering in detail</td>
<td>0</td>
<td>Null Is Highest Value</td>
</tr>
<tr>
<td>Null Ordering in detail</td>
<td>1</td>
<td>Null Is Lowest Value</td>
</tr>
<tr>
<td>Null Ordering in master</td>
<td>0</td>
<td>Null Is Highest Value</td>
</tr>
<tr>
<td>Null Ordering in master</td>
<td>1</td>
<td>Null Is Lowest Value</td>
</tr>
<tr>
<td>On Pre-Post SQL error</td>
<td>0</td>
<td>Stop</td>
</tr>
<tr>
<td>On Pre-Post SQL error</td>
<td>1</td>
<td>Continue</td>
</tr>
<tr>
<td>On Pre-session command task error</td>
<td>0</td>
<td>Stop</td>
</tr>
<tr>
<td>On Pre-session command task error</td>
<td>1</td>
<td>Continue</td>
</tr>
<tr>
<td>On Stored Procedure error</td>
<td>0</td>
<td>Stop</td>
</tr>
<tr>
<td>On Stored Procedure error</td>
<td>1</td>
<td>Continue</td>
</tr>
<tr>
<td>Output Is Repeatable</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>Output Is Repeatable</td>
<td>1</td>
<td>Based On Input Order</td>
</tr>
<tr>
<td>Output Is Repeatable</td>
<td>2</td>
<td>Always</td>
</tr>
<tr>
<td>Override Tracing</td>
<td>0</td>
<td>None</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Attribute Value</td>
<td>Decoded Attribute Value</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Override Tracing</td>
<td>1</td>
<td>Terse</td>
</tr>
<tr>
<td>Override Tracing</td>
<td>2</td>
<td>Normal</td>
</tr>
<tr>
<td>Override Tracing</td>
<td>3</td>
<td>Verbose Initialization</td>
</tr>
<tr>
<td>Override Tracing</td>
<td>4</td>
<td>Verbose Data</td>
</tr>
<tr>
<td>Pre-build Lookup Cache</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>Pre-build Lookup Cache</td>
<td>1</td>
<td>Always allowed</td>
</tr>
<tr>
<td>Pre-build Lookup Cache</td>
<td>2</td>
<td>Always disallowed</td>
</tr>
<tr>
<td>Pushdown Optimization</td>
<td>0</td>
<td>None</td>
</tr>
<tr>
<td>Pushdown Optimization</td>
<td>1</td>
<td>To Source</td>
</tr>
<tr>
<td>Pushdown Optimization</td>
<td>2</td>
<td>To Target</td>
</tr>
<tr>
<td>Pushdown Optimization</td>
<td>3</td>
<td>Full</td>
</tr>
<tr>
<td>Pushdown Optimization</td>
<td>4</td>
<td>$$PushdownConfig</td>
</tr>
<tr>
<td>Recovery Strategy</td>
<td>0</td>
<td>Fail task and continue workflow</td>
</tr>
<tr>
<td>Recovery Strategy</td>
<td>1</td>
<td>Resume from last checkpoint</td>
</tr>
<tr>
<td>Recovery Strategy</td>
<td>2</td>
<td>Restart task</td>
</tr>
<tr>
<td>Save Session log by</td>
<td>0</td>
<td>Session Runs</td>
</tr>
<tr>
<td>Save Session log by</td>
<td>1</td>
<td>Session timestamp</td>
</tr>
<tr>
<td>Save Workflow log by</td>
<td>0</td>
<td>By Runs</td>
</tr>
<tr>
<td>Save Workflow log by</td>
<td>1</td>
<td>By Timestamp</td>
</tr>
<tr>
<td>Source Type</td>
<td>1</td>
<td>Database</td>
</tr>
<tr>
<td>Source Type</td>
<td>2</td>
<td>Flat File</td>
</tr>
<tr>
<td>Source Type</td>
<td>3</td>
<td>Source Qualifier</td>
</tr>
<tr>
<td>Stored Procedure Type</td>
<td>1</td>
<td>Target Pre Load</td>
</tr>
<tr>
<td>Stored Procedure Type</td>
<td>2</td>
<td>Target Post Load</td>
</tr>
<tr>
<td>Stored Procedure Type</td>
<td>3</td>
<td>Normal</td>
</tr>
<tr>
<td>Stored Procedure Type</td>
<td>4</td>
<td>Source Pre Load</td>
</tr>
<tr>
<td>Stored Procedure Type</td>
<td>5</td>
<td>Source Post Load</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Attribute Value</td>
<td>Decoded Attribute Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Thousand Separator</td>
<td>0</td>
<td>None</td>
</tr>
<tr>
<td>Thousand Separator</td>
<td>1</td>
<td>.</td>
</tr>
<tr>
<td>Thousand Separator</td>
<td>2</td>
<td>.</td>
</tr>
<tr>
<td>Top/Bottom</td>
<td>0</td>
<td>Bottom</td>
</tr>
<tr>
<td>Top/Bottom</td>
<td>1</td>
<td>Top</td>
</tr>
<tr>
<td>Tracing Level</td>
<td>1</td>
<td>Terse</td>
</tr>
<tr>
<td>Tracing Level</td>
<td>2</td>
<td>Normal</td>
</tr>
<tr>
<td>Tracing Level</td>
<td>3</td>
<td>Verbose Initialization</td>
</tr>
<tr>
<td>Tracing Level</td>
<td>4</td>
<td>Verbose Data</td>
</tr>
<tr>
<td>Transformation Scope</td>
<td>0</td>
<td>Row</td>
</tr>
<tr>
<td>Transformation Scope</td>
<td>1</td>
<td>Transaction</td>
</tr>
<tr>
<td>Transformation Scope</td>
<td>2</td>
<td>All Input</td>
</tr>
<tr>
<td>Treat Source Rows As</td>
<td>0</td>
<td>Insert</td>
</tr>
<tr>
<td>Treat Source Rows As</td>
<td>1</td>
<td>Delete</td>
</tr>
<tr>
<td>Treat Source Rows As</td>
<td>2</td>
<td>Update</td>
</tr>
<tr>
<td>Treat Source Rows As</td>
<td>3</td>
<td>Data Driven</td>
</tr>
<tr>
<td>Type</td>
<td>0</td>
<td>Informatica</td>
</tr>
<tr>
<td>Type</td>
<td>1</td>
<td>COM</td>
</tr>
</tbody>
</table>
## 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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_is_valid</td>
<td>Indicates whether the session status is valid.</td>
</tr>
<tr>
<td>session_is_impacted</td>
<td>Indicates whether there is an impact on a session status when a user makes a change in the session.</td>
</tr>
<tr>
<td>curr_tstamp</td>
<td>Indicates the current time of event generation.</td>
</tr>
<tr>
<td>version_number</td>
<td>Indicates the version number of the PowerCenter session that a user modifies within the incremental time window.</td>
</tr>
<tr>
<td>session_last_saved</td>
<td>Indicates the time stamp when the PowerCenter session was last saved within the incremental time window.</td>
</tr>
<tr>
<td>workflow_name</td>
<td>Indicates the workflow name of the associated PowerCenter session.</td>
</tr>
<tr>
<td>tstamp</td>
<td>Indicates the time stamp when the PowerCenter session was last saved within the incremental time window.</td>
</tr>
<tr>
<td>session_id</td>
<td>Indicates the internal ID generated within PowerCenter for the session.</td>
</tr>
<tr>
<td>mapping_last_saved</td>
<td>Indicates the last saved time for the mapping associated with the PowerCentre session.</td>
</tr>
<tr>
<td>is_reusable</td>
<td>Indicates whether you can reuse the session.</td>
</tr>
<tr>
<td>is_enabled</td>
<td>Indicates whether you can enable or disable the session.</td>
</tr>
<tr>
<td>session_name</td>
<td>Indicates the name of the PowerCenter session.</td>
</tr>
<tr>
<td>mapping_name</td>
<td>Indicates the mapping name associated with the PowerCenter session.</td>
</tr>
<tr>
<td>rs</td>
<td>Indicates the Repository Service name associated with the PowerCenter session.</td>
</tr>
<tr>
<td>session_comments</td>
<td>Provides the comments in the section content of the session.</td>
</tr>
<tr>
<td>folder</td>
<td>Indicates the folder name associated with the session.</td>
</tr>
</tbody>
</table>
The following table lists the properties for the `pc_mapplets` topic:

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

The following table lists the properties for the `pc_worklets` topic:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>worklet_id</td>
<td>Indicates the internal ID generated within PowerCenter for the worklet.</td>
</tr>
<tr>
<td>comments</td>
<td>Provides comments of the PowerCenter worklet.</td>
</tr>
<tr>
<td>last_saved</td>
<td>Indicates the time stamp when the PowerCenter worklet was last saved within the incremental time window.</td>
</tr>
<tr>
<td>version_number</td>
<td>Indicates the version number of the modified PowerCenter worklet within the incremental time window.</td>
</tr>
<tr>
<td>worklet_name</td>
<td>Indicates the name of the PowerCenter worklet.</td>
</tr>
</tbody>
</table>
The following table lists the properties for the pc_transforms topic:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mapping_id</td>
<td>Indicates the internal ID generated within PowerCenter for the mapping.</td>
</tr>
<tr>
<td>transform_type</td>
<td>Indicates the type of PowerCenter transformation. For example, type can be Source Definition or Target Definition.</td>
</tr>
<tr>
<td>last_saved</td>
<td>Indicates the time stamp when the PowerCenter transformation was last saved within the incremental time window.</td>
</tr>
<tr>
<td>transform_type_id</td>
<td>Provides the internal ID of the transformation type.</td>
</tr>
<tr>
<td>version_number</td>
<td>Indicates the version number of the modified PowerCenter transformation within the incremental time window.</td>
</tr>
<tr>
<td>transform_description</td>
<td>Provides the description of the PowerCenter transformation.</td>
</tr>
<tr>
<td>transform_name</td>
<td>Indicates the name of the PowerCenter transformation.</td>
</tr>
<tr>
<td>transform_id</td>
<td>Indicates the internal ID generated within PowerCenter for the transformation.</td>
</tr>
<tr>
<td>tstamp</td>
<td>Indicates the time stamp when the PowerCenter transformation was last saved within the incremental time window.</td>
</tr>
<tr>
<td>workflow_name</td>
<td>Indicates the workflow name associated with the PowerCenter transformation.</td>
</tr>
<tr>
<td>mapping_name</td>
<td>Indicates the mapping name associated with the PowerCenter transformation.</td>
</tr>
<tr>
<td>rs</td>
<td>Indicates the Repository Service name associated with the PowerCenter transformation.</td>
</tr>
<tr>
<td>folder</td>
<td>Indicates the folder name associated with the PowerCenter transformation.</td>
</tr>
</tbody>
</table>
The following table lists the properties for the `pc_mappings` topic:

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

The following table lists the properties for the `pc_workflows` topic:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflow_last_saved</td>
<td>Indicates the time stamp when the PowerCenter workflow was last saved within the incremental time window.</td>
</tr>
<tr>
<td>workflow_is_valid</td>
<td>Indicates whether the workflow status is valid.</td>
</tr>
<tr>
<td>workflow_is_runnable_service</td>
<td>Indicates whether the workflow is runnable, is valid, and is assigned to an Integration Service that is accessible.</td>
</tr>
<tr>
<td>version_number</td>
<td>Indicates the version number of the modified PowerCenter workflow within the incremental time window.</td>
</tr>
</tbody>
</table>
## Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflow_comments</td>
<td>Provides the comments of the PowerCenter workflow.</td>
</tr>
<tr>
<td>workflow_is_service</td>
<td>Indicates whether the workflow is a service workflow. You can only run a service workflow.</td>
</tr>
<tr>
<td>workflow_name</td>
<td>Indicates the name of the PowerCenter workflow.</td>
</tr>
<tr>
<td>tstamp</td>
<td>Indicates the time stamp when the PowerCenter workflow was last saved within the incremental time window.</td>
</tr>
<tr>
<td>rs</td>
<td>Indicates the Repository Service name associated with the PowerCenter workflow.</td>
</tr>
<tr>
<td>workflow_id</td>
<td>Indicates the internal ID generated within PowerCenter for the workflow.</td>
</tr>
<tr>
<td>folder</td>
<td>Indicates the folder name associated with the PowerCenter workflow.</td>
</tr>
<tr>
<td>domain</td>
<td>Indicates the domain name associated with the PowerCenter workflow.</td>
</tr>
<tr>
<td>user_name</td>
<td>Indicates the name of the user who enforced a change to the PowerCenter workflow within the incremental time window.</td>
</tr>
</tbody>
</table>

The following table lists the properties for the pc_command_tasks topic:

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

The following table lists the properties for the pc_running_sessions_workflows_count topic:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_name</td>
<td>Indicates the Integration Service name associated with the PowerCenter sessions and workflows that are running.</td>
</tr>
<tr>
<td>session_cnt</td>
<td>Indicates the number of sessions running within the Informatica domain.</td>
</tr>
<tr>
<td>tstamp</td>
<td>Indicates the snapshot time when the count of running sessions and workflows was extracted.</td>
</tr>
<tr>
<td>rs</td>
<td>Indicates the Repository Service name associated with the running PowerCenter sessions and workflows.</td>
</tr>
<tr>
<td>workflow_cnt</td>
<td>Indicates the number of workflows that run within the Informatica domain.</td>
</tr>
<tr>
<td>domain</td>
<td>Indicates the domain name associated with the running PowerCenter sessions and workflows.</td>
</tr>
</tbody>
</table>
APPENDIX C

Windows Authentication Mode

This appendix includes the following topics:

- Windows Authentication Mode Overview
- Enable Windows Authentication Mode

Windows Authentication Mode Overview

Users can connect to Proactive Monitoring for PowerCenter installed on an instance of SQL Server using Windows Authentication. Windows Authentication mode allows a user to connect through the Microsoft Windows user account.

Enable Windows Authentication Mode

Perform the following steps to enable authentication mode in Windows.

1. Copy the .dll file from <INSTALLER_HOME>/bin\common\dll directory to a specific location.
2. When you install Proactive Monitoring for PowerCenter, use the below format for the custom JDBC connection string for the DataDirect driver:

   jdbc:informatica:sqlserver://<HOST>:<PORT>;DatabaseName=<DATABASE_NAME>;AuthenticationMethod=ntlm;LoadLibraryPath=\<DLL_PATH>

   where DLL_PATH is the path where the dll file is copied to.

   You must use double slash - \ to separate the path. For example, db.url=jdbc:informatica:sqlserver://LOCALHOST:1433;databaseName=rulepoint61;AuthenticationMethod=ntlm;LoadLibraryPath=E:\\Installs

3. Create a directory named endorsed in <PROACTIVE_MONITORING_HOME>/rulepoint/design and <PROACTIVE_MONITORING_HOME>/rulepoint/system/java/lib.
6. Copy dwsq1server.jar from <PROACTIVE_MONITORING_HOME>/rulepoint/design/webapps/rulepoint/web-inf/lib to <PROACTIVE_MONITORING_HOME>/rulepoint/design/endorsed.

7. Start the Proactive Monitoring for PowerCenter instance.
   a. Go to: <PROACTIVE_MONITORING_HOME>/bin.
      Enter the following command:
      solutions.bat start

8. Import the objects.
   a. Go to <PROACTIVE_MONITORING_HOME>/bin.
   b. Enter the following command:
      pmpc.bat import Governance
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 I do not configure reports during Proactive Monitoring installation, can I configure reports after installation?
Yes. Refer to the "Getting Started Guide" for information on how to import the PMPC report XML.

What are the prerequisite steps for PMPC Reporting to work?
PMPC reports use predefined PowerCenter workflows to transform PMPC alert data to report-specific format. You must import the workflows and schedule the workflows in the Informatica domain to generate PMPC reports. Refer to "Getting Started Guide" for information on how to import the PMPC reporting XML and start the PMPC reporting workflows.

If you use Proactive Monitoring for PowerCenter 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. It is recommended that you use the Proactive Monitoring for PowerCenter Management Console to manage the PowerCenter Monitored Folders watchlist.

Why do I 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 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 Management for PowerCenter 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.
Does the Proactive Monitoring for PowerCenter Governance support the same version of the Apache Tomcat that the PowerCenter supports?

No. The Proactive Monitoring for PowerCenter Governance supports Apache Tomcat 7.0.25.

Does the Proactive Monitoring for PowerCenter Governance share the Apache Tomcat instance with the PowerCenter during run time?

No. The Proactive Monitoring for PowerCenter Governance needs a dedicated Apache Tomcat server on a separate machine.

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 a single instance of the Proactive Monitoring for PowerCenter Governance monitor multiple PowerCenter repositories?

Yes. You can monitor multiple PowerCenter repositories through a single instance of the Proactive Monitoring for PowerCenter Governance.

Can the Proactive Monitoring for PowerCenter Governance monitor multiple Informatica domains?

No. You cannot monitor multiple Informatica domains from the Proactive Monitoring for PowerCenter Governance. You can monitor a single domain with an instance of the Proactive Monitoring solution.

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

In the Proactive Monitoring for PowerCenter Governance, you can use the Proactive Monitoring for PowerCenter 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.

Can you install both Proactive Monitoring for PowerCenter 3.0 and RulePoint 6.1 on the same machine?

You do not need to install a separate instance of RulePoint. You can use RulePoint 6.1 that is packaged along with the Proactive Monitoring for PowerCenter 3.0 installer. Use the topology configurations to administer the nodes for Proactive Monitoring for PowerCenter and RulePoint. You can create nodes that are specific for RulePoint and Proactive Monitoring for PowerCenter. Create projects specific for RulePoint and Proactive Monitoring for PowerCenter to keep the corresponding objects separate.
How do you register RulePoint 6.1 as Windows services after you completed installation of Proactive Monitoring for PowerCenter?

You can register Windows services after installation. Go to the command prompt, navigate to C:\<PROACTIVE_MONITORING_HOME>\rulepoint\bin\services, and run the following scripts:

- To register the design-time service, run design.exe install.
- To register the topology service, run topology.exe.
- To register host agent, run hostagent.exe
Appendix E

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
Alert Recipients
parameters 81
analytics
predefined analytics 113

C
configuration
Proactive Monitoring 77, 80
settings 80
setup 77
configure
host 78
host properties 78
node 79
node properties 79

E
email
host configuration 53
environment variables
DISPLAY 26

G
Global Settings
alert hyperlink 80
alert purge frequency 80
configure 80
do not disturb 80
workflows and sessions persisted 80
governance alerts
monitor 100
graphical mode
installation requirements 26

I
IBM DB2
create schemas 30
Install
validation 56
installation requirements
X Window Server 26

M
manage
monitored folders watchlist 91
PMPC SQL source service 89
management console
configure source timestamp 83
log in 77
Management Console
settings 76
setup 76
Microsoft SQL
create schemas 31
monitor
governance alerts 100
operations alerts 98
reports 95
monitored folders watchlist
manage 91

O
on-demand reports
create 102
run 103
operations alerts
monitor 98
Oracle
create schemas 29

P
PMPC SQL source service
manage 89
Proactive Monitoring
configuration 75
Proactive Monitoring for PowerCenter Management Console
overview 76

R
reports
monitor 95
schedule workflow 53
responder
predefined responder 115
response
predefined response 137
rule
advanced rule
description 21
RulePoint
responders 14
RulePoint (continued)
  rules 14
  sources 14
  rules
    advanced rules 129
    predefined advanced rules 129
  run
    on-demand reports 103

S
  schedule workflow
    reports 53
  SNMP
    alerts 105
    responder 106

T
  template rules
    predefined template rules 124
  templates
    predefined templates 118
  topics
    predefined topics 109

tstamp
  configuration 83

U
  upgrade
    cleanup old objects 74
    post-installation tasks 74
  Upgrade 23

W
  Watchlist
    configuration 83
    watchlists
      predefined watchlists 107

X
  X Window Server
    installation requirements 26