INFORMATICA®

Informatica (Version 9.1.0)

Administrator Guide



Informatica Administrator Guide

Version 9.1.0
March 2011

Copyright (c) 1998-2011 Informatica. All rights reserved.

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

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

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

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

Portions of this software and/or documentation are subject to copyright held by third parties, including without limitation: Copyright DataDirect Technologies. All rights reserved. Copyright © Sun Microsystems. All rights reserved. Copyright © RSA Security Inc. All Rights Reserved. Copyright © Ordinal Technology Corp. All rights reserved.Copyright © Aandacht c.v. All rights reserved. Copyright Genivia, Inc. All rights reserved. Copyright 2007 Isomorphic Software. All rights reserved. Copyright © Meta Integration Technology, Inc. All rights reserved. Copyright © Oracle. All rights reserved. Copyright © Adobe Systems Incorporated. All rights reserved. Copyright © DataArt, Inc. All rights reserved. Copyright © ComponentSource. All rights reserved. Copyright © Microsoft Corporation. All rights reserved. Copyright © Rogue Wave Software, Inc. All rights reserved. Copyright © Teradata Corporation. All rights reserved. Copyright © Yahoo! Inc. All rights reserved. Copyright © Glyph & Cog, LLC. All rights reserved. Copyright © Thinkmap, Inc. All rights reserved. Copyright © Clearpace Software Limited. All rights reserved. Copyright © Information Builders, Inc. All rights reserved. Copyright © OSS Nokalva, Inc. All rights reserved. Copyright Edifecs, Inc. All rights reserved.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/), and other software which is licensed under the Apache License, Version 2.0 (the "License"). You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

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

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

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

This product includes Curl software which is Copyright 1996-2007, Daniel Stenberg, <daniel@haxx.se>. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at http://curl.haxx.se/docs/copyright.html. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

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

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

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

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

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

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

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

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

This product includes software licensed under the terms at http://www.tcl.tk/software/tcltk/license.html, http://www.bosrup.com/web/overlib/?License, http://www.stlport.org/doc/license.html, http://www.asm.ow2.org/license.html, http://www.cryptix.org/LICENSE.TXT, http://hsqldb.org/web/hsqlLicense.html, http://httpunit.sourceforge.net/doc/license.html, http://jung.sourceforge.net/license.txt , http://www.gzip.org/zlib/zlib_license.html, http://www.openldap.org/software/release/license.html, http://www.libssh2.org, http://slf4j.org/license.html, http://www.sente.ch/software/OpenSourceLicense.html, http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3-license-agreement, http://antlr.org/license.html, http://aopalliance.sourceforge.net/, http://www.bouncycastle.org/licence.html, http://www.jgraph.com/jgraphdownload.html, http://www.jgraph.com/jgraphdownload.html, http://www.jcraft.com/jsch/LICENSE.txt and http://jotm.objectweb.org/bsd_license.html.

This product includes software licensed under the Academic Free License (http://www.opensource.org/licenses/afl-3.0.php), the Common Development and Distribution License (http://www.opensource.org/licenses/cddl1.php) the Common Public License (http://www.opensource.org/licenses/cpl1.0.php) and the BSD License (http://www.opensource.org/licenses/bsd-license.php).

This product includes software copyright © 2003-2006 Joe WaInes, 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 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; 6,339,775; 6,640,226; 6,789,096; 6,820,077; 6,823,373; 6,850,947; 6,895,471; 7,117,215; 7,162,643; 7,254,590; 7,281,001; 7,421,458; 7,496,588; 7,523,121; 7,584,422; 7,720,842; 7,721,270; and 7,774,791, 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 non-infringement, 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 NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

Part Number: IN-ADG-91000-0001

Table of Contents

Preface . . . . . **xxiv**

Informatica Resources xxiv

Informatica Customer Portal xxiv

Informatica Documentation xxiv

Informatica Web Site xxiv

Informatica How-To Library xxiv

Informatica Knowledge Base xxv

Informatica Multimedia Knowledge Base xxv

Informatica Global Customer Support xxv

Chapter 1: Understanding Domains **1**

Understanding Domains Overview 1

Nodes 2

Gateway Nodes 2

Worker Nodes 2

Service Manager 2

Application Services 3

Analyst Service 4

Content Management Service 4

Data Integration Service 4

Metadata Manager Service 5

Model Repository Service 5

PowerCenter Integration Service 5

PowerCenter Repository Service 5

PowerExchange Listener Service 5

PowerExchange Logger Service 6

Reporting Service 6

SAP BW Service 6

Web Services Hub 6

User Security 6

Encryption 7

Authentication 7

Authorization 7

High Availability 8

Chapter 2: Managing Your Account **9**

Managing Your Account Overview 9

Logging In 9

Informatica Administrator URL. . . . 10
Changing Your Password. . . . 10
Editing Preferences. . . . 11
Preferences. . . . 11

Chapter 3: Using Informatica Administrator. . . . 12
Using Informatica Administrator Overview. . . . 12
Domain Tab Overview. . . . 13
Domain Tab - Services and Nodes View. . . . 13
Domain. . . . 14
Folders. . . . 14
Application Services. . . . 15
Nodes. . . . 18
Grids. . . . 19
Licenses. . . . 19
Domain Tab - Connections View. . . . 19
Logs Tab. . . . 20
Reports Tab. . . . 20
Monitoring Tab. . . . 21
Security Tab. . . . 21
Using the Search Section. . . . 21
Using the Security Navigator. . . . 22
Groups. . . . 22
Users. . . . 23
Roles. . . . 23
Keyboard Shortcuts. . . . 23

Chapter 4: Domain Management. . . . 25
Domain Management Overview. . . . 25
Alert Management. . . . 26
Configuring SMTP Settings. . . . 26
Subscribing to Alerts. . . . 26
Viewing Alerts. . . . 27
Folder Management. . . . 27
Creating a Folder. . . . 28
Moving Objects to a Folder. . . . 28
Removing a Folder 28
Domain Security Management. . . . 29
User Security Management. . . . 29
Application Service Management. . . . 30
Enabling and Disabling Services and Service Processes. . . . 30
Viewing Service Processes. . . . 31
Configuring Restart for Service Processes. . . . 31

Removing Application Services. . . . 31
Troubleshooting Application Services. . . . 32
Node Management. . . . 32
Defining and Adding Nodes. . . . 32
Configuring Node Properties. . . . 33
Viewing Processes on the Node. . . . 35
Shutting Down and Restarting the Node. . . . 35
Removing the Node Association. . . . 36
Removing a Node. . . . 36
Gateway Configuration. . . . 37
Domain Configuration Management. . . . 37
Backing Up the Domain Configuration. . . . 38
Restoring the Domain Configuration. . . . 38
Migrating the Domain Configuration. . . . 39
Updating the Domain Configuration Database Connection. . . . 40
Domain Tasks. . . . 41
Managing and Monitoring Application Services and Nodes. . . . 41
Viewing Dependencies for Application Services, Nodes, and Grids. . . . 42
Shutting Down a Domain. . . . 43
Domain Properties. . . . 44
General Properties. . . . 44
Database Properties. . . . 45
Gateway Configuration Properties. . . . 46
Service Level Management. . . . 46
SMTP Configuration. . . . 47
Custom Properties. . . . 47

Chapter 5: Application Service Upgrade. . . . 48

Application Service Upgrade Overview. . . . 48
Service Upgrade for Data Quality 9.0.1. . . . 48
Service Upgrade for Data Services 9.0.1. . . . 49
Service Upgrade for PowerCenter 9.0.1. . . . 49
Service Upgrade for PowerCenter 8.6.1. . . . 49
Service Upgrade for PowerCenter 8.5.x or 8.6. . . . 49
Service Upgrade for PowerCenter 8.1.x. . . . 49
Service Upgrade Wizard. . . . 50
Upgrade Report. . . . 51
Running the Service Upgrade Wizard. . . . 51
Users and Groups Conflict Resolution. . . . 52

Chapter 6: Domain Security. . . . 53

Domain Security Overview. . . . 53
Secure Communication Within the Domain. . . . 53

Configuring Secure Communication Within the Domain. . . . 54
TLS Configuration Using infasetup. . . . 54
Secure Communication with External Components. . . . 55
Secure Communication to the Administrator Tool. . . . 55

Chapter 7: Users and Groups. . . . 57

Users and Groups Overview. . . . 57
Default Everyone Group. . . . 58
Understanding User Accounts. . . . 58
Default Administrator. . . . 58
Domain Administrator. . . . 58
Application Client Administrator. . . . 59
User. . . . 59
Understanding Authentication and Security Domains 60
Native Authentication. . . . 60
LDAP Authentication. . . . 60
Setting Up LDAP Authentication. . . . 60
Step 1. Set Up the Connection to the LDAP Server. . . . 61
Step 2. Configure Security Domains. . . . 62
Step 3. Schedule the Synchronization Times. . . . 64
Deleting an LDAP Security Domain. . . . 65
Using a Self-Signed SSL Certificate. . . . 65
Using Nested Groups in the LDAP Directory Service. . . . 65
Managing Users. . . . 66
Adding Native Users. . . . 66
Editing General Properties of Native Users. . . . 67
Assigning Users to Native Groups. . . . 67
Enabling and Disabling User Accounts. . . . 67
Deleting Native Users. . . . 68
LDAP Users. . . . 69
Increasing System Memory for Many Users. . . . 69
Managing Groups. . . . 69
Adding a Native Group. . . . 69
Editing Properties of a Native Group. . . . 70
Moving a Native Group to Another Native Group. . . . 70
Deleting a Native Group. . . . 71
LDAP Groups. . . . 71
Managing Operating System Profiles. . . . 71
Create Operating System Profiles 71
Properties of Operating System Profiles 72
Creating an Operating System Profile. . . . 73

Chapter 8: Privileges and Roles. 74

Privileges and Roles Overview. 74
Privileges. 74
Roles. 75
Domain Privileges. 75
Security Administration Privilege Group. 77
Domain Administration Privilege Group. 77
Monitoring Privilege Group. 80
Tools Privilege Group. 81
Analyst Service Privilege. 81
Data Integration Service Privilege. 81
Metadata Manager Service Privileges. 82
Catalog Privilege Group. 83
Load Privilege Group. 85
Model Privilege Group. 85
Security Privilege Group. 86
Model Repository Service Privilege. 86
PowerCenter Repository Service Privileges. 87
Tools Privilege Group. 88
Folders Privilege Group. 89
Design Objects Privilege Group. 90
Sources and Targets Privilege Group. 91
Run-time Objects Privilege Group. 92
Global Objects Privilege Group. 94
PowerExchange Application Service Privileges. 96
Reporting Service Privileges. 96
Administration Privilege Group. 98
Alerts Privilege Group. 99
Communication Privilege Group. 99
Content Directory Privilege Group. 100
Dashboards Privilege Group. 101
Indicators Privilege Group. 101
Manage Account Privilege Group. 102
Reports Privilege Group. 102
Managing Roles. 103
System-Defined Roles. 104
Custom Roles. 105
Managing Custom Roles. 105
Assigning Privileges and Roles to Users and Groups. 106
Inherited Privileges. 107
Steps to Assign Privileges and Roles to Users and Groups. 107
Viewing Users with Privileges for a Service. 108

Troubleshooting Privileges and Roles. 108

Chapter 9: Permissions. 111

Permissions Overview. 111
Types of Permissions. 112
Permission Search Filters. 113
Domain Object Permissions. 113
Permissions by Domain Object. 114
Permissions by User or Group. 115
Operating System Profile Permissions. 116
Connection Permissions. 117
Types of Connection Permissions. 118
Default Connection Permissions. 118
Assigning Permissions on a Connection. 118
Editing Permissions on a Connection. 119
SQL Data Service Permissions. 119
Types of SQL Data Service Permissions. 120
Assigning Permissions on an SQL Data Service. 120
Viewing Permission Details on an SQL Data Service. 121
Editing Permissions on an SQL Data Service. 121
Denying Permissions on an SQL Data Service. 122
Column Level Security. 122
Web Service Permissions. 123
Types of Web Service Permissions. 124
Assigning Permissions on a Web Service. 124
Viewing Permission Details on a Web Service. 125
Editing Permissions on a Web Service. 125

Chapter 10: High Availability. 126

High Availability Overview. 126
Resilience. 127
Restart and Failover. 128
Recovery. 129
High Availability in the Base Product. 129
Internal PowerCenter Resilience. 130
PowerCenter Repository Service Resilience to PowerCenter Repository Database. 130
Restart Services. 130
Manual PowerCenter Workflow and Session Recovery. 130
Multiple Gateway Nodes. 130
Achieving High Availability. 131
Configuring PowerCenter Internal Components for High Availability. 131
Using Highly Available External Systems. 132
Rules and Guidelines for Configuring for High Availability. 132

Managing Resilience. 133
Configuring Service Resilience for the Domain. 134
Configuring Application Service Resilience. 134
Understanding PowerCenter Client Resilience. 134
Configuring Command Line Program Resilience 134
Managing High Availability for the PowerCenter Repository Service. 136
Resilience. 136
Restart and Failover. 136
Recovery. 137
Managing High Availability for the PowerCenter Integration Service. 137
Resilience. 137
Restart and Failover. 138
Recovery. 141
Troubleshooting High Availability. 142

Chapter 11: Analyst Service. 143

Analyst Service Overview. 143
Analyst Service Architecture. 144
Configuration Prerequisites. 144
Associated Services. 145
Staging Databases. 145
Flat File Cache. 146
Keystore File. 146
Configure the TLS Protocol. 146
Recycling and Disabling the Analyst Service. 147
Properties for the Analyst Service. 147
General Properties for the Analyst Service. 147
Model Repository Service Options. 148
Data Integration Service Options. 148
Staging Database. 149
Logging Options. 149
Custom Properties. 149
Process Properties for the Analyst Service. 149
Node Properties for the Analyst Service Process. 150
Analyst Security Options for the Analyst Service Process. 150
Advanced Properties for the Analyst Service Process. 150
Custom Properties for the Analyst Service Process. 151
Environment Variables for the Analyst Service Process. 151
Creating and Deleting Audit Trail Tables. 151
Creating and Configuring the Analyst Service. 152
Creating an Analyst Service. 152

Chapter 12: Content Management Service 153

Content Management Service Overview 153
Content Management Service Architecture 154
Recycling and Disabling the Content Management Service 154
Content Management Service Properties 155
General Properties 155
Data Integration Service Property 155
Logging Options 155
Custom Properties 156
Content Management Service Process Properties 156
Content Management Service Security Options 156
Address Validation Properties 156
Custom Properties for the Content Management Service Process 158
Creating a Content Management Service 158

Chapter 13: Data Integration Service 159

Data Integration Service Overview 159
Data Integration Service Components 160
Data Transformation Manager 160
Profiling Service Module 160
Mapping Service Module 161
SQL Service Module 161
Web Service Module 162
Data Object Cache Manager 162
Result Set Cache Manager 162
Deployment Manager 162
Data Integration Service Architecture 163
Data and File Caching 163
Data Integration Service Logs 164
Data Integration Service Properties 164
General Properties 164
Model Repository Properties 164
Logging Properties 165
Logical Data Object/Virtual Table Cache Properties 165
Profiling Warehouse Database Properties 166
Mapping Service Properties 166
Advanced Profiling Properties 167
Modules 167
Pass-through Security Properties 168
HTTP Proxy Server Properties 168
HTTP Configuration Properties 168
Custom Properties 169

Data Integration Service Management. . . . 169
Enabling, Disabling, and Recycling the Data Integration Service. . . . 169
Pass-through Security. . . . 170
Data Integration Service Processes. . . . 171
Creating a Data Integration Service. . . . 175
Application Management. . . . 176
Application Properties View. . . . 176
Deploying an Application. . . . 181
Enabling an Application . . . 182
Renaming an Application. . . . 182
Enabling an SQL Data Service. . . . 182
Renaming an SQL Data Service. . . . 183
Enabling a Web Service. . . . 183
Renaming a Web Service. . . . 183
Downloading the WSDL of a Web Service. . . . 183
Starting an Application. . . . 184
Backing Up an Application. . . . 184
Restoring an Application. . . . 184
Refreshing the Applications View . . . 185

Chapter 14: Metadata Manager Service. . . . 186

Metadata Manager Service Overview. . . . 186
Configuring a Metadata Manager Service. . . . 187
Creating a Metadata Manager Service. . . . 188
Metadata Manager Service Properties. . . . 188
Database Connect Strings. . . . 190
Overriding the Repository Database Code Page. . . . 190
Creating and Deleting Repository Content. . . . 190
Creating the Metadata Manager Repository. . . . 191
Restoring the PowerCenter Repository . . . 191
Deleting the Metadata Manager Repository . . . 192
Enabling and Disabling the Metadata Manager Service. . . . 192
Configuring the Metadata Manager Service Properties. . . . 192
General Properties. . . . 193
Metadata Manager Service Properties. . . . 193
Database Properties. . . . 194
Configuration Properties. . . . 195
Connection Pool Properties. . . . 196
Advanced Properties. . . . 196
Custom Properties. . . . 197
Configuring the Associated PowerCenter Integration Service. . . . 198
Privileges for the Associated PowerCenter Integration Service User. . . . 198

Chapter 15: PowerCenter Integration Service 200

PowerCenter Integration Service Overview 200
Creating a PowerCenter Integration Service 201
Enabling and Disabling PowerCenter Integration Services and Processes 202
Enabling or Disabling a PowerCenter Integration Service Process 203
Enabling or Disabling the PowerCenter Integration Service 203
Operating Mode 204
Normal Mode 204
Safe Mode 205
Running the PowerCenter Integration Service in Safe Mode 205
Configuring the PowerCenter Integration Service Operating Mode 207
PowerCenter Integration Service Properties 207
General Properties 208
PowerCenter Integration Service Properties 209
Advanced Properties 210
Operating Mode Configuration 212
Compatibility and Database Properties 212
Configuration Properties 213
HTTP Proxy Properties 215
Custom Properties 215
Operating System Profiles 215
Operating System Profile Components 216
Configuring Operating System Profiles 216
Troubleshooting Operating System Profiles 217
Associated Repository for the PowerCenter Integration Service 217
PowerCenter Integration Service Processes 218
Code Pages 218
Directories for PowerCenter Integration Service Files 218
Directories for Java Components 219
General Properties 220
Custom Properties 221
Environment Variables 221

Chapter 16: PowerCenter Integration Service Architecture 223

PowerCenter Integration Service Architecture Overview 223
PowerCenter Integration Service Connectivity 224
PowerCenter Integration Service Process 224
Load Balancer 226
Dispatch Process 226
Resources 227
Resource Provision Thresholds 227
Dispatch Mode 228

Service Levels. . . . 228
Data Transformation Manager (DTM) Process. . . . 229
Processing Threads. . . . 230
Thread Types. . . . 231
Pipeline Partitioning. . . . 232
DTM Processing. . . . 233
Reading Source Data. . . . 233
Blocking Data. . . . 233
Block Processing. . . . 234
Grids. . . . 234
Workflow on a Grid. . . . 234
Session on a Grid. . . . 235
System Resources. . . . 236
CPU Usage. . . . 236
DTM Buffer Memory. . . . 237
Cache Memory. . . . 237
Code Pages and Data Movement Modes. . . . 238
ASCII Data Movement Mode. . . . 238
Unicode Data Movement Mode. . . . 238
Output Files and Caches. . . . 238
Workflow Log. . . . 239
Session Log. . . . 240
Session Details 240
Performance Detail File. . . . 240
Reject Files. . . . 240
Row Error Logs. . . . 240
Recovery Tables Files. . . . 241
Control File. . . . 241
Email. . . . 241
Indicator File. . . . 241
Output File. . . . 241
Cache Files. . . . 242

Chapter 17: Model Repository Service. . . . 243

Model Repository Service Overview. . . . 243
Model Repository Architecture. . . . 243
Model Repository Schema. . . . 244
Model Repository Connectivity. . . . 244
Model Repository Database Requirements. . . . 245
IBM DB2 Database Requirements. . . . 246
IBM DB2 Version 9.1. . . . 246
Microsoft SQL Server Database Requirements. . . . 247
Oracle Database Requirements. . . . 247

Model Repository Service Status. 247
Enabling, Disabling, and Recycling the Model Repository Service. 247
Properties for the Model Repository Service. 248
General Properties for the Model Repository Service. 248
Repository Database Properties for the Model Repository Service. 248
Search Properties for the Model Repository Service. 249
Advanced Properties for the Model Repository Service. 249
Cache Properties for the Model Repository Service. 250
Custom Properties for the Model Repository Service. 250
Properties for the Model Repository Service Process. 250
Node Properties for the Model Repository Service Process. 250
Model Repository Service Management. 252
Content Management for the Model Repository Service 253
Model Repository Backup and Restoration. 253
Security Management for the Model Repository Service. 254
Search Management for the Model Repository Service 254
Repository Log Management for the Model Repository Service. 255
Audit Log Management for Model Repository Service 256
Cache Management for the Model Repository Service. 256
Creating a Model Repository Service. 257

Chapter 18: PowerCenter Repository Service. 258

PowerCenter Repository Service Overview. 258
Creating a Database for the PowerCenter Repository. 259
Creating the PowerCenter Repository Service. 259
Before You Begin. 259
Creating a PowerCenter Repository Service. 259
Database Connect Strings. 261
PowerCenter Repository Service Configuration. 262
Node Assignments. 262
General Properties. 262
Repository Properties. 262
Database Properties. 263
Advanced Properties. 264
Metadata Manager Service Properties. 266
Custom Properties. 266
PowerCenter Repository Service Process Configuration. 266
Custom Properties. 267
Environment Variables. 267

Chapter 19: PowerCenter Repository Management. 268

PowerCenter Repository Management Overview. 268
PowerCenter Repository Service and Service Processes. 269

Enabling and Disabling a PowerCenter Repository Service. . . . 269
Enabling and Disabling PowerCenter Repository Service Processes. . . . 270
Operating Mode. . . . 271
Running a PowerCenter Repository Service in Exclusive Mode. . . . 271
Running a PowerCenter Repository Service in Normal Mode. . . . 272
PowerCenter Repository Content. . . . 272
Creating PowerCenter Repository Content. . . . 272
Deleting PowerCenter Repository Content. . . . 273
Upgrading PowerCenter Repository Content. . . . 273
Enabling Version Control. . . . 273
Managing a Repository Domain. . . . 274
Prerequisites for a PowerCenter Repository Domain. . . . 274
Building a PowerCenter Repository Domain. . . . 275
Promoting a Local Repository to a Global Repository. . . . 275
Registering a Local Repository. . . . 276
Viewing Registered Local and Global Repositories. . . . 277
Moving Local and Global Repositories. . . . 277
Managing User Connections and Locks. . . . 277
Viewing Locks. . . . 278
Viewing User Connections. . . . 278
Closing User Connections and Releasing Locks. . . . 279
Sending Repository Notifications. . . . 280
Backing Up and Restoring the PowerCenter Repository. . . . 280
Backing Up a PowerCenter Repository. . . . 280
Viewing a List of Backup Files. . . . 281
Restoring a PowerCenter Repository. . . . 281
Copying Content from Another Repository. . . . 282
Repository Plug-in Registration. . . . 283
Registering a Repository Plug-in. . . . 283
Unregistering a Repository Plug-in. . . . 283
Audit Trails. . . . 284
Repository Performance Tuning. . . . 284
Repository Statistics. . . . 284
Repository Copy, Backup, and Restore Processes. . . . 284

Chapter 20: PowerExchange Listener Service. . . . 285

PowerExchange Listener Service Overview. . . . 285
Listener Service Restart and Failover. . . . 286
DBMOVER Statements for the Listener Service. . . . 286
Properties of the Listener Service. . . . 287
PowerExchange Listener Service General Properties. . . . 287
PowerExchange Listener Service Configuration Properties. . . . 288
Listener Service Management. . . . 288

Configuring Listener Service General Properties. . . . 288
Configuring Listener Service Configuration Properties. . . . 289
Configuring the Listener Service Process Properties. . . . 289
Service Status of the Listener Service. . . . 289
Enabling the Listener Service. . . . 289
Disabling the Listener Service. . . . 289
Restarting the Listener Service. . . . 290
Listener Service Logs. . . . 290
Creating a Listener Service. . . . 290

Chapter 21: PowerExchange Logger Service. . . . 291

PowerExchange Logger Service Overview. . . . 291
Logger Service Restart and Failover. . . . 292
Configuration Statements for the Logger Service. . . . 292
Properties of the PowerExchange Logger Service. . . . 293
PowerExchange Logger Service General Properties. . . . 293
PowerExchange Logger Service Configuration Properties. . . . 293
Logger Service Management. . . . 294
Configuring Logger Service General Properties. . . . 294
Configuring Logger Service Configuration Properties. . . . 294
Configuring the Logger Service Process Properties. . . . 295
Service Status of the Logger Service. . . . 295
Enabling the Logger Service. . . . 295
Disabling the Logger Service. . . . 295
Restarting the Logger Service. . . . 295
Logger Service Logs. . . . 296
Creating a Logger Service. . . . 296

Chapter 22: Reporting Service. . . . 297

Reporting Service Overview. . . . 297
PowerCenter Repository Reports. . . . 298
Metadata Manager Repository Reports. . . . 298
Data Profiling Reports. . . . 298
Other Reporting Sources. . . . 298
Data Analyzer Repository. . . . 299
Creating the Reporting Service. . . . 299
Managing the Reporting Service. . . . 301
Configuring the Edit Mode. . . . 302
Enabling and Disabling a Reporting Service. . . . 302
Creating Contents in the Data Analyzer Repository. . . . 303
Backing Up Contents of the Data Analyzer Repository. . . . 303
Restoring Contents to the Data Analyzer Repository. . . . 303
Deleting Contents from the Data Analyzer Repository. . . . 304

Upgrading Contents of the Data Analyzer Repository. . . . 304
Viewing Last Activity Logs. . . . 304
Configuring the Reporting Service. . . . 304
General Properties. . . . 305
Reporting Service Properties. . . . 305
Data Source Properties. . . . 306
Repository Properties. . . . 307
Granting Users Access to Reports. . . . 307

Chapter 23: SAP BW Service. . . . 308

SAP BW Service Overview. . . . 308
Load Balancing for the SAP NetWeaver BI System and the SAP BW Service. . . . 308
Creating the SAP BW Service. . . . 309
Enabling and Disabling the SAP BW Service. . . . 310
Enabling the SAP BW Service. . . . 310
Disabling the SAP BW Service. . . . 310
Configuring the SAP BW Service Properties. . . . 311
General Properties. . . . 311
SAP BW Service Properties. . . . 311
Configuring the Associated Integration Service. . . . 312
Configuring the SAP BW Service Processes. . . . 312
Viewing Log Events. . . . 313

Chapter 24: Web Services Hub. . . . 314

Web Services Hub Overview. . . . 314
Creating a Web Services Hub. . . . 315
Enabling and Disabling the Web Services Hub. . . . 316
Configuring the Web Services Hub Properties. . . . 317
General Properties. . . . 318
Service Properties. . . . 318
Advanced Properties. . . . 319
Custom Properties. . . . 320
Configuring the Associated Repository. . . . 321
Adding an Associated Repository. . . . 321
Editing an Associated Repository. . . . 322

Chapter 25: Connection Management. . . . 323

Connection Management Overview. . . . 323
Tools Reference for Creating and Managing Connections. . . . 323
Connection Pooling. . . . 324
Considerations for PowerExchange Connection Pooling. . . . 325
Creating a Connection. . . . 327
Configuring Pooling for a Connection. . . . 328

Viewing a Connection. . . . 329
Editing and Testing a Connection. . . . 329
Deleting a Connection. . . . 330
Connection Properties. . . . 330
Relational Database Connection Properties. . . . 330
DB2 for i5/OS Connection Properties. . . . 332
DB2 for z/OS Connection Properties. . . . 334
Nonrelational Database Connection Properties. . . . 336
Rules and Guidelines to Update Connection Properties. . . . 338
Pooling Properties. . . . 338

Chapter 26: Domain Object Export and Import. . . . 339

Domain Object Export and Import Overview. . . . 339
Export Process. . . . 340
Rules and Guidelines for Exporting Domain Objects. . . . 340
View Domain Objects. . . . 340
Viewable Domain Object Names. . . . 341
Import Process. . . . 347
Rules and Guidelines for Importing Domain Objects. . . . 347
Conflict Resolution. . . . 347

Chapter 27: Managing the Grid. . . . 348

Managing the Grid Overview. . . . 348
Configuring the Grid. . . . 348
Configuring the PowerCenter Integration Service. . . . 349
Configuring the PowerCenter Integration Service to Run on a Grid. . . . 349
Configuring the Service Processes. . . . 349
Configuring Resources. . . . 350
Viewing Resources in a Domain. . . . 351
Assigning Connection Resources. . . . 351
Defining Custom and File/Directory Resources. . . . 351
Troubleshooting the Grid. . . . 352

Chapter 28: Load Balancer. . . . 353

Load Balancer Overview. . . . 353
Configuring the Dispatch Mode. . . . 354
Round-Robin Dispatch Mode. . . . 354
Metric-Based Dispatch Mode. . . . 354
Adaptive Dispatch Mode. . . . 355
Service Levels. . . . 355
Creating Service Levels. . . . 356
Configuring Resources. . . . 356
Calculating the CPU Profile. . . . 357

Defining Resource Provision Thresholds. 357

Chapter 29: License Management. 359

License Management Overview. 359
License Validation. 360
Licensing Log Events. 360
License Management Tasks. 360
Types of License Keys. 361
Original Keys. 361
Incremental Keys. 361
Creating a License Object. 361
Assigning a License to a Service. 362
Rules and Guidelines for Assigning a License to a Service. 363
Unassigning a License from a Service. 363
Updating a License. 363
Removing a License. 364
License Properties. 364
License Details. 365
Supported Platforms. 366
Repositories. 366
PowerCenter Options. 366
Connections. 367
Metadata Exchange Options. 367

Chapter 30: Log Management. 368

Log Management Overview. 368
Log Manager Architecture. 369
Log Manager Recovery. 369
Troubleshooting the Log Manager. 370
Log Location. 370
Log Management Configuration. 370
Purging Log Events. 371
Time Zone. 371
Configuring Log Management Properties. 371
Using the Logs Tab. 372
Viewing Log Events. 372
Configuring Log Columns. 374
Saving Log Events. 374
Exporting Log Events. 375
Viewing Administrator Tool Log Errors. 376
Log Events. 376
Log Event Components. 377
Domain Log Events. 377

Analyst Service Log Events. . . . 378
Data Integration Service Log Events. . . . 378
Listener Service Log Events. . . . 378
Logger Service Log Events. . . . 379
Model Repository Service Log Events. . . . 379
Metadata Manager Service Log Events. . . . 379
PowerCenter Integration Service Log Events. . . . 379
PowerCenter Repository Service Log Events. . . . 380
Reporting Service Log Events. . . . 380
SAP BW Service Log Events. . . . 380
Web Services Hub Log Events. . . . 381
User Activity Log Events. . . . 381

Chapter 31: Monitoring. . . . 382

Monitoring Overview. . . . 382
Navigator in the Monitoring Tab. . . . 383
Views in the Monitoring Tab. . . . 383
Statistics in the Monitoring Tab. . . . 384
Reports in the Monitoring Tab. . . . 385
Monitoring Setup. . . . 386
Step 1. Configure Global Settings. . . . 386
Step 2. Configure Monitoring Preferences. . . . 387
Monitor Data Integration Services 388
Properties View for a Data Integration Service. . . . 388
Reports View for a Data Integration Service. . . . 389
Monitor Jobs. . . . 389
Viewing Logs for a Job. . . . 389
Viewing the Context of a Job. . . . 390
Canceling a Job. . . . 390
Monitor Applications. . . . 390
Properties View for an Application. . . . 390
Reports View for an Application. . . . 391
Monitor Deployed Mapping Jobs. . . . 391
Viewing Logs for a Deployed Mapping Job. . . . 391
Reissuing a Deployed Mapping Job. . . . 392
Canceling a Deployed Mapping Job. . . . 392
Monitor SQL Data Services. . . . 392
Properties View for an SQL Data Service. . . . 393
Connections View for an SQL Data Service. . . . 393
Requests View for an SQL Data Service. . . . 394
Virtual Tables View for an SQL Data Service. . . . 394
Reports View for an SQL Data Service. . . . 395
Monitor Web Services. . . . 395

Properties View for a Web Service. . . . 396
Reports View for a Web Service. . . . 396
Operations View for a Web Service. . . . 396
Requests View for a Web Service. . . . 397
Monitor Logical Data Objects. . . . 397
Properties View for a Logical Data Object. . . . 397
Cache Refresh Runs View for a Logical Data Object. . . . 397
Viewing Logs for Data Object Cache Refresh Runs. . . . 397
Monitoring a Folder of Objects. . . . 398
Configuring the Date and Time Custom Filter. . . . 398
Configuring the Elapsed Time Custom Filter. . . . 398
Configuring the Multi-Select Custom Filter. . . . 398
Monitoring an Object. . . . 399

Chapter 32: Domain Reports. . . . 400

Domain Reports Overview. . . . 400
License Management Report. . . . 400
Licensing. . . . 401
CPU Summary. . . . 401
CPU Detail. . . . 402
Repository Summary. . . . 402
User Summary. . . . 403
User Detail. . . . 403
Hardware Configuration. . . . 404
Node Configuration. . . . 404
Licensed Options. . . . 405
Running the License Management Report. . . . 405
Sending the License Management Report in an Email. . . . 406
Web Services Report. . . . 407
Understanding the Web Services Report. . . . 407
General Properties and Web Services Hub Summary. . . . 408
Web Services Historical Statistics. . . . 409
Web Services Run-time Statistics. . . . 409
Web Service Properties. . . . 410
Web Service Top IP Addresses. . . . 410
Web Service Historical Statistics Table. . . . 410
Running the Web Services Report. . . . 411
Running the Web Services Report for a Secure Web Services Hub. . . . 411

Chapter 33: Node Diagnostics. . . . 413

Node Diagnostics Overview. . . . 413
Customer Support Portal Login. . . . 414
Logging In to the Customer Support Portal. . . . 414

Generating Node Diagnostics. 415
Downloading Node Diagnostics. 415
Uploading Node Diagnostics. 416
Analyzing Node Diagnostics. 417
Identify Bug Fixes. 417
Identify Recommendations. 417

Chapter 34: Understanding Globalization. 418

Globalization Overview. 418
Unicode. 419
Working with a Unicode PowerCenter Repository. 419
Locales. 420
System Locale. 420
User Locale. 420
Input Locale. 421
Data Movement Modes. 421
Character Data Movement Modes. 421
Changing Data Movement Modes. 422
Code Page Overview. 423
UNIX Code Pages. 423
Windows Code Pages. 424
Choosing a Code Page. 424
Code Page Compatibility. 424
Domain Configuration Database Code Page. 426
Administrator Tool Code Page. 426
PowerCenter Client Code Page. 426
PowerCenter Integration Service Process Code Page. 427
PowerCenter Repository Code Page. 427
Metadata Manager Repository Code Page. 428
PowerCenter Source Code Page. 428
PowerCenter Target Code Page. 428
Command Line Program Code Pages. 429
Code Page Compatibility Summary. 430
Code Page Validation. 431
Relaxed Code Page Validation. 432
Configuring the PowerCenter Integration Service. 432
Selecting Compatible Source and Target Code Pages. 433
Troubleshooting for Code Page Relaxation. 433
PowerCenter Code Page Conversion. 433
Choosing Characters for PowerCenter Repository Metadata. 434
Case Study: Processing ISO 8859-1 Data. 434
Configuring the ISO 8859-1 Environment. 435
Case Study: Processing Unicode UTF-8 Data. 436

Configuring the UTF-8 Environment. 437

Appendix A: Code Pages. 440

Supported Code Pages for Application Services. 440

Supported Code Pages for Sources and Targets. 442

Appendix B: Command Line Privileges and Permissions. 452

infacmd as Commands. 452

infacmd dis Commands. 453

infacmd ipc Commands. 454

infacmd isp Commands. 454

infacmd mrs Commands. 464

infacmd ms Commands. 465

infacmd oie Commands. 465

infacmd ps Commands. 465

infacmd pwx Commands. 466

infacmd rtm Commands. 467

infacmd sql Commands. 467

pmcmd Commands. 468

pmrep Commands. 470

Appendix C: Custom Roles. 475

PowerCenter Repository Service Custom Roles. 475

Metadata Manager Service Custom Roles. 476

Reporting Service Custom Roles. 477

Appendix D: Repository Database Configuration for PowerCenter 482

Repository Database Configuration Overview. 482

Guidelines for Setting Up Database User Accounts. 482

PowerCenter Repository Database Requirements. 483

Oracle. 483

IBM DB2. 483

Sybase ASE. 483

Data Analyzer Repository Database Requirements. 484

Oracle. 484

Microsoft SQL Server. 484

Sybase ASE. 485

Metadata Manager Repository Database Requirements. 485

Oracle. 485

IBM DB2 486

Microsoft SQL Server. 486

Appendix E: PowerCenter Platform Connectivity 487

Connectivity Overview. 487
Domain Connectivity. 488
PowerCenter Connectivity. 488
Repository Service Connectivity. 489
Integration Service Connectivity. 490
PowerCenter Client Connectivity. 491
Reporting Service and Metadata Manager Service Connectivity. 492
Native Connectivity. 492
ODBC Connectivity. 492
JDBC Connectivity. 493

Appendix F: Connecting to Databases in PowerCenter from Windows 495

Connecting to Databases from Windows Overview. 495
Connecting to an IBM DB2 Universal Database. 495
Configuring Native Connectivity. 496
Configuring ODBC Connectivity. 496
Connecting to Microsoft Access and Microsoft Excel. 496
Configuring ODBC Connectivity. 497
Connecting to a Microsoft SQL Server Database. 497
Configuring Native Connectivity. 497
Configuring ODBC Connectivity. 497
Connecting to an Oracle Database. 498
Configuring Native Connectivity. 498
Configuring ODBC Connectivity. 499
Connecting to a Sybase ASE Database. 499
Configuring Native Connectivity. 499
Configuring ODBC Connectivity. 500
Connecting to a Teradata Database. 500
Configuring ODBC Connectivity. 501
Connecting to a Neoview Database. 501
Configuring ODBC Connectivity. 502
Connecting to a Netezza Database. 502
Configuring ODBC Connectivity. 503

Appendix G: Connecting to Databases in PowerCenter from UNIX 504

Connecting to Databases from UNIX Overview. 504
Connecting to Microsoft SQL Server. 505
Connecting to an IBM DB2 Universal Database. 505
Configuring Native Connectivity. 505
Connecting to an Informix Database. 507
Configuring Native Connectivity. 507

Connecting to an Oracle Database. 509
Configuring Native Connectivity. 509
Connecting to a Sybase ASE Database. 512
Configuring Native Connectivity. 512
Connecting to a Teradata Database. 513
Configuring ODBC Connectivity. 514
Connecting to a Neoview Database. 516
Configuring ODBC Connectivity. 516
Connecting to a Netezza Database. 518
Configuring ODBC Connectivity. 518
Connecting to an ODBC Data Source. 521
Sample odbc.ini File. 523

Index. 526

Preface

The *Informatica Administrator Guide* is written for Informatica users. It contains information you need to manage the domain and security. The *Informatica Administrator Guide* assumes you have basic working knowledge of Informatica.

Informatica Resources

Informatica Customer Portal

As an Informatica customer, you can access the Informatica Customer Portal site at http://mysupport.informatica.com. 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, the Informatica Multimedia 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 Multimedia Knowledge Base

As an Informatica customer, you can access the Informatica Multimedia Knowledge Base at http://mysupport.informatica.com. The Multimedia Knowledge Base is a collection of instructional multimedia files that help you learn about common concepts and guide you through performing specific tasks. If you have questions, comments, or ideas about the Multimedia Knowledge Base, contact the Informatica Knowledge Base team through email at KB_Feedback@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.

Use the following telephone numbers to contact Informatica Global Customer Support:

North America / South America	Europe / Middle East / Africa	Asia / Australia
Toll Free Brazil: 0800 891 0202 Mexico: 001 888 209 8853 North America: +1 877 463 2435 **Standard Rate** North America: +1 650 653 6332	**Toll Free** France: 00800 4632 4357 Germany: 00800 4632 4357 Israel: 00800 4632 4357 Italy: 800 915 985 Netherlands: 00800 4632 4357 Portugal: 800 208 360 Spain: 900 813 166 Switzerland: 00800 4632 4357 or 0800 463 200 United Kingdom: 00800 4632 4357 or 0800 023 4632 **Standard Rate** France: 0805 804632 Germany: 01805 702702 Netherlands: 030 6022 797	**Toll Free** Australia: 1 800 151 830 New Zealand: 1 800 151 830 Singapore: 001 800 4632 4357 **Standard Rate** India: +91 80 4112 5738

CHAPTER 1

Understanding Domains

This chapter includes the following topics:

- Understanding Domains Overview, 1
- Nodes, 2
- Service Manager, 2
- Application Services, 3
- User Security, 6
- High Availability, 8

Understanding Domains Overview

Informatica has a service-oriented architecture that provides the ability to scale services and share resources across multiple machines. High availability functionality helps minimize service downtime due to unexpected failures or scheduled maintenance in the Informatica environment.

The Informatica domain is the fundamental administrative unit in Informatica. The domain supports the administration of the distributed services. A domain is a collection of nodes and services that you can group in folders based on administration ownership.

A node is the logical representation of a machine in a domain. One node in the domain acts as a gateway to receive service requests from clients and route them to the appropriate service and node. Services and processes run on nodes in a domain. The availability of a service or process on a node depends on how you configure the service and the node.

Services for the domain include the Service Manager and a set of application services:

- Service Manager. A service that manages all domain operations. It runs the application services and performs domain functions on each node in the domain. Some domain functions include authentication, authorization, and logging.
- Application Services. Services that represent server-based functionality, such as the Model Repository Service and the Data Integration Service. The application services that run on a node depend on the way you configure the services.

The Service Manager and application services control security. The Service Manager manages users and groups that can log in to application clients and authenticates the users who log in to the application clients. The Service Manager and application services authorize user requests from application clients.

Informatica Administrator (the Administrator tool), consolidates the administrative tasks for domain objects such as services, nodes, licenses, and grids. You manage the domain and the security of the domain through the Administrator tool.

If you have the PowerCenter high availability option, you can scale services and eliminate single points of failure for services. Services can continue running despite temporary network or hardware failures.

Nodes

During installation, you add the installation machine to the domain as a node. You can add multiple nodes to a domain. Each node in the domain runs a Service Manager that manages domain operations on that node. The operations that the Service Manager performs depend on the type of node. A node can be a gateway node or a worker node. You can subscribe to alerts to receive notification about node events such as node failure or a master gateway election. You can also generate and upload node diagnostics to the Configuration Support Manager and review information such as available EBFs and Informatica recommendations.

Gateway Nodes

A gateway node is any node that you configure to serve as a gateway for the domain. One node acts as the gateway at any given time. That node is called the master gateway. A gateway node can run application services, and it can serve as a master gateway node. The master gateway node is the entry point to the domain.

The Service Manager on the master gateway node performs all domain operations on the master gateway node. The Service Managers running on other gateway nodes perform limited domain operations on those nodes.

You can configure more than one node to serve as a gateway. If the master gateway node becomes unavailable, the Service Manager on other gateway nodes elect another master gateway node. If you configure one node to serve as the gateway and the node becomes unavailable, the domain cannot accept service requests.

Worker Nodes

A worker node is any node not configured to serve as a gateway. A worker node can run application services, but it cannot serve as a gateway. The Service Manager performs limited domain operations on a worker node.

Service Manager

The Service Manager is a service that manages all domain operations. It runs within Informatica services. It runs as a service on Windows and as a daemon on UNIX. When you start Informatica services, you start the Service Manager. The Service Manager runs on each node. If the Service Manager is not running, the node is not available.

The Service Manager runs on all nodes in the domain to support application services and the domain:

- Application service support. The Service Manager on each node starts application services configured to run on that node. It starts and stops services and service processes based on requests from clients. It also directs service requests to application services. The Service Manager uses TCP/IP to communicate with the application services.
- Domain support. The Service Manager performs functions on each node to support the domain. The functions that the Service Manager performs on a node depend on the type of node. For example, the Service Manager running on the master gateway node performs all domain functions on that node. The Service Manager running on any other node performs some domain functions on that node.

The following table describes the domain functions that the Service Manager performs:

Function	Description
Alerts	The Service Manager sends alerts to subscribed users. You subscribe to alerts to receive notification for node failure and master gateway election on the domain, and for service process failover for services on the domain. When you subscribe to alerts, you receive notification emails.
Authentication	The Service Manager authenticates users who log in to application clients. Authentication occurs on the master gateway node.
Authorization	The Service Manager authorizes user requests for domain objects based on the privileges, roles, and permissions assigned to the user. Requests can come from the Administrator tool. Domain authorization occurs on the master gateway node. Some application services authorize user requests for other objects.
Domain Configuration	The Service Manager manages the domain configuration metadata. Domain configuration occurs on the master gateway node.
Node Configuration	The Service Manager manages node configuration metadata in the domain. Node configuration occurs on all nodes in the domain.
Licensing	The Service Manager registers license information and verifies license information when you run application services. Licensing occurs on the master gateway node.
Logging	The Service Manager provides accumulated log events from each service in the domain and for sessions and workflows. To perform the logging function, the Service Manager runs a Log Manager and a Log Agent. The Log Manager runs on the master gateway node. The Log Agent runs on all nodes where the PowerCenter Integration Service runs.
User Management	The Service Manager manages the native and LDAP users and groups that can log in to application clients. It also manages the creation of roles and the assignment of roles and privileges to native and LDAP users and groups. User management occurs on the master gateway node.
Monitoring	The Service Manager persists, updates, retrieves, and publishes run-time statistics for integration objects in the Model repository. The Service Manager stores the monitoring configuration in the Model repository.

Application Services

Application services represent server-based functionality. Application services include the following services:

- Analyst Service
- Content Management Service
- Data Integration Service
- Metadata Manager Service
- Model Repository Service
- PowerCenter Integration Service
- PowerCenter Repository Service
- PowerExchange Listener Service
- PowerExchange Logger Service

- Reporting Service
- SAP BW Service
- Web Services Hub

When you configure an application service, you designate a node to run the service process. When a service process runs, the Service Manager assigns a port number from the range of port numbers assigned to the node.

The service process is the runtime representation of a service running on a node. The service type determines how many service processes can run at a time. For example, the PowerCenter Integration Service can run multiple service processes at a time when you run it on a grid.

If you have the high availability option, you can run a service on multiple nodes. Designate the primary node to run the service. All other nodes are backup nodes for the service. If the primary node is not available, the service runs on a backup node. You can subscribe to alerts to receive notification in the event of a service process failover.

If you do not have the high availability option, configure a service to run on one node. If you assign multiple nodes, the service will not start.

Analyst Service

The Analyst Service is an application service that runs the Informatica Analyst application in the Informatica domain. The Analyst Service manages the connections between service components and the users that have access to Informatica Analyst. The Analyst Service has connections to a Data Integration Service, Model Repository Service, the Informatica Analyst application, staging database, and a flat file cache location.

You can use the Administrator tool to administer the Analyst Service. You can create and recycle an Analyst Service in the Informatica domain to access the Analyst tool. You can launch the Analyst tool from the Administrator tool.

Content Management Service

The Content Management Service is an application service that manages reference data. It provides reference data information to the Data Integration Service and to the Developer tool.

The Content Management Service provides reference data properties to the Data Integration Service. The Data Integration Service uses these properties when it runs mappings that require address reference data.

The Content Management Service also provides Developer tool transformations with information about the address reference data and identity populations installed in the file system. The Developer tool displays the installed address reference datasets in the Content Status view within application preferences. The Developer tool displays the installed identity populations in the Match transformation and Comparison transformation.

Data Integration Service

The Data Integration Service is an application service that performs data integration tasks for Informatica Analyst, Informatica Developer, and external clients.

When you preview or run data profiles, SQL data services, and mappings in Informatica Analyst or Informatica Developer, the application sends requests to the Data Integration Service to perform the data integration tasks. When you start a command from the command line or an external client to run SQL data services and mappings in an application, the command sends the request to the Data Integration Service.

Metadata Manager Service

The Metadata Manager Service is an application service that runs the Metadata Manager application and manages connections between the Metadata Manager components.

Use Metadata Manager to browse and analyze metadata from disparate source repositories. You can load, browse, and analyze metadata from application, business intelligence, data integration, data modelling, and relational metadata sources.

You can configure the Metadata Manager Service to run on only one node. The Metadata Manager Service is not a highly available service. However, you can run multiple Metadata Manager Services on the same node.

Model Repository Service

The Model Repository Service is an application service that manages the Model repository. The Model repository is a relational database that stores the metadata for projects created in Informatica Analyst and Informatica Designer. The Model repository also stores run-time and configuration information for applications that are deployed to a Data Integration Service.

You can configure the Model Repository Service to run on one node. The Model Repository Service is not a highly available service. However, you can run multiple Model Repository Services on the same node. If the Model Repository Service fails, it automatically restarts on the same node.

PowerCenter Integration Service

The PowerCenter Integration Service runs PowerCenter sessions and workflows. When you configure the PowerCenter Integration Service, you can specify where you want it to run:

- On a grid. When you configure the service to run on a grid, it can run on multiple nodes at a time. The PowerCenter Integration Service dispatches tasks to available nodes assigned to the grid. If you do not have the high availability option, the task fails if any service process or node becomes unavailable. If you have the high availability option, failover and recovery is available if a service process or node becomes unavailable.
- On nodes. If you have the high availability option, you can configure the service to run on multiple nodes. By default, it runs on the primary node. If the primary node is not available, it runs on a backup node. If the service process fails or the node becomes unavailable, the service fails over to another node. If you do not have the high availability option, you can configure the service to run on one node.

PowerCenter Repository Service

The PowerCenter Repository Service manages the PowerCenter repository. It retrieves, inserts, and updates metadata in the repository database tables. If the service process fails or the node becomes unavailable, the service fails.

If you have the high availability option, you can configure the service to run on primary and backup nodes. By default, the service process runs on the primary node. If the service process fails, a new process starts on the same node. If the node becomes unavailable, a service process starts on one of the backup nodes.

PowerExchange Listener Service

The PowerExchange Listener Service is an application service that manages the PowerExchange Listener. The PowerExchange Listener manages communication between a PowerCenter or PowerExchange client and a data source for bulk data movement and change data capture. The PowerCenter Integration Service connects to the PowerExchange Listener through the Listener Service. Use the Administrator tool to manage the service and view service logs.

If you have the PowerCenter high availability option, you can run the Listener Service on multiple nodes. If the Listener Service process fails on the primary node, it fails over to a backup node.

PowerExchange Logger Service

The Logger Service is an application service that manages the PowerExchange Logger for Linux, UNIX, and Windows. The PowerExchange Logger captures change data from a data source and writes the data to PowerExchange Logger log files. Use the Admnistrator tool to manage the service and view service logs.

If you have the PowerCenter high availability option, you can run the Logger Service on multiple nodes. If the Logger Service process fails on the primary node, it fails over to a backup node.

Reporting Service

The Reporting Service is an application service that runs the Data Analyzer application in an Informatica domain. You log in to Data Analyzer to create and run reports on data in a relational database or to run the following PowerCenter reports: PowerCenter Repository Reports, Data Profiling Reports, or Metadata Manager Reports. You can also run other reports within your organization.

The Reporting Service is not a highly available service. However, you can run multiple Reporting Services on the same node.

Configure a Reporting Service for each data source you want to run reports against. If you want a Reporting Service to point to different data sources, create the data sources in Data Analyzer.

SAP BW Service

The SAP BW Service listens for RFC requests from SAP NetWeaver BI and initiates workflows to extract from or load to SAP NetWeaver BI. The SAP BW Service is not highly available. You can configure it to run on one node.

Web Services Hub

The Web Services Hub receives requests from web service clients and exposes PowerCenter workflows as services. The Web Services Hub does not run an associated service process. It runs within the Service Manager.

User Security

The Service Manager and some application services control user security in application clients. Application clients include Data Analyzer, Informatica Administrator, Informatica Analyst, Informatica Developer, Metadata Manager, and PowerCenter Client.

The Service Manager and application services control user security by performing the following functions:

Encryption

When you log in to an application client, the Service Manager encrypts the password.

Authentication

When you log in to an application client, the Service Manager authenticates your user account based on your user name and password or on your user authentication token.

Authorization

When you request an object in an application client, the Service Manager and some application services authorize the request based on your privileges, roles, and permissions.

Encryption

Informatica encrypts passwords sent from application clients to the Service Manager. Informatica uses AES encryption with multiple 128-bit keys to encrypt passwords and stores the encrypted passwords in the domain configuration database. Configure HTTPS to encrypt passwords sent to the Service Manager from application clients.

Authentication

The Service Manager authenticates users who log in to application clients.

The first time you log in to an application client, you enter a user name, password, and security domain. A security domain is a collection of user accounts and groups in an Informatica domain.

The security domain that you select determines the authentication method that the Service Manager uses to authenticate your user account:

- Native. When you log in to an application client as a native user, the Service Manager authenticates your user name and password against the user accounts in the domain configuration database.
- Lightweight Directory Access Protocol (LDAP). When you log in to an application client as an LDAP user, the Service Manager passes your user name and password to the external LDAP directory service for authentication.

Single Sign-On

After you log in to an application client, the Service Manager allows you to launch another application client or to access multiple repositories within the application client. You do not need to log in to the additional application client or repository.

The first time the Service Manager authenticates your user account, it creates an encrypted authentication token for your account and returns the authentication token to the application client. The authentication token contains your user name, security domain, and an expiration time. The Service Manager periodically renews the authentication token before the expiration time.

When you launch one application client from another one, the application client passes the authentication token to the next application client. The next application client sends the authentication token to the Service Manager for user authentication.

When you access multiple repositories within an application client, the application client sends the authentication token to the Service Manager for user authentication.

Authorization

The Service Manager authorizes user requests for domain objects. Requests can come from the Administrator tool. The following application services authorize user requests for other objects:

- Data Integration Service
- Metadata Manager Service
- Model Repository Service
- PowerCenter Repository Service

- Reporting Service

When you create native users and groups or import LDAP users and groups, the Service Manager stores the information in the domain configuration database into the following repositories:

- Data Analyzer repository
- Model repository
- PowerCenter repository
- PowerCenter repository for Metadata Manager

The Service Manager synchronizes the user and group information between the repositories and the domain configuration database when the following events occur:

- You restart the Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service.
- You add or remove native users or groups.
- The Service Manager synchronizes the list of LDAP users and groups in the domain configuration database with the list of users and groups in the LDAP directory service.

When you assign permissions to users and groups in an application client, the application service stores the permission assignments with the user and group information in the appropriate repository.

When you request an object in an application client, the appropriate application service authorizes your request. For example, if you try to edit a project in Informatica Developer, the Model Repository Service authorizes your request based on your privilege, role, and permission assignments.

High Availability

High availability is an option that eliminates a single point of failure in a domain and provides minimal service interruption in the event of failure. High availability consists of the following components:

- Resilience. The ability of application services to tolerate transient network failures until either the resilience timeout expires or the external system failure is fixed.
- Failover. The migration of an application service or task to another node when the node running the service process becomes unavailable.
- Recovery. The automatic completion of tasks after a service is interrupted. Automatic recovery is available for PowerCenter Integration Service and PowerCenter Repository Service tasks. You can also manually recover PowerCenter Integration Service workflows and sessions. Manual recovery is not part of high availability.

CHAPTER 2

Managing Your Account

This chapter includes the following topics:

- Managing Your Account Overview, 9
- Logging In, 9
- Changing Your Password, 10
- Editing Preferences, 11
- Preferences, 11

Managing Your Account Overview

Manage your account to change your password or edit user preferences.

If you have a native user account, you can change your password at any time. If someone else created your user account, change your password the first time you log in to the Administrator tool.

The Service Manager uses the user password associated with a worker node to authenticate the node in the domain. If you change a user password that is associated with one or more worker nodes, the Service Manager updates the password for each worker node. The Service Manager cannot update nodes that are not running. For nodes that are not running, the Service Manager updates the password when the nodes restart.

Note: For an LDAP user account, change the password in the LDAP directory service.

User preferences control the options that appear in the Administrator tool when you log in. User preferences do not affect the options that appear when another user logs in to the Administrator tool.

Logging In

To log in to the Administrator tool, you must have a user account and the Access Informatica Administrator domain privilege.

1. Open Microsoft Internet Explorer or Mozilla Firefox.
2. In the Address field, enter the following URL for the Administrator tool login page:

   ```
   http://<host>:<port>/administrator
   ```

   The Administrator tool login page appears.
3. Enter the user name and password.

4. If the Informatica domain contains an LDAP security domain, select **Native** or the name of a specific security domain.

   The **Security Domain** box appears when the Informatica domain contains an LDAP security domain. If you do not know the security domain to which your user account belongs, contact the Informatica domain administrator.

5. Click **Log In**.

Informatica Administrator URL

In the Administrator tool URL, `<host>:<port>` represents the host name of the master gateway node and the Administrator tool port number.

You configure the Administrator tool port when you define the domain. You can define the domain during installation or by running the *infasetup* DefineDomain command line program. If you enter the domain port instead of the Administrator tool port in the URL, the browser is directed to the Administrator tool port.

If you do not use the Internet Explorer Enhanced Security Configuration, you can enter the following URL, and the browser is directed to the full URL for the login page:

```
http://<host>:<port>
```

If you configure HTTPS for the Administrator tool, the URL redirects to the following HTTPS enabled site:

```
https://<host>:<https port>/administrator
```

If the node is configured for HTTPS with a keystore that uses a self-signed certificate, a warning message appears. To enter the site, accept the certificate.

Note: If the domain fails over to a different master gateway node, the host name in the Administrator tool URL is equal to the host name of the elected master gateway node.

Changing Your Password

Change the password for a native user account at any time. For a user account created by someone else, change the password the first time you log in to the Administrator tool.

1. In the Administrator tool header area, click **Manage** > **Change Password**.

   The **Change Password** dialog box appears.

2. In the **Change Password** dialog box, enter the current password in the **Current Password** box, and the new password in the **New Password** and **Confirm New Password** boxes.

   Then, click **OK**.

   If you change a user password that is associated with one or more worker nodes, the Service Manager updates the password for each worker node. The Service Manager cannot update nodes that are not running. For nodes that are not running, the Service Manager updates the password when the nodes restart.

Editing Preferences

Edit your preferences to determine the options that appear in the Administrator tool when you log in.

1. In the Administrator tool header area, click **Manage** > **Preferences**.

   The **Preferences** window appears.

2. Click **Edit**.

   The **Edit Preferences** dialog box appears.

Preferences

Your preferences determine the options that appear in the Administrator tool when you log in. Your preferences do not affect the options that appear when another user logs in to the Administrator tool.

The following table describes the options that you can configure for your preferences:

Option	Description
Subscribe for Alerts	Subscribes you to domain and service alerts. You must have a valid email address configured for your user account. Default is No.
Show Custom Properties	Displays custom properties in the contents panel when you click an object in the Navigator. You use custom properties to configure Informatica behavior for special cases or to increase performance. Hide the custom properties to avoid inadvertently changing the values. Use custom properties only if Informatica Global Customer Support instructs you to.

CHAPTER 3

Using Informatica Administrator

This chapter includes the following topics:

- Using Informatica Administrator Overview, 12
- Domain Tab Overview, 13
- Domain Tab - Services and Nodes View, 13
- Domain Tab - Connections View, 19
- Logs Tab, 20
- Reports Tab, 20
- Monitoring Tab, 21
- Security Tab, 21

Using Informatica Administrator Overview

Informatica Administrator is the administration tool that you use to administer the Informatica domain and Informatica security.

Use the Administrator tool to complete the following types of tasks:

- Domain administrative tasks. Manage logs, domain objects, user permissions, and domain reports. Generate and upload node diagnostics. Monitor jobs and applications that run on the Data Integration Service. Domain objects include application services, nodes, grids, folders, database connections, operating system profiles, and licenses.
- Security administrative tasks. Manage users, groups, roles, and privileges.

The Administrator tool has the following tabs:

- **Domain**. View and edit the properties of the domain and objects within the domain.
- **Logs**. View log events for the domain and services within the domain.
- **Monitoring**. View the status of profile jobs, scorecard jobs, preview jobs, mapping jobs, and SQL data services for each Data Integration Service.
- **Reports**. Run a Web Services Report or License Management Report.
- **Security**. Manage users, groups, roles, and privileges.

The Administrator tool has the following header items:

- Log out. Log out of the Administrator tool.
- Manage. Manage your account.
- Help. Access help for the current tab.

Domain Tab Overview

On the **Domain** tab, you can view information about the domain and view and manage objects in the domain.

The contents that appear and the tasks you can complete on the **Domain** tab vary based on the view that you select. You can select the following views:

- **Services and Nodes**. View and manage application services and nodes.
- **Connections**. View and manage connections.

You can configure the appearance of these views.

Related Topics:

- "Domain Tab - Services and Nodes View" on page 13
- "Domain Tab - Connections View" on page 19

Domain Tab - Services and Nodes View

The **Services and Nodes** view shows all application services and nodes defined in the domain.

The **Services and Nodes** view has the following components:

Navigator

Appears in the left pane of the **Domain** tab. The Navigator displays the following types of objects:

- Domain. You can view one domain, which is the highest object in the Navigator hierarchy.
- Folders. Use folders to organize domain objects in the Navigator. Select a folder to view information about the folder and the objects in the folder.
- Application services. An application service represents server-based functionality. Select an application service to view information about the service and its processes.
- Nodes. A node represents a machine in the domain. You assign resources to nodes and configure service processes to run on nodes.
- Grids. Create a grid to run the PowerCenter Integration Service on multiple nodes. Select a grid to view nodes assigned to the grid.
- Licenses. Create a license on the **Domain** tab based on a license key file provided by Informatica. Select a license to view services assigned to the license.

Contents panel

Appears in the right pane of the **Domain** tab and displays information about the domain or domain object that you select in the Navigator.

Actions menu in the Navigator

When you select the domain in the Navigator, you can create a folder, service, node, grid, or license.

When you select a domain object in the Navigator, you can delete the object, move it to a folder, or refresh the object.

Actions menu on the Domain tab

When you select the domain in the Navigator, you shut down or view logs for the domain.

When you select a node in the Navigator, you can remove a node association, recalculate the CPU profile benchmark, or shut down the node.

When you select a service in the Navigator, you can recycle or disable the service, view back up files in or back up the repository contents, manage the repository domain, notify users, and view logs.

When you select a license in the Navigator, you can add an incremental key to the license.

Domain

You can view one domain in the **Services and Nodes** view on the **Domain** tab. It is the highest object in the Navigator hierarchy.

When you select the domain in the Navigator, the contents panel shows the following views and buttons, which enable you to complete the following tasks:

- **Overview** view. View an overview grid of all application services, nodes, and grids in the domain organized by object type. From this grid, you can view statuses of application services and nodes and information about grids. You can also view dependencies among application services, nodes, and grids, and view properties for objects. You can also recycle application services.

  Click an application service to see its name, version, status, and the statuses of its individual processes. Click a node to see its name, status, the number of service processes running on the node, and the name of any grids to which the node belongs. Click a grid to see the name of the grid, the number of service processes running in the grid, and the names of the nodes in the grid. The statuses are available, disabled, and unavailable.

  By default, each object in the grid shows an abbreviated version of its name. Click the **Show Details** button to show the full names of objects. Click the **Hide Details** button to show abbreviated versions of object names.

  To view the dependencies among application services, nodes, and grids, right-click an object and click **View Dependency**. The **View Dependency** graph appears.

  To view properties for an application service, node, or grid, right-click an object and click **View Properties**. The contents panel shows the object properties.

  To recycle an application service, right-click a service and click **Recycle Service**.
- **Properties** view. View or edit domain resilience properties.
- **Resources** view. View available resources for each node in the domain.
- **Permissions** view. View or edit group and user permissions on the domain.
- **Diagnostics** view. View node diagnostics, generate and upload node diagnostics to Customer Support Manager, or edit customer portal login details.
- View Logs for Domain button. View logs for the domain and services within the domain.

In the **Actions** menu in the Navigator, you can add a node, grid, application service, or license to the domain. You can also add folders, which you use to organize domain objects.

In the **Actions** menu on the **Domain** tab, you can shut down, view logs, or access help on the current view.

Related Topics:

- “Viewing Dependencies for Application Services, Nodes, and Grids” on page 42

Folders

You can use folders in the domain to organize objects and to manage security.

Folders can contain nodes, services, grids, licenses, and other folders.

When you select a folder in the Navigator, the Navigator opens to display the objects in the folder. The contents panel displays the following information:

- **Overview** view. Displays services in the folder and the nodes where the service processes run.
- **Properties** view. Displays the name and description of the folder.
- **Permissions** view. View or edit group and user permissions on the folder.

In the **Actions** menu in the Navigator, you can delete the folder, move the folder into another folder, refresh the contents on the **Domain** tab, or access help on the current tab.

Application Services

Application services are a group of services that represent Informatica server-based functionality.

In the **Services and Nodes** view on the **Domain** tab, you can create and manage the following application services:

Analyst Service

Runs Informatica Analyst in the Informatica domain. The Analyst Service manages the connections between service components and the users that have access to Informatica Analyst.

The Analyst Service connects to a Data Integration Service, Model Repository Service, Analyst tool, staging database, and a flat file cache location.

You can create and recycle the Analyst Service in the Informatica domain to access the Analyst tool. You can launch the Analyst tool from the Administrator tool.

When you select an Analyst Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The contents panel also displays the URL of the Analyst Service instance.
- **Properties** view. Manage general, model repository, data integration, metadata manager, staging database, logging, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Permissions** view. View or edit group and user permissions on the Analyst Service.
- **Actions** menu. Manage the service and repository contents.

Content Management Service

Manages reference data, provides the Data Integration Service with address reference data properties, and provides Informatica Developer with information about the address reference data and identity populations installed in the file system.

When you select a Content Management Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, data integration, logging, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Permissions** view. View or edit group and user permissions on the Content Management Service.
- **Actions** menu. Manage the service.

Data Integration Service

Completes data integration tasks for Informatica Analyst, Informatica Developer, and external clients. When you preview or run data profiles, SQL data services, and mappings in Informatica Analyst or Informatica

Developer, the application sends requests to the Data Integration Service to perform the data integration tasks. When you start a command from the command line or an external client to run SQL data services and mappings in an application, the command sends the request to the Data Integration Service.

When you select a Data Integration Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, model repository, logging, logical data object and virtual table cache, profiling, data object cache, and custom properties. Set the default deployment option.
- **Processes** view. View and edit service process properties on each assigned node.
- **Applications** view. Start and stop applications and SQL data services. Back up applications. Manage application properties.
- **Actions** menu. Manage the service and repository contents.

Metadata Manager Service

Runs the Metadata Manager application and manages connections between the Metadata Manager components.

When you select a Metadata Manager Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The contents panel also displays the URL of the Metadata Manager Service instance.
- **Properties** view. View or edit Metadata Manager properties.
- **Associated Services** view. View and configure the Integration Service associated with the Metadata Manager Service.
- **Permissions** view. View or edit group and user permissions on the Metadata Manager Service.
- **Actions** menu. Manage the service and repository contents.

Model Repository Service

Manages the Model repository. The Model repository stores metadata created by Informatica products, such as Informatica Developer, Informatica Analyst, Data Integration Service, and Informatica Administrator. The Model repository enables collaboration among the products.

When you select a Model Repository Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, repository database, search, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Actions** menu. Manage the service and repository contents.

PowerCenter Integration Service

Runs PowerCenter sessions and workflows. Select a PowerCenter Integration Service in the Navigator to access information about the service.

When you select a PowerCenter Integration Service in the Navigator, the contents panel displays the following information:

- Service and service processes status. View the status of the service and the service process for each node.

- **Properties** view. View or edit Integration Service properties.
- **Associated Repository** view. View or edit the repository associated with the Integration Service.
- **Processes** view. View or edit the service process properties on each assigned node.
- **Permissions** view. View or edit group and user permissions on the Integration Service.
- **Actions** menu. Manage the service.

PowerCenter Repository Service

Manages the PowerCenter repository. It retrieves, inserts, and updates metadata in the repository database tables. Select a PowerCenter Repository Service in the Navigator to access information about the service.

When you select a PowerCenter Repository Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The service status also displays the operating mode for the PowerCenter Repository Service. The contents panel also displays a message if the repository has no content or requires upgrade.
- **Properties** view. Manage general and advanced properties, node assignments, and database properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Connections and Locks** view. View and terminate repository connections and object locks.
- **Plug-ins** view. View and manage registered plug-ins.
- **Permissions** view. View or edit group and user permissions on the PowerCenter Repository Service.
- **Actions** menu. Manage the contents of the repository and perform other administrative tasks.

PowerExchange Listener Service

Runs the PowerExchange Listener.

When you select a Listener Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the PowerExchange Listener instance.
- **Properties** view. View or edit Listener Service properties.
- **Actions** menu. Contains actions that you can perform on the Listener Service, such as viewing logs or enabling and disabling the service.

PowerExchange Logger Service

Runs the PowerExchange Logger for Linux, UNIX, and Windows.

When you select a Logger Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the PowerExchange Logger instance.
- **Properties** view. View or edit Logger Service properties.
- **Actions** menu. Contains actions that you can perform on the Logger Service, such as viewing logs or enabling and disabling the service.

Reporting Service

Runs the Data Analyzer application in an Informatica domain. You log in to Data Analyzer to create and run reports on data in a relational database or to run the following PowerCenter reports: PowerCenter Repository Reports, Data Profiling Reports, or Metadata Manager Reports. You can also run other reports within your organization.

When you select a Reporting Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the Data Analyzer instance.
- **Properties** view. The Reporting Service properties such as the data source properties or the Data Analyzer repository properties. You can edit some of these properties.
- **Permissions** view. View or edit group and user permissions on the Reporting Service.
- **Actions** menu. Manage the service and repository contents.

SAP BW Service

Listens for RFC requests from SAP BW and initiates workflows to extract from or load to SAP BW. Select an SAP BW Service in the Navigator to access properties and other information about the service.

When you select an SAP BW Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process.
- **Properties** view. Manage general properties and node assignments.
- **Associated Integration Service** view. View or edit the Integration Service associated with the SAP BW Service.
- **Processes** view. View or edit the directory of the BWParam parameter file.
- **Permissions** view. View or edit group and user permissions on the SAP BW Service.
- **Actions** menu. Manage the service.

Web Services Hub

A web service gateway for external clients. It processes SOAP requests from web service clients that want to access PowerCenter functionality through web services. Web service clients access the PowerCenter Integration Service and PowerCenter Repository Service through the Web Services Hub.

When you select a Web Services Hub in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process.
- **Properties** view. View or edit Web Services Hub properties.
- **Associated Repository** view. View the PowerCenter Repository Services associated with the Web Services Hub.
- **Permissions** view. View or edit group and user permissions on the Web Services Hub.
- **Actions** menu. Manage the service.

Nodes

A node is a logical representation of a physical machine in the domain. On the **Domain** tab, you assign resources to nodes and configure service processes to run on nodes.

When you select a node in the Navigator, the contents panel displays the following information:

- Node status. View the status of the node.
- **Properties** view. View or edit node properties, such as the repository backup directory or range of port numbers for the processes that run on the node.
- **Processes** view. View the status of processes configured to run on the node.
- **Resources** view. View or edit resources assigned to the node.
- **Permissions** view. View or edit group and user permissions on the node.

In the **Actions** menu in the Navigator, you can delete the node, move the node to a folder, refresh the contents on the **Domain** tab, or access help on the current tab.

In the **Actions** menu on the **Domain** tab, you can remove the node association, recalculate the CPU profile benchmark, or shut down the node.

Grids

A grid is an alias assigned to a group of nodes that run PowerCenter sessions and workflows.

When you run a workflow or session on a grid, you distribute the processing across multiple nodes in the grid. You assign nodes to the grid in the **Services and Nodes** view on the **Domain** tab.

When you select a grid in the Navigator, the contents panel displays the following information:

- **Properties** view. View or edit node assignments to a grid.
- **Permissions** view. View or edit group and user permissions on the grid.

In the **Actions** menu in the Navigator, you can delete the grid, move the grid to a folder, refresh the contents on the **Domain** tab, or access help on the current tab.

Licenses

You create a license object on the **Domain** tab based on a license key file provided by Informatica.

After you create the license, you can assign services to the license.

When you select a license in the Navigator, the contents panel displays the following information:

- **Properties** view. View license properties, such as supported platforms, repositories, and licensed options. You can also edit the license description.
- **Assigned Services** view. View or edit the services assigned to the license.
- **Options** view. View the licensed PowerCenter options.
- **Permissions** view. View or edit user permissions on the license.

In the **Actions** menu in the Navigator, you can delete the license, move the license to a folder, refresh the contents on the **Domain** tab, or access help on the current tab.

In the **Actions** menu on the **Domain** tab, you can add an incremental key to a license.

Domain Tab - Connections View

The **Connections** view shows the domain and all connections in the domain.

The **Connections** view has the following components:

Navigator

Appears in the left pane of the **Domain** tab and displays the domain and the connections in the domain.

Contents panel

Appears in the right pane of the **Domain** tab and displays information about the domain or the connection that you select in the Navigator.

When you select the domain in the Navigator, the contents panel shows all connections in the domain. In the contents panel, you can filter or sort connections, or search for specific connections.

When you select a connection in the Navigator, the contents panel displays information about the connection and lets you complete tasks for the connection, depending on which of the following views you select:

- **Properties** view. View or edit connection properties.
- **Pooling** view. View or edit pooling properties for the connection.
- **Permissions** view. View or edit group or user permissions on the connection.

Also, the **Actions** menu lets you test a connection.

Actions menu in the Navigator

When you select the domain in the Navigator, you can create a connection.

When you select a connection in the Navigator, you can delete the connection.

Actions menu on the Domain tab

When you select a connection in the Navigator, you can edit direct permissions or assign permissions to the connection.

Logs Tab

The **Logs** tab shows logs.

On the **Logs** tab, you can view the following types of logs:

- Domain log. Domain log events are log events generated from the domain functions the Service Manager performs.
- Service log. Service log events are log events generated by each application service.
- User Activity log. User Activity log events monitor user activity in the domain.

The **Logs** tab displays the following components for each type of log:

- Filter. Configure filter options for the logs.
- Log viewer. Displays log events based on the filter criteria.
- Reset filter. Reset the filter criteria.
- Copy rows. Copy the log text of the selected rows.
- **Actions** menu. Contains options to save, purge, and manage logs. It also contains filter options.

Reports Tab

The **Reports** tab shows domain reports.

On the **Reports** tab, you can run the following domain reports:

- License Management Report. Run a report to monitor the number of software options purchased for a license and the number of times a license exceeds usage limits. Run a report to monitor the usage of logical CPUs and PowerCenter Repository Services. You run the report for a license.
- Web Services Report. Run a report to analyze the performance of web services running on a Web Services Hub. You run the report for a time interval.

Monitoring Tab

On the **Monitoring** tab, you can monitor Data Integration Services and integration objects that run on the Data Integration Service.

Integration objects include jobs, applications, deployed mappings, SQL data services, web services, and logical objects. The **Monitoring** tab displays properties, run-time statistics, and run-time reports about the integration objects.

The **Monitoring** tab contains the following components:

- Navigator. Appears in the left pane of the **Monitoring** tab and displays jobs, applications, and application components. Application components include deployed mappings, web services, and logical data objects.
- Contents panel. Appears in the right pane of the **Monitoring** tab. It contains information about the object that is selected in the Navigator. If you select a folder in the Navigator, the contents panel lists all objects in the folder. If you select an application component in the Navigator, multiple views of information about the object appear in the contents panel.
- Details panel. Appears below the contents panel in some cases. The details panel allows you to view details about the object that is selected in the contents panel.
- Actions menu. Appears on the **Monitoring** tab. Allows you to view context, clear search filters, abort a selected job, and view logs for a selected object.

Security Tab

You administer Informatica security on the Security tab of the Administrator tool.

The Security tab has the following components:

- Search section. Search for users, groups, or roles by name.
- Navigator. The Navigator appears in the left pane and display groups, users, and roles.
- Contents panel. The contents panel displays properties and options based on the object selected in the Navigator and the tab selected in the contents panel.
- Security Actions Menu. Contains options to create or delete a group, user, or role. You can manage LDAP and operating system profiles. You can also view users that have privileges for a service.

Using the Search Section

Use the Search section to search for users, groups, and roles by name. Search is not case sensitive.

1. In the Search section, select whether you want to search for users, groups, or roles.
2. Enter the name or partial name to search for.

   You can include an asterisk (*) in a name to use a wildcard character in the search. For example, enter “ad*” to search for all objects starting with “ad”. Enter “*ad” to search for all objects ending with “ad”.
3. Click Go.

   The Search Results section appears and displays a maximum of 100 objects. If your search returns more than 100 objects, narrow your search criteria to refine the search results.
4. Select an object in the Search Results section to display information about the object in the contents panel.

Using the Security Navigator

The Navigator appears in the contents panel of the Security tab. When you select an object in the Navigator, the contents panel displays information about the object.

The Navigator on the Security tab includes the following sections:

- Groups section. Select a group to view the properties of the group, the users assigned to the group, and the roles and privileges assigned to the group.
- Users section. Select a user to view the properties of the user, the groups the user belongs to, and the roles and privileges assigned to the user.
- Roles section. Select a role to view the properties of the role, the users and groups that have the role assigned to them, and the privileges assigned to the role.

The Navigator provides different ways to complete a task. You can use any of the following methods to manage groups, users, and roles:

- Click the Actions menu. Each section of the Navigator includes an Actions menu to manage groups, users, or roles. Select an object in the Navigator and click the Actions menu to create, delete, or move groups, users, or roles.
- Right-click an object. Right-click an object in the Navigator to display the create, delete, and move options available in the Actions menu.
- Drag an object from one section to another section. Select an object and drag it to another section of the Navigator to assign the object to another object. For example, to assign a user to a native group, you can select a user in the Users section of the Navigator and drag the user to a native group in the Groups section.
- Drag multiple users or roles from the contents panel to the Navigator. Select multiple users or roles in the contents panel and drag them to the Navigator to assign the objects to another object. For example, to assign multiple users to a native group, you can select the Native folder in the Users section of the Navigator to display all native users in the contents panel. Use the Ctrl or Shift keys to select multiple users and drag the selected users to a native group in the Groups section of the Navigator.
- Use keyboard shortcuts. Use keyboard shortcuts to move to different sections of the Navigator.

Groups

A group is a collection of users and groups that can have the same privileges, roles, and permissions.

The Groups section of the Navigator organizes groups into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Groups section of the Navigator, the contents panel displays all groups belonging to the security domain. Right-click a group and select Navigate to Item to display the group details in the contents panel.

When you select a group in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the group and users assigned to the group.
- Privileges. Displays the privileges and roles assigned to the group for the domain and for application services in the domain.

Users

A user with an account in the Informatica domain can log in to the following application clients:

- Informatica Administrator
- PowerCenter Client
- Metadata Manager
- Data Analyzer
- Informatica Developer
- Informatica Analyst

The Users section of the Navigator organizes users into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Users section of the Navigator, the contents panel displays all users belonging to the security domain. Right-click a user and select Navigate to Item to display the user details in the contents panel.

When you select a user in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the user and all groups to which the user belongs.
- Privileges. Displays the privileges and roles assigned to the user for the domain and for application services in the domain.

Roles

A role is a collection of privileges that you assign to a user or group. Privileges determine the actions that users can perform. You assign a role to users and groups for the domain and for application services in the domain.

The Roles section of the Navigator organizes roles into the following folders:

- System-defined Roles. Contains roles that you cannot edit or delete. The Administrator role is a system-defined role.
- Custom Roles. Contains roles that you can create, edit, and delete. The Administrator tool includes some custom roles that you can edit and assign to users and groups.

When you select a folder in the Roles section of the Navigator, the contents panel displays all roles belonging to the folder. Right-click a role and select Navigate to Item to display the role details in the contents panel.

When you select a role in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the role and the users and groups that have the role assigned for the domain and application services.
- Privileges. Displays the privileges assigned to the role for the domain and application services.

Keyboard Shortcuts

Use the following keyboard shortcuts to navigate to different components in the Administrator tool.

The following table lists the keyboard shortcuts for the Administrator tool:

Shortcut	Task
Shift+Alt+G	On the Security page, move to the Groups section of the Navigator.
Shift+Alt+U	On the Security page, move to the Users section of the Navigator.
Shift+Alt+R	On the Security page, move to the Roles section of the Navigator.

CHAPTER 4

Domain Management

This chapter includes the following topics:

- Domain Management Overview, 25
- Alert Management, 26
- Folder Management, 27
- Domain Security Management, 29
- User Security Management, 29
- Application Service Management, 30
- Node Management, 32
- Gateway Configuration, 37
- Domain Configuration Management, 37
- Domain Tasks, 41
- Domain Properties, 44

Domain Management Overview

An Informatica domain is a collection of nodes and services that define the Informatica environment. To manage the domain, you manage the nodes and services within the domain.

Use the Administrator tool to complete the following tasks:

- Manage alerts. Configure, enable, and disable domain and service alerts for users.
- Create folders. Create folders to organize domain objects and manage security by setting permission on folders.
- Manage domain security. Configure secure communication between domain components.
- Manage user security. Assign privileges and permissions to users and groups.
- Manage application services. Enable, disable, and remove application services. Enable, disable, and restart service processes.
- Manage nodes. Configure node properties, such as the backup directory and resources, and shut down nodes.
- Configure gateway nodes. Configure nodes to serve as a gateway.
- Shut down the domain. Shut down the domain to complete administrative tasks on the domain.
- Manage domain configuration. Back up the domain configuration on a regular basis. You might need to restore the domain configuration from a backup to migrate the configuration to another database user account. You might also need to reset the database information for the domain configuration if it changes.

- Complete domain tasks. You can monitor the statuses of all application services and nodes, view dependencies among application services and nodes, and shut down the domain.
- Configure domain properties. For example, you can change the database properties, SMTP properties for alerts, and domain resiliency properties.

To manage nodes and services through a single interface, all nodes and services must be in the same domain. You cannot access multiple Informatica domains in the same Administrator tool window. You can share metadata between domains when you register or unregister a local repository in the local Informatica domain with a global repository in another Informatica domain.

Alert Management

Alerts provide users with domain and service alerts. Domain alerts provide notification about node failure and master gateway election. Service alerts provide notification about service process failover. To use the alerts, complete the following tasks:

- Configure the SMTP settings for the outgoing email server.
- Subscribe to alerts.

After you configure the SMTP settings, users can subscribe to domain and service alerts.

Configuring SMTP Settings

You configure the SMTP settings for the outgoing mail server to enable alerts.

Configure SMTP settings on the domain **Properties** view.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the domain.
3. In the contents panel, click the **Properties** view.
4. In the SMTP Configuration area of the, click **Edit**.
5. Edit the SMTP settings and click **OK**.

Related Topics:

- “SMTP Configuration” on page 47

Subscribing to Alerts

After you complete the SMTP configuration, you can subscribe to alerts.

1. Verify that the domain administrator has entered a valid email address for your user account on the **Security** page.

   If the email address or the SMTP configuration is not valid, the Service Manager cannot deliver the alert notification.
2. In the Administrator tool header area, click **Manage** > **Preferences**.

   The **Preferences** page appears.
3. In the User Preferences section, click **Edit**.

   The **Edit Preferences** dialog box appears.

4. Select **Subscribe for Alerts**.
5. Click **OK**.
6. Click **OK**.

The Service Manager sends alert notification emails based on your domain privileges and permissions.

The following table lists the alert types and events for notification emails:

Alert Type	Event
Domain	Node Failure Master Gateway Election
Service	Service Process Failover

Viewing Alerts

When you subscribe to alerts, you can receive domain and service notification emails for certain events. When a domain or service event occurs that triggers a notification, you can track the alert status in the following ways:

- The Service Manager sends an alert notification email to all subscribers with the appropriate privilege and permission on the domain or service.
- The Log Manager logs alert notification delivery success or failure in the domain or service log.

For example, the Service Manager sends the following notification email to all alert subscribers with the appropriate privilege and permission on the service that failed:

```
From: Administrator@<database host>
To: Jon Smith
Subject: Alert message of type [Service] for object [HR_811].
The service process on node [node01] for service [HR_811] terminated unexpectedly.
```

In addition, the Log Manager writes the following message to the service log:

```
ALERT_10009 Alert message [service process failover] of type [service] for object [HR_811] was
successfully sent.
```

You can review the domain or service logs for undeliverable alert notification emails. In the domain log, filter by Alerts as the category. In the service logs, search on the message code ALERT. When the Service Manager cannot send an alert notification email, the following message appears in the related domain or service log:

```
ALERT_10004: Unable to send alert of type [alert type] for object [object name], alert message [alert
message], with error [error].
```

Folder Management

Use folders in the domain to organize objects and to manage security. Folders can contain nodes, services, grids, licenses, and other folders. You might want to use folders to group services by type. For example, you can create a folder called IntegrationServices and move all Integration Services to the folder. Or, you might want to create folders to group all services for a functional area, such as Sales or Finance.

When you assign a user permission on the folder, the user inherits permission on all objects in the folder.

You can perform the following tasks with folders:

- View services and nodes. View all services in the folder and the nodes where they run. Click a node or service name to access the properties for that node or service.

- Create folders. Create folders to group objects in the domain.
- Move objects to folders. When you move an object to a folder, folder users inherit permission on the object in the folder. When you move a folder to another folder, the other folder becomes a parent of the moved folder.
- Remove folders. When you remove a folder, you can delete the objects in the folder or move them to the parent folder.

Creating a Folder

You can create a folder in the domain or in another folder.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the domain or folder in which you want to create a folder.
3. On the Navigator Actions menu, click New > Folder.
4. Edit the following properties:

Node Property	Description
Name	Name of the folder. The name is not case sensitive and must be unique within the domain. It cannot exceed 80 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the folder. The description cannot exceed 765 characters.
Path	Location in the Navigator.

5. Click OK.

Moving Objects to a Folder

When you move an object to a folder, folder users inherit permission on the object. When you move a folder to another folder, the moved folder becomes a child object of the folder where it resides.

Note: The domain serves as a folder when you move objects in and out of folders.

1. In the Informatica tool, click the Domain tab.
2. In the Navigator, select an object.
3. On the Navigator Actions menu, select Move to Folder.
4. In the Select Folder dialog box, select a folder, and click OK.

Removing a Folder

When you remove a folder, you can delete the objects in the folder or move them to the parent folder.

1. In the Informatica tool, click the Domain tab.
2. In the Navigator, select a folder.
3. On the Navigator Actions menu, select Delete.
4. Confirm that you want to delete the folder.

   You can delete the contents only if you have the appropriate privileges and permissions on all objects in the folder.

5. Choose to wait until all processes complete or to abort all processes.
6. Click OK.

Domain Security Management

You can configure Informatica domain components to use the Secure Sockets Layer (SSL) protocol or the Transport Layer Security (TLS) protocol to encrypt connections with other components. When you enable SSL or TLS for domain components, you ensure secure communication.

You can configure secure communication in the following ways:

Between services within the domain

You can configure secure communication between services within the domain.

Between the domain and external components

You can configure secure communication between Informatica domain components and web browsers or web service clients.

Each method of configuring secure communication is independent of the other methods. When you configure secure communication for one set of components, you do not need to configure secure communication for any other set.

User Security Management

You manage user security within the domain with privileges and permissions.

Privileges determine the actions that users can complete on domain objects. Permissions define the level of access a user has to a domain object. Domain objects include the domain, folders, nodes, grids, licenses, database connections, operating system profiles, and application services.

Even if a user has the domain privilege to complete certain actions, the user may also require permission to complete the action on a particular object. For example, a user has the Manage Services domain privilege which grants the user the ability to edit application services. However, the user also must have permission on the application service. A user with the Manage Services domain privilege and permission on the Development Repository Service but not on the Production Repository Service can edit the Development Repository Service but not the Production Repository Service.

To log in to the Administrator tool, a user must have have the Access Informatica Administrator domain privilege. If a user has the Access Informatica Administrator privilege and permission on an object, but does not have the domain privilege that grants the ability to modify the object type, then the user can view the object. For example, if a user has permission on a node, but does not have the Manage Nodes and Grids privilege, the user can view the node properties but cannot configure, shut down, or remove the node.

If a user does not have permission on a selected object in the Navigator, the contents panel displays a message indicating that permission on the object is denied.

Application Service Management

You can perform the following common administration tasks for application services:

- Enable and disable services and service processes.
- Configure the domain to restart service processes.
- Remove an application service.
- Troubleshoot problems with an application service.

Enabling and Disabling Services and Service Processes

You can enable and disable application services and service processes in the Administrator tool. When a service is enabled, there must be at least one service process enabled and running for the service to be available. By default, all service processes are enabled.

The behavior of a service when it starts service processes depends on its configuration:

- If the service is configured for high availability, the service starts the service process on the primary node. All backup nodes are on standby.
- If the service is configured to run on a grid, the service starts service processes on all nodes.

A service does not start a disabled service process in any situation.

The state of a service depends on the state of the constituent service processes. A service can have the following states:

- Available. You have enabled the service and at least one service process is running. The service is available to process requests.
- Unavailable. You have enabled the service but there are no service processes running. This can be a result of service processes being disabled or failing to start. The service is not available to process requests.
- Disabled. You have disabled the service.

You can disable a service to perform a management task, such as changing the data movement mode for a PowerCenter Integration Service. You might want to disable the service process on a node if you need to shut down the node for maintenance. When you disable a service, all associated service processes stop, but they remain enabled.

The following table describes the different states of a service process:

Service Process State	Process Configuration	Description
Running	Enabled	The service process is running on the node.
Standing By	Enabled	The service process is enabled but is not running because another sevice process is running as the primary service process. It is on standby to run in case of service failover. **Note:** Service processes cannot have a standby state when the PowerCenter Integration Service runs on a grid. If you run the PowerCenter Integration Service on a grid, all service processes run concurrently.
Disabled	Disabled	The service is enabled but the service process is stopped and is not running on the node.

Service Process State	Process Configuration	Description
Stopped	Enabled	The service is unavailable.
Failed	Enabled	The service and service process are enabled, but the service process could not start.

Note: A service process will be in a failed state if it cannot start on the assigned node.

Viewing Service Processes

You can view the state of a service process on the Processes view of a service. You can view the state of all service processes on the Overview view of the domain.
To view the state of a service process:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a service.
3. In the contents panel, select the Processes view.

   The Processes view displays the state of the processes.

Configuring Restart for Service Processes

If an application service process becomes unavailable while a node is running, the domain tries to restart the process on the same node based on the restart options configured in the domain properties.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the domain.
3. In the Properties view, configure the following restart properties:

Domain Property	Description
Maximum Restart Attempts	Number of times within a specified period that the domain attempts to restart an application service process when it fails. The value must be greater than or equal to 1. Default is 3.
Within Restart Period (sec)	Maximum period of time that the domain spends attempting to restart an application service process when it fails. If a service fails to start after the specified number of attempts within this period of time, the service does not restart. Default is 900.

Removing Application Services

You can remove an application service using the Administrator tool. Before removing an application service, you must disable it.

Disable the service before you delete the service to ensure that the service is not running any processes. If you do not disable the service, you may have to choose to wait until all processes complete or abort all processes when you delete the service.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the application service.

3. In the Domain tab Actions menu, select Delete.
4. In the warning message that appears, click Yes to stop other services that depend on the application service.
5. If the Disable Service dialog box appears, choose to wait until all processes complete or abort all processes, and then click OK.

Troubleshooting Application Services

I think that a service is using incorrect environment variable values. How can I find out which environment variable values are used by a service.

Set the error severity level for the node to debug. When the service starts on the node, the Domain log will display the environment variables that the service is using.

Node Management

A node is a logical representation of a physical machine in the domain. During installation, you define at least one node that serves as the gateway for the domain. You can define other nodes using the installation program or *infasetup* command line program.

After you define a node, you must add the node to the domain. When you add a node to the domain, the node appears in the Navigator, and you can view and edit its properties. Use the Domain tab of Administrator tool to manage nodes, including configuring node properties and removing nodes from a domain.

You perform the following tasks to manage a node:

- Define the node and add it to the domain. Adds the node to the domain and enables the domain to communicate with the node. After you add a node to a domain, you can start the node.
- Configure properties. Configure node properties, such as the repository backup directory and ports used to run processes.
- View processes. View the processes configured to run on the node and their status. Before you remove or shut down a node, verify that all running processes are stopped.
- Shut down the node. Shut down the node if you need to perform maintenance on the machine or to ensure that domain configuration changes take effect.
- Remove a node. Remove a node from the domain if you no longer need the node.
- Define resources. When the Integration Service runs on a grid, you can configure it to check the resources available on each node. Assign connection resources and define custom and file/directory resources on a node.
- Edit permissions. View inherited permissions for the node and manage the object permissions for the node.

Defining and Adding Nodes

You must define a node and add it to the domain so that you can start the node. When you install Informatica services, you define at least one node that serves as the gateway for the domain. You can define other nodes. The other nodes can be gateway nodes or worker nodes.

A master gateway node receives service requests from clients and routes them to the appropriate service and node. You can define one or more gateway nodes.

A worker node can run application services but cannot serve as a gateway.

When you define a node, you specify the host name and port number for the machine that hosts the node. You also specify the node name. The Administrator tool uses the node name to identify the node.

Use either of the following programs to define a node:

- Informatica installer. Run the installer on each machine you want to define as a node.
- *infasetup* command line program. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command on each machine you want to serve as a gateway or worker node.

When you define a node, the installation program or *infasetup* creates the nodemeta.xml file, which is the node configuration file for the node. A gateway node uses information in the nodemeta.xml file to connect to the domain configuration database. A worker node uses the information in nodemeta.xml to connect to the domain. The nodemeta.xml file is stored in the \isp\config directory on each node.

After you define a node, you must add it to the domain. When you add a node to the domain, the node appears in the Navigator. You can add a node to the domain using the Administrator tool or the *infacmd* AddDomainNode command.

To add a node to the domain:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the folder where you want to add the node. If you do not want the node to appear in a folder, select the domain.
3. On the Navigator Actions menu, click New > Node.

   The Create Node dialog box appears.
4. Enter the node name. This must be the same node name you specified when you defined the node.
5. If you want to change the folder for the node, click Select Folder and choose a new folder or the domain.
6. Click Create.

   If you add a node to the domain before you define the node using the installation program or *infasetup*, the Administrator tool displays a message saying that you need to run the installation program to associate the node with a physical host name and port number.

Configuring Node Properties

You configure node properties on the Properties view for the node. You can configure properties such as the error severity level, minimum and maximum port numbers, and the maximum number of Session and Command tasks that can run on a PowerCenter Integration Service process.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. Click the Properties view.

   The Properties view displays the node properties in separate sections.
4. In the Properties view, click Edit for the section that contains the property you want to set.
5. Edit the following properties:

Node Property	Description
Name	Name of the node. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters:

Node Property	Description
	` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the node. The description cannot exceed 765 characters.
Host Name	Host name of the machine represented by the node.
Port	Port number used by the node.
Gateway Node	Indicates whether the node can serve as a gateway. If this property is set to No, then the node is a worker node.
Backup Directory	Directory to store repository backup files. The directory must be accessible by the node.
Error Severity Level	Level of error logging for the node. These messages are written to the Log Manager application service and Service Manager log files. Set one of the following message levels: - Error. Writes ERROR code messages to the log. - Warning. Writes WARNING and ERROR code messages to the log. - Info. Writes INFO, WARNING, and ERROR code messages to the log. - Tracing. Writes TRACE, INFO, WARNING, and ERROR code messages to the log. - Debug. Writes DEBUG, TRACE, INFO, WARNING, and ERROR code messages to the log. Default is WARNING.
Minimum Port Number	Minimum port number used by service processes on the node. To apply changes, restart Informatica services. The default value is the value entered when the node was defined.
Maximum Port Number	Maximum port number used by service processes on the node. To apply changes, restart Informatica services. The default value is the value entered when the node was defined.
CPU Profile Benchmark	Ranking of the CPU performance of the node compared to a baseline system. For example, if the CPU is running 1.5 times as fast as the baseline machine, the value of this property is 1.5. You can calculate the benchmark by clicking **Actions** > **Recalculate CPU Profile Benchmark**. The calculation takes approximately five minutes and uses 100% of one CPU on the machine. Or, you can update the value manually. Default is 1.0. Minimum is 0.001. Maximum is 1,000,000. Used in adaptive dispatch mode. Ignored in round-robin and metric-based dispatch modes.
Maximum Processes	Maximum number of running processes allowed for each PowerCenter Integration Service process that runs on the node. This threshold specifies the maximum number of running Session *or* Command tasks allowed for each Integration Service process running on the node. Set this threshold to a high number, such as 200, to cause the Load Balancer to ignore it. To prevent the Load Balancer from dispatching tasks to this node, set this threshold to 0. Default is 10. Minimum is 0. Maximum is 1,000,000,000. Used in all dispatch modes.
Maximum CPU Run Queue Length	Maximum number of runnable threads waiting for CPU resources on the node. Set this threshold to a low number to preserve computing resources for other applications. Set this threshold to a high value, such as 200, to cause the Load Balancer to ignore it. Default is 10. Minimum is 0. Maximum is 1,000,000,000. Used in metric-based and adaptive dispatch modes. Ignored in round-robin dispatch mode.
Maximum Memory %	Maximum percentage of virtual memory allocated on the node relative to the total physical memory size. Set this threshold to a value greater than 100% to allow the allocation of virtual memory to exceed the physical memory size when dispatching tasks. Set this threshold to a high value, such as 1,000, if you want the Load Balancer to ignore it. Default is 150. Minimum is 0. Maximum is 1,000,000,000.

Node Property	Description
	Used in metric-based and adaptive dispatch modes. Ignored in round-robin dispatch mode.

6. Click OK.

Related Topics:

- "Defining Resource Provision Thresholds" on page 357

Viewing Processes on the Node

You can view the status of all processes configured to run on a node. Before you shut down or remove a node, you can view the status of each process to determine which processes you need to disable.

To view processes on a node:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. In the content panel, select the Processes view.

   The tab displays the status of each process configured to run on the node.

Shutting Down and Restarting the Node

Some administrative tasks may require you to shut down a node. For example, you might need to perform maintenance or benchmarking on a machine. You might also need to shut down and restart a node for some configuration changes to take effect. For example, if you change the shared directory for the Log Manager or domain, you must shut down the node and restart it to update the configuration files.

You can shut down a node from the Administrator tool or from the operating system. When you shut down a node, you stop Informatica services and abort all processes running on the node.

To restart a node, start Informatica services on the node.

Note: To avoid loss of data or metadata when you shut down a node, disable all running processes in complete mode.

Shutting Down a Node from the Administrator Tool

To shut down a node from the Administrator tool:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. On the Domain tab Actions menu, select Shutdown.

   The Administrator tool displays the list of service processes running on that node.
4. Click OK to stop all processes and shut down the node, or click Cancel to cancel the operation.

Starting or Stopping a Node on Windows

To start or stop the node on Windows:

1. Open the Windows Control Panel.
2. Select **Administrative Tools**.

3. Select **Services**.
4. Right-click the Informatica9.0 service.
5. If the service is running, click **Stop**.

   If the service is stopped, click **Start**.

Starting or Stopping a Node on UNIX

On UNIX, run infaservice.sh to start and stop the Informatica daemon. By default, infaservice.sh is installed in the following directory:

```
<InformaticaInstallationDir>/tomcat/bin
```

1. Go to the directory where infaservice.sh is located.
2. At the command prompt, enter the following command to start the daemon:

   ```
   infaservice.sh startup
   ```

   Enter the following command to stop the daemon:

   ```
   infaservice.sh shutdown
   ```

   Note: If you use a softlink to specify the location of infaservice.sh, set the INFA_HOME environment variable to the location of the Informatica installation directory.

Removing the Node Association

You can remove the host name and port number associated with a node. When you remove the node association, the node remains in the domain, but it is not associated with a host machine.

To associate a different host machine with the node, you must run the installation program or *infasetup* DefineGatewayNode or DefineWorkerNode command on the new host machine, and then restart the node on the new host machine.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. In the Domain tab Actions menu, select Remove Node Association.

Removing a Node

When you remove a node from a domain, it is no longer visible in the Navigator. If the node is running when you remove it, the node shuts down and all service processes are aborted.

Note: To avoid loss of data or metadata when you remove a node, disable all running processes in complete mode.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. In the Navigator Actions menu, select Delete.
4. In the warning message that appears, click OK.

Gateway Configuration

One gateway node in the domain serves as the master gateway node for the domain. The Service Manager on the master gateway node accepts service requests and manages the domain and services in the domain.

During installation, you create one gateway node. After installation, you can create additional gateway nodes. You might want to create additional gateway nodes as backups. If you have one gateway node and it becomes unavailable, the domain cannot accept service requests. If you have multiple gateway nodes and the master gateway node becomes unavailable, the Service Managers on the other gateway nodes elect a new master gateway node. The new master gateway node accepts service requests. Only one gateway node can be the master gateway node at any given time. You must have at least one node configured as a gateway node at all times. Otherwise, the domain is inoperable.

You can configure a worker node to serve as a gateway node. The worker node must be running when you configure it to serve as a gateway node.

Note: You can also run the *infasetup* DefineGatewayNode command to create a gateway node. If you configure a worker node to serve as a gateway node, you must specify the log directory. If you have multiple gateway nodes, configure all gateway nodes to write log files to the same directory on a shared disk.

After you configure the gateway node, the Service Manager on the master gateway node writes the domain configuration database connection to the nodemeta.xml file of the new gateway node.

If you configure a master gateway node to serve as a worker node, you must restart the node to make the Service Managers elect a new master gateway node. If you do not restart the node, the node continues as the master gateway node until you restart the node or the node becomes unavailable.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the domain.
3. In the contents panel, select the Properties view.
4. In the Properties view, click Edit in the Gateway Configuration Properties section.
5. Select the check box next to the node that you want to serve as a gateway node.

   You can select multiple nodes to serve as gateway nodes.
6. Configure the directory path for the log files.

   If you have multiple gateway nodes, configure all gateway nodes to point to the same location for log files.
7. Click OK.

Domain Configuration Management

The Service Manager on the master gateway node manages the domain configuration. The domain configuration is a set of metadata tables stored in a relational database that is accessible by all gateway nodes in the domain. Each time you make a change to the domain, the Service Manager writes the change to the domain configuration. For example, when you add a node to the domain, the Service Manager adds the node information to the domain configuration. The gateway nodes use a JDBC connection to access the domain configuration database.

You can perform the following domain configuration management tasks:

- Back up the domain configuration. Back up the domain configuration on a regular basis. You may need to restore the domain configuration from a backup if the domain configuration in the database becomes corrupt.

- Restore the domain configuration. You may need to restore the domain configuration if you migrate the domain configuration to another database user account. Or, you may need to restore the backup domain configuration to a database user account.
- Migrate the domain configuration. You may need to migrate the domain configuration to another database user account.
- Configure the connection to the domain configuration database. Each gateway node must have access to the domain configuration database. You configure the database connection when you create a domain. If you change the database connection information or migrate the domain configuration to a new database, you must update the database connection information for each gateway node.
- Configure custom properties. Configure domain properties that are unique to your environment or that apply in special cases. Use custom properties only if Informatica Global Customer Support instructs you to do so.

Note: The domain configuration database and the Model repository cannot use the same database user schema.

Backing Up the Domain Configuration

Back up the domain configuration on a regular basis. You may need to restore the domain configuration from a backup file if the domain configuration in the database becomes corrupt.

Run the *infasetup* BackupDomain command to back up the domain configuration to a binary file.

Restoring the Domain Configuration

You can restore domain configuration from a backup file. You may need to restore the domain configuration if the domain configuration in the database becomes inconsistent or if you want to migrate the domain configuration to another database.

Informatica restores the domain configuration from the current version. If you have a backup file from an earlier product version, you must use the earlier version to restore the domain configuration.

You can restore the domain configuration to the same or a different database user account. If you restore the domain configuration to a database user account with existing domain configuration, you must configure the command to overwrite the existing domain configuration. If you do not configure the command to overwrite the existing domain configuration, the command fails.

Each node in a domain has a host name and port number. When you restore the domain configuration, you can disassociate the host names and port numbers for all nodes in the domain. You might do this if you want to run the nodes on different machines. After you restore the domain configuration, you can assign new host names and port numbers to the nodes. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command to assign a new host name and port number to a node.

If you restore the domain configuration to another database, you must reset the database connections for all gateway nodes.

Important: You lose all data in the summary tables when you restore the domain configuration.

Complete the following tasks to restore the domain:

1. Disable the application services. Disable the application services in complete mode to ensure that you do not abort any running service process. You must disable the application services to ensure that no service process is running when you shut down the domain.
2. Shut down the domain. You must shut down the domain to ensure that no change to the domain occurs while you are restoring the domain.

3. Run the *infasetup* RestoreDomain command to restore the domain configuration to a database. The RestoreDomain command restores the domain configuration in the backup file to the specified database user account.
4. Assign new host names and port numbers to the nodes in the domain if you disassociated the previous host names and port numbers when you restored the domain configuration. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command to assign a new host name and port number to a node.
5. Reset the database connections for all gateway nodes if you restored the domain configuration to another database. All gateway nodes must have a valid connection to the domain configuration database.

Migrating the Domain Configuration

You can migrate the domain configuration to another database user account. You may need to migrate the domain configuration if you no longer support the existing database user account. For example, if your company requires all departments to migrate to a new database type, you must migrate the domain configuration.

1. Shut down all application services in the domain.
2. Shut down the domain.
3. Back up the domain configuration.
4. Create the database user account where you want to restore the domain configuration.
5. Restore the domain configuration backup to the database user account.
6. Update the database connection for each gateway node.
7. Start all nodes in the domain.
8. Enable all application services in the domain.

Important: Summary tables are lost when you restore the domain configuration.

Step 1. Shut Down All Application Services

You must disable all application services to disable all service processes. If you do not disable an application service and a user starts running a service process while you are backing up and restoring the domain, the service process changes may be lost and data may become corrupt.

Tip: Shut down the application services in complete mode to ensure that you do not abort any running service processes.

Shut down the application services in the following order:

1. Web Services Hub
2. SAP BW Service
3. Metadata Manager Service
4. PowerCenter Integration Service
5. PowerCenter Repository Service
6. Reporting Service
7. Analyst Service
8. Content Management Service
9. Data Integration Service
10. Model Repository Service

Step 2. Shut Down the Domain

You must shut down the domain to ensure that users do not modify the domain while you are migrating the domain configuration. For example, if the domain is running when you are backing up the domain configuration, users can create new services and objects. Also, if you do not shut down the domain and you restore the domain configuration to a different database, the domain becomes inoperative. The connections between the gateway nodes and the domain configuration database become invalid. The gateway nodes shut down because they cannot connect to the domain configuration database. A domain is inoperative if it has no running gateway node.

Step 3. Back Up the Domain Configuration

Run the *infasetup* BackupDomain command to back up the domain configuration to a binary file.

Step 4. Create a Database User Account

Create a database user account if you want to restore the domain configuration to a new database user account.

Step 5. Restore the Domain Configuration

Run the *infasetup* RestoreDomain command to restore the domain configuration to a database. The RestoreDomain command restores the domain configuration in the backup file to the specified database user account.

Step 6. Update the Database Connection

If you restore the domain configuration to a different database user account, you must update the database connection information for each gateway node in the domain. Gateway nodes must have a connection to the domain configuration database to retrieve and update domain configuration.

Step 7. Start All Nodes in the Domain

Start all nodes in the domain. You must start the nodes to enable services to run.

1. Shut down the gateway node that you want to update.
2. Run the *infasetup* UpdateGatewayNode command to update the gateway node.
3. Start the gateway node.
4. Repeat this process for each gateway node.

Step 8. Enable All Application Services

Enable all application services that you previously shut down. Application services must be enabled to run service processes.

Updating the Domain Configuration Database Connection

All gateway nodes must have a connection to the domain configuration database to retrieve and update domain configuration. When you create a gateway node or configure a node to serve as a gateway, you specify the database connection, including the database user name and password. If you migrate the domain configuration to a different database or change the database user name or password, you must update the database connection for each gateway node. For example, as part of a security policy, your company may require you to change the password for the domain configuration database every three months.

To update the node with the new database connection information, complete the following steps:

1. Shut down the gateway node.
2. Run the *infasetup* UpdateGatewayNode command.

If you change the user or password, you must update the node.

To update the node after you change the user or password, complete the following steps:

1. Shut down the gateway node.
2. Run the *infasetup* UpdateGatewayNode command.

If you change the host name or port number, you must redefine the node.

To redefine the node after you change the host name or port number, complete the following steps:

1. Shut down the gateway node.
2. In the Administrator tool, remove the node association.
3. Run the *infasetup* DefineGatewayNode command.

Domain Tasks

On the **Domain** tab, you can complete domain tasks such as monitoring application services and nodes, managing domain objects, managing logs, and viewing service and node dependencies.

You can monitor all application services and nodes in a domain.You can also manage domain objects by moving them into folders or deleting them. You can also recycle, enable, or disable application services and view logs for application services.

In addition, you can view dependencies among all application services and nodes. An application service is dependent on the node on which it runs. It might also be dependent on another application service. For example, the Data Integration Service must be associated with a Model Repository Service. If the Model Repository Service is unavailable, the Data Integration Service does not work.

To perform impact analysis, view dependencies among application services and nodes. Impact analysis helps you determine the implications of particular domain actions, such as shutting down a node or an application service. For example, you want to shut down a node to run maintenance on the node. Before you shut down the node, you must determine all application services that run on the node. If this is the only node on which an application service runs, that application service is unavailable when you shut down the node.

Managing and Monitoring Application Services and Nodes

You can manage and monitor application services and nodes in a domain.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Services and Nodes** view.
3. In the Navigator, select the domain.

   The contents panel shows the objects defined in the domain.
4. To filter the list of domain objects in the contents panel, enter filter criteria in the filter bar.

   The contents panel shows objects that meet the filter criteria.
5. To remove the filter criteria, click **Reset**.

   The contents panel shows all objects defined in the domain.

6. To show the names of the application services and nodes in the contents panel, click the Show Details button.

   The contents panel shows the names of the application services and nodes in the domain.

7. To hide the names of the application services and nodes in the contents panel, click the Hide Details button.

   The contents panel hides the names of the application services and nodes in the domain.

8. To view details for an object, select the object in the Navigator.

   For example, select an application service in the Navigator to view the service version, service status, process status, and last error message for the service.

   Object details appear.

9. To view properties for an object, click an object in the Navigator.

   The contents panels shows properties for the object.

10. To recycle, enable, disable, or show logs for an application service, double-click the application service in the Navigator.
    - To recycle the application service, click the Recycle the Service button.
    - To enable the application service, click the Enable the Service button.
    - To disable the application service, click the Disable the Service button.
    - To view logs for the application service, click the View Logs for Service button.

11. To move an object to a folder, complete the following steps:
    a. Right-click the object in the Navigator.
    b. Click **Move to Folder**.

       The **Select Folder** dialog box appears.
    c. In the **Select Folder** dialog box, select a folder.

       Alternatively, to create a new folder, click **Create Folder**.

       The **Create Folder** dialog box appears.

       Enter the folder name and click **OK**.
    d. Click **OK**.

       The object is moved to the folder that you specify.

12. To delete an object, right-click the object in the Navigator.

    Click **Delete**.

Viewing Dependencies for Application Services, Nodes, and Grids

In the **Services and Nodes** view on the **Domain** tab, you can view dependencies for application services, nodes, and grids in an Informatica domain.

To view the **View Dependency** window, you must install and enable Adobe Flash Player 10.0.0 or later in your browser. If you use Internet Explorer, enable the **Run ActiveX Controls and Plug-ins** option.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Services and Nodes** view.
3. In the Navigator, select the domain.

   The contents panel displays the objects in the domain.

4. In the contents panel, right-click a domain object and click **View Dependencies**.

The **View Dependency** window shows domain objects connected by blue and orange lines, as follows:

- The blue lines represent service-to-node and service-to-grid dependencies.
- The orange lines represent service-to-service dependencies. To hide or show the service-to-service dependencies, clear or select the **Show Service dependencies** option in the **View Dependency** window. When you clear this option, the orange lines disappear but the services are still visible.

The following table describes the information that appears in the **View Dependency** window based on the object:

Object	View Dependency Window
Node	Shows all service processes running on the node and the status of each process. Shows any grids of to which the node belongs. Also shows secondary dependencies, which are dependencies that are not directly related to the object for which you are viewing dependencies. For example, a Model Repository Service, MRS1, runs on node1. A Data Integration Service, DIS1, and an Analyst Service, AT1, retrieve information from MRS1 but run on node2. The **View Dependency** window shows the following information: - A dependency between node1 and MRS1. - A secondary dependency between node1 and the DIS1 and AT1 services. These services appear greyed out because they are secondary dependencies. If you want to shut down node1, the window indicates that MRS1 is impacted, as well as DIS1 and AT1 due to their dependency on MRS1.
Service	Shows the upstream and downstream dependencies, and the node on which the service runs. An upstream dependency is a service on which the selected service depends. A downstream dependency is a service that depends on the selected service. For example, if you show the dependencies for a Data Integration Service, you see the Model Repository Service upstream dependency, the Analyst Service downstream dependency, and the node on which the Data Integration Service runs.
Grid	Shows the nodes that are part of the grid and the application services running on the grid.

5. In the **View Dependency** window, you can optionally complete the following actions:
   - To view additional dependency information for any object, place the cursor over the object.
   - To highlight the downstream dependencies and show additional process details for a service, place the cursor over the service.
   - To view the **View Dependency** window for any object in the window, right-click the object and click **Show Dependency**.

     The **View Dependency** window refreshes and shows the dependencies for the selected object.

Related Topics:

- "Domain" on page 14

Shutting Down a Domain

To run administrative tasks on a domain, you might need to shut down the domain.

For example, to back up and restore a domain configuration, you must first shut down the domain. When you shut down the domain, the Service Manager on the master gateway node stops all application services and Informatica services in the domain. After you shut down the domain, restart Informatica services on each node in the domain.

When you shut down a domain, any processes running on nodes in the domain are aborted. Before you shut down a domain, verify that all processes, including workflows, have completed and no users are logged in to repositories in the domain.

Note: To avoid a possible loss of data or metadata and allow the currently running processes to complete, you can shut down each node from the Administrator tool or from the operating system.

1. Click the **Domain** tab.
2. In the Navigator, select the domain.
3. On the **Domain** tab, click **Actions** > **Shutdown Domain**.

   The **Shutdown** dialog box lists the processes that run on the nodes in the domain.
4. Click **Yes**.

   The **Shutdown** dialog box shows a warning message.
5. Click **Yes**.

   The Service Manager on the master gateway node shuts down the application services and Informatica services on each node in the domain.
6. To restart the domain, restart Informatica services on the gateway and worker nodes in the domain.

Domain Properties

On the **Domain** tab, you can configure domain properties including database properties, gateway configuration, and service levels.

To view and edit properties, click the **Domain** tab. In the Navigator, select a domain. Then click the **Properties** view in the contents panel. The contents panel shows the properties for the domain.

You can configure the properties to change the domain. For example, you can change the database properties, SMTP properties for alerts, and the domain resiliency properties.

You can also monitor the domain at a high level. In the **Services and Nodes** view, you can view the statuses of the application services and nodes that are defined in the domain.

You can configure the following domain properties:

- General properties. Edit general properties, such as service resilience and dispatch mode.
- Database properties. View the database properties, such as database name and database host.
- Gateway configuration. Configure a node to serve as gateway and specify the location to write log events.
- Service level management. Create and configure service levels.
- SMTP configuration. Edit the SMTP settings for the outgoing mail server to enable alerts.
- Custom properties. Edit custom properties that are unique to the Informatica environment or that apply in special cases. When you create a domain, it has no custom properties. Use custom properties only at the request of Informatica Global Customer Support.

General Properties

In the General Properties area, you can configure general properties for the domain such as service resilience and load balancing.

To edit general properties, click **Edit**.

The following table describes the properties that you can edit in the General Properties area:

Property	Description
Name	Read-only. The name of the domain.
Resilience Timeout (sec)	The amount of time in seconds that a client is allowed to try to connect or reconnect to a service. Valid values are from 0 to 1000000.
Limit on Resilience Timeouts (sec)	The amount of time in seconds that a service waits for a client to connect or reconnect to the service. A client is a PowerCenter client application or the PowerCenter Integration Service. Valid values are from 0 to 1000000.
Restart Period	The maximum amount of time in seconds that the domain spends trying to restart an application service process. Valid values are from 0 to 1000000.
Maximum Restart Attempts within Restart Period	The number of times that the domain tries to restart an application service process. Valid values are from 1 to 1000.
Dispatch Mode	The mode that the Load Balancer uses to dispatch tasks to nodes in a grid. The options are: - MetricBased - RoundRobin - Adaptive
Enable Transport Layer Security (TLS)	Configures services to use the TLS protocol to transfer data securely within the domain. When you enable TLS for the domain, services use TLS connections to communicate with other Informatica application services and clients. Enabling TLS for the domain does not apply to PowerCenter application services. Verify that all domain nodes are available before you enable TLS. If a node is unavailable, then the TLS updates cannot be applied to the Service Manager on the unavailable node. To apply changes, restart the domain. Valid values are true and false.

Database Properties

In the Database Properties area, you can view or edit the database properties for the domain, such as database name and database host.

The following table describes the properties that you can edit in the Database Properties area:

Property	Description
Database Type	The type of database that stores the domain configuration metadata.
Database Host	The name of the machine hosting the database.
Database Port	The port number used by the database.
Database Name	The name of the database.
Database User	The user account for the database containing the domain configuration information.

Gateway Configuration Properties

In the Gateway Configuration Properties area, you can configure a node to serve as gateway for a domain and specify the directory where the Service Manager on this node writes the log event files.

If you edit gateway configuration properties, previous logs do not appear. Also, the changed properties apply to restart and failover scenarios only.

To edit gateway configuration properties, click **Edit**.

To sort gateway configuration properties, click in the header for the column by which you want to sort.

The following table describes the properties that you can edit in the Gateway Configuration Properties area:

Property	Description
Node Name	Read-only. The name of the node.
Status	The status of the node.
Gateway	To configure the node as a gateway node, select this option. To configure the node as a worker node, clear this option.
Log Directory Path	The directory path for the log event files. If the Log Manager cannot write to the directory path, it writes log events to the node.log file on the master gateway node.

Service Level Management

In the Service Level Management area, you can view, add, and edit service levels.

Service levels set priorities among tasks that are waiting to be dispatched. When the Load Balancer has more tasks to dispatch than the PowerCenter Integration Service can run at the time, the Load Balancer places those tasks in the dispatch queue. When multiple tasks are in the dispatch queue, the Load Balancer uses service levels to determine the order in which to dispatch tasks from the queue.

Because service levels are domain properties, you can use the same service levels for all repositories in a domain. You create and edit service levels in the domain properties or by using infacmd.

You can edit but you cannot delete the Default service level, which has a dispatch priority of 5 and a maximum dispatch wait time of 1800 seconds.

To add a service level, click **Add**.

To edit a service level, click the link for the service level.

To delete a service level, select the service level and click the Delete button.

The following table describes the properties that you can edit in the Service Level Management area:

Property	Description
Name	The name of the service level. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with the @ character. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : / ? . < > | ! ( )] [

Property	Description
	After you add a service level, you cannot change its name.
Dispatch Priority	A number that sets the dispatch priority for the service level. The Load Balancer dispatches high priority tasks before low priority tasks. Dispatch priority 1 is the highest priority. Valid values are from 1 to 10. Default is 5.
Maximum Dispatch Wait Time (seconds)	The amount of time in seconds that the Load Balancer waits before it changes the dispatch priority for a task to the highest priority. Setting this property ensures that no task waits forever in the dispatch queue. Valid values are from 1 to 86400. Default is 1800.

Related Topics:

- "Creating Service Levels" on page 356

SMTP Configuration

In the SMTP Configuration area, you can configure SMTP settings for the outgoing mail server to enable alerts.

The following table describes the properties that you can edit in the SMTP Configuration area:

Property	Description
Host Name	The SMTP outbound mail server host name. For example, enter the Microsoft Exchange Server for Microsoft Outlook.
Port	Port used by the outgoing mail server. Valid values are from 1 to 65535. Default is 25.
User Name	The user name for authentication upon sending, if required by the outbound mail server.
Password	The user password for authentication upon sending, if required by the outbound mail server.
Sender Email Address	The email address that the Service Manager uses in the From field when sending notification emails. If you leave this field blank, the Service Manager uses `Administrator@<host name>` as the sender.

Related Topics:

- "Configuring SMTP Settings" on page 26

Custom Properties

Custom properties include properties that are unique to your environment or that apply in special cases.

When you create a domain, it has no custom properties.

Define custom properties only at the request of Informatica Global Customer Support.

CHAPTER 5

Application Service Upgrade

This chapter includes the following topics:

- Application Service Upgrade Overview, 48
- Service Upgrade Wizard, 50

Application Service Upgrade Overview

The product and product version determines the service upgrade process.

Some service versions require a service upgrade. When you upgrade a service, you must also upgrade the dependent services.

Use the service upgrade wizard, the actions menu of each service, or command line to upgrade services. The service upgrade wizard upgrades multiple services in the appropriate order and checks for dependencies. If you use the command line to upgrade services, you must upgrade services in the correct order and verify that you upgrade dependent services.

After you upgrade a service, you must restart the service.

After you upgrade the PowerCenter Repository Service, you must restart the service and its dependent services.

The first time you enable the Metadata Manager Service after you upgrade it, the service takes a long time to start.

Service Upgrade for Data Quality 9.0.1

Before you upgrade services, verify that the services are enabled. You must upgrade the Model Repository Service before you upgrade Data Integration Service.

A user with the Administrator role on the domain, the Model Repository Service, and the Data Integration Service can upgrade services.

To upgrade services, upgrade the following object types:

- Model Repository Service.
- Data Integration Service.
- Profiling Service Module for Data Integration Service.

Service Upgrade for Data Services 9.0.1

Before you upgrade services, verify that the services are enabled. You must upgrade the Model Repository Service before you upgrade Data Integration Service.

A user with the Administrator role on the domain, the Model Repository Service, and the Data Integration Service can upgrade services.

To upgrade services, upgrade the following object types:

- Model Repository Service.
- Data Integration Service.
- If Data Services 9.0.1 has the profiling option, upgrade the Profiling Service Module for Data Integration Service.

Service Upgrade for PowerCenter 9.0.1

You must upgrade the Metadata Manager Service.

A user with the Administrator role on the domain can upgrade the Metadata Manager Service.

Before you upgrade a Metadata Manager Service, verify that the service is disabled.

Service Upgrade for PowerCenter 8.6.1

You must upgrade the PowerCenter Repository Service, Reporting Service, and Metadata Manager Service.

Before you upgrade PowerCenter 8.6.1 services, verify the following prerequisites:

- You have the Administrator role on the domain.
- PowerCenter Repository Services are enabled and running in exclusive mode.
- Reporting Services and Metadata Manager Services are disabled.

Service Upgrade for PowerCenter 8.5.x or 8.6

You must upgrade all PowerCenter 8.5.x or 8.6 Repository Services.

A user with the Administrator role on the domain can upgrade the PowerCenter Repository Service.

Before you upgrade a PowerCenter Repository Service, verify that the service is enabled and running in exclusive mode.

Service Upgrade for PowerCenter 8.1.x

Before you upgrade PowerCenter 8.1.x services, verify the following prerequisites:

- If you upgrade a repository that uses LDAP authentication, run the infacmd isp SetRepositoryLDAPConfiguration command to update LDAP configuration properties. Optionally, run infacmd isp ListRepoLDAPConfiguration to list LDAP configuration parameters.
- PowerCenter Repository Services are enabled and running in exclusive mode.
- You have the Administrator role on the domain.

To upgrade services, upgrade the following object types:

1. PowerCenter Repository Service
2. Users and groups of each PowerCenter Repository Service

Upgrading Users and Groups

When you upgrade the PowerCenter Repository Service users and groups, the Service Manager moves the users and groups to the domain. You can assign permissions to users after you upgrade users and groups.

You can upgrade users and groups one time for each repository.

Rules and Guidelines for Upgrading Native Users

Review the following rules and guidelines before you upgrade users in a repository:

- The default repository administrator in the repository is merged with the existing default Administrator user account in the domain. The password for the default repository administrator is not merged. You can change the password for the Administrator user account after you complete the user upgrade process.
- The names of upgraded users and groups must conform to the same rules as the names of users and groups in the domain. During the upgrade, the names of users and groups that are not valid are modified to conform to the following rules:
  - Any character in the user or group name that is not valid is replaced with an underscore. A numeric suffix is added to the name. For example, the user name Tom*Jones is modified to Tom_Jones0. The following characters are not valid for user or group names: , + " \ < > ; / * % ?
  - If the new name with underscore and suffix exists in the native security domain, the suffix is increased by one.
  - If a user or group name exceeds 80 characters, the name is shortened to 75 characters plus a numeric suffix. If the new name exists in the security domain, the suffix is increased by one. If the modified name exceeds 80 characters, the user account is not upgraded.
- During the upgrade, any tab, carriage return, or character that is not valid in user or group descriptions is replaced with a space. The characters < > “ are not valid in user and group descriptions. For example, the description [<title>An example</title>] is modified to [title An example /title].
- The user and group names are not case sensitive. A user account in the PowerCenter repository with the name JSmith is a duplicate of a user account in the domain with the name jsmith.

Rules and Guidelines for Upgrading LDAP Users

Review the following rules and guidelines before you upgrade users in a repository that uses LDAP authentication:

- If the repository uses LDAP authentication, native users in the repository are not valid and will not be upgraded.
- The repository administrator user does not retain Administrator privileges. After you upgrade, use the user name Administrator to perform domain administrator tasks. The Administrator user can assign privileges to the previous repository administrator user after you upgrade users.
- If the repository you upgrade uses LDAP authentication, you must create a security domain and import LDAP users into the domain before you upgrade users and groups. The domain does not verify that upgraded LDAP users are associated with the LDAP server that PowerCenter used for LDAP.
- LDAP users that are not part of a security domain are not upgraded. The Administrator is granted permission on all repository objects owned by LDAP users that are not upgraded.

Service Upgrade Wizard

Use the service upgrade wizard to upgrade services.

The service upgrade wizard provides the following options:

- Upgrade multiple services.

- Enable services before the upgrade.
- Automatically or manually reconcile user name and group conflicts.
- Display upgraded services in a list along with services that require an upgrade.
- Save the current or previous upgrade report.
- Automatically restart the services after they have been upgraded.

You can access the service upgrade wizard from the Manage menu in the header area.

Upgrade Report

The upgrade report contains the upgrade start time, upgrade end time, upgrade status, and upgrade processing details. The Services Upgrade Wizard generates the upgrade report.

To save the upgrade report, choose one of the following options:

Save Report

The **Save Report** option appears on step 4 of the service upgrade wizard.

Save Previous Report

The second time you run the service upgrade wizard, the **Save Previous Report** option appears on step 1 of the service upgrade wizard. If you did not save the upgrade report after upgrading services, you can select this option to view or save the previous upgrade report.

Running the Service Upgrade Wizard

Use the service upgrade wizard to upgrade services.

1. In the Informatica Administrator header area click **Manage** > **Upgrade**.
2. Select the objects to upgrade.
3. Optionally, specify if you want to **Automatically recycle services after upgrade**.

   If you choose to automatically recycle services after upgrade, the upgrade wizard restarts the services after they have been upgraded.
4. Optionally, specify if you want to **Automatically reconcile user and group name conflicts**.
5. Click **Next**.
6. If dependency errors exist, the **Dependency Errors** dialog box appears. Review the dependency errors and click **OK**. Then, resolve dependency errors and click **Next**.
7. Enter the repository login information. Optionally, choose to use the same login information for all repositories.
8. Click **Next**.

   The service upgrade wizard upgrades each service and displays the status and processing details.
9. If you are upgrading 8.1.1 PowerCenter Repository Service users and groups for a repository that uses an LDAP authentication, select the LDAP security domain and click **OK**.
10. If the **Reconcile Users and Groups** dialog box appears, specify a resolution for each conflict and click **OK**.

    This dialog box appears when you upgrade 8.1.1 PowerCenter Repository Service users and groups and you choose not to automatically reconcile user and group conflicts.
11. When the upgrade completes, the **Summary** section displays the list of services and their upgrade status. Click each service to view the upgrade details in the **Service Details** section.
12. Optionally, click **Save Report** to save the upgrade details to a file.

If you choose not to save the report, you can click **Save Previous Report** the next time you launch the service upgrade wizard.

13. Click **Close**.
14. If you did not choose to automatically recycle services after upgrade, restart upgraded services.

    After you upgrade the PowerCenter Repository Service, you must restart the service and its dependent services.

Users and Groups Conflict Resolution

When you upgrade PowerCenter Repository Service users and groups, you can select a resolution for user name and group name conflicts.

Use the service upgrade wizard to automatically use the same resolution for all conflicts or manually specify a resolution for each conflict.

The following table describes the conflict resolution options for users and groups:

Resolution	Description
Merge with or Merge	Adds the privileges of the user or group in the repository to the privileges of the user or group in the domain. Retains the password and properties of the user account in the domain, including full name, description, email address, and phone. Retains the parent group and description of the group in the domain. Maintains user and group relationships. When a user is merged with a domain user, the list of groups the user belongs to in the repository is merged with the list of groups the user belongs to in the domain. When a group is merged with a domain group, the list of users the group is merged with the list of users the group has in the domain. You cannot merge multiple users or groups with one user or group.
Rename	Creates a new group or user account with the group or user name you provide. The new group or user account takes the privileges and properties of the group or user in the repository.
Upgrade	No conflict. Upgrades user and assign permissions.

When you upgrade a repository that uses LDAP authentication, the **Users and Groups Without Conflicts** section of the conflict resolution screen lists the users that will be upgraded. LDAP user privileges are merged with users in the security domain that have the same name. The LDAP user retains the password and properties of the account in the LDAP security domain.

The **Users and Groups With Conflicts** section shows a list of users that are not in the security domain and will not be upgraded. If you want to upgrade users that are not in the security domain, use the Security page to update the security domain and synchronize users before you upgrade users.

CHAPTER 6

Domain Security

This chapter includes the following topics:

- Domain Security Overview, 53
- Secure Communication Within the Domain, 53
- Secure Communication with External Components, 55

Domain Security Overview

You can configure Informatica domain components to use the Secure Sockets Layer (SSL) protocol or the Transport Layer Security (TLS) protocol to encrypt connections with other components. When you enable SSL or TLS for domain components, you ensure secure communication.

You can configure secure communication in the following ways:

Between services within the domain

You can configure secure communication between services within the domain.

Between the domain and external components

You can configure secure communication between Informatica domain components and web browsers or web service clients.

Each method of configuring secure communication is independent of the other methods. When you configure secure communication for one set of components, you do not need to configure secure communication for any other set.

Secure Communication Within the Domain

To configure services to use the TLS protocol to transfer data securely within the domain, enable the TLS protocol for the domain.

When you enable the TLS protocol for the domain, you secure the communication between the following components:

- Between Service Managers on all domain nodes
- Between application services
- Between application services and application clients

- Between infacmd and Service Managers and application services

You cannot enable the TLS protocol for all application service types. For example, enabling TLS for the domain does not apply to the PowerCenter Repository Service, PowerCenter Integration Service, Metadata Manager Service, Reporting Service, SAP BW Service, or Web Services Hub.

The services use a self-signed keystore file generated by Informatica. The keystore file stores the certificates and keys that authorize the secure connection between the services and other domain components.

You can use the Administrator tool or the infasetup command line program to configure secure communication within the domain.

Note: Passwords are encrypted for all application services, application clients, and command line programs regardless of whether the TLS protocol is enabled for the domain.

Configuring Secure Communication Within the Domain

You can use the Administrator tool to enable or disable the TLS protocol for the domain. When you enable the TLS protocol, you configure secure communication between services within the domain.

Verify that all domain nodes are available before you enable TLS for the domain. If a node is unavailable, then use infasetup commands to enable TLS for the Service Manager on the unavailable node.

1. On the **Domain** tab, select the **Services and Nodes** view.
2. In the Navigator, select the domain.
3. In the General Properties area, click **Edit**.
4. Select **Enable Transport Layer Security (TLS)** and click **OK**.
5. Shut down and restart the domain to apply the change.

TLS Configuration Using infasetup

You can use the infasetup command line program to enable or disable the TLS protocol for the domain. When you enable the TLS protocol, you configure secure communication between services within the domain.

Verify that all domain nodes are available before you enable TLS for the domain. After you change the TLS protocol for the domain, you must shut down and restart the domain to apply the change.

To configure secure communication within the domain, use one of the following infasetup commands:

DefineDomain

To enable the TLS protocol when you create a domain, use the DefineDomain command and set the enable TLS option to true.

UpdateGatewayNode

To enable the TLS protocol for an existing domain, use the UpdateGatewayNode command and set the enable TLS option to true. To disable the TLS protocol for an existing domain, use the UpdateGatewayNode command and set the enable TLS option to false.

To enable or disable the TLS protocol for the Service Manager on a gateway node that was unavailable when you changed the TLS protocol for the domain, use the UpdateGatewayNode command.

UpdateWorkerNode

To enable or disable the TLS protocol for the Service Manager on a worker node that was unavailable when you changed the TLS protocol for the domain, use the UpdateWorkerNode command.

DefineGatewayNode

To add a gateway node to a domain that has the TLS protocol enabled, use the DefineGatewayNode command. When you define the node, enable the TLS protocol for the Service Manager on the node.

DefineWorkerNode

To add a worker node to a domain that has the TLS protocol enabled, use the DefineWorkerNode command. When you define the node, enable the TLS protocol for the Service Manager on the node.

Secure Communication with External Components

You can configure secure communication between Informatica domain components and web browsers or web service clients.

You can configure secure communication between the following Informatica domain components and external components:

Informatica web application and web browser

You can configure secure communication for Informatica web applications to transfer data securely between the web browser and the web application. To secure the connection to the Administrator tool, configure HTTPS for all nodes in the domain. To secure the connection to the Analyst tool, Metadata Manager application, Data Analyzer, or Web Services Hub Console, configure the HTTPS port that the web application runs on.

Data Integration Service and web service client

To use the TLS protocol for a secure connection between a web service client and the Data Integration Service, configure the HTTPS port that the Data Integration Service runs on and enable TLS for the web service.

Secure Communication to the Administrator Tool

To use the SSL protocol for a secure connection to the Administrator tool, configure HTTPS for all nodes in the domain. You can configure HTTPS during installation or using infasetup commands.

To configure HTTPS for a node, define the following information:

- HTTPS port. The port used by the node for communication to the Administrator tool. When you configure an HTTPS port, the gateway or worker node port does not change. Application services and application clients communicate with the Service Manager using the gateway or worker node port.
- Keystore file name and location. A file that includes private or public key pairs and associated certificates. You can create the keystore file during installation or you can create a keystore file with a *keytool*. You can use a self-signed certificate or a certificate signed by a certificate authority.
- Keystore password. A plain-text password for the keystore file.

After you configure the node to use HTTPS, the Administrator tool URL redirects to the following HTTPS enabled site:

```
https://<host>:<https port>/administrator
```

When the node is enabled for HTTPS with a self-signed certificate, a warning message appears when you access the Administrator tool. To enter the site, accept the certificate.

The HTTPS port and keystore file location you configure appear in the Node Properties.

Note: If you configure HTTPS for the Administrator tool on a domain that runs on 64-bit AIX, Internet Explorer requires TLS 1.0. To enable TLS 1.0, click Tools > Internet Options > Advanced. The TLS 1.0 setting is listed below the Security heading.

Creating a Keystore File

You can create the keystore file during installation or you can create a keystore file with a *keytool*.

keytool is a utility that generates and stores private or public key pairs and associated certificates in a file called a "keystore." When you generate a public or private key pair, *keytool* wraps the public key into a self-signed certificate. You can use the self-signed certificate or use a certificate signed by a certificate authority.

Find *keytool* in one of the following directories:

- `%JAVA_HOME%\jre\bin`
- java\bin directory of the Informatica installation directory

For more information about using keytool, see the documentation on the Sun web site:

`http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html`

HTTPS Configuration Using infasetup

Use the infasetup command line program to configure HTTPS for the Administrator tool.

Use one of the following infasetup commands:

- To enable HTTPS support for a worker node, use the infasetup UpdateWorkerNode command.
- To enable HTTPS support for a gateway node, use the infasetup UpdateGatewayNode command.
- To create a new worker or gateway node with HTTPS support, use the infasetup DefineDomain, DefineGatewayNode, or DefineWorkerNode command.

To disable HTTPS support for a node, use the infasetup UpdateGatewayNode or UpdateWorkerNode command. When you update the node, set the HTTPS port option to zero.

CHAPTER 7

Users and Groups

This chapter includes the following topics:

- Users and Groups Overview, 57
- Understanding User Accounts, 58
- Understanding Authentication and Security Domains , 60
- Setting Up LDAP Authentication, 60
- Managing Users, 66
- Managing Groups, 69
- Managing Operating System Profiles, 71

Users and Groups Overview

To access the application services and objects in the Informatica domain and to use the application clients, you must have a user account. The tasks you can perform depend on the type of user account you have.

During installation, a default administrator user account is created. Use the default administrator account to initially log in to the Informatica domain and create application services, domain objects, and other user accounts. When you log in to the Informatica domain after installation, change the password to ensure security for the Informatica domain and applications.

User account management in Informatica involves the following key components:

- Users. You can set up different types of user accounts in the Informatica domain. Users can perform tasks based on the roles, privileges, and permissions assigned to them.
- Authentication. When a user logs in to an application client, the Service Manager authenticates the user account in the Informatica domain and verifies that the user can use the application client. The Informatica domain can use native or LDAP authentication to authenticate users. The Service Manager organizes user accounts and groups by security domain. It authenticates users based on the security domain the user belongs to.
- Groups. You can set up groups of users and assign different roles, privileges, and permissions to each group. The roles, privileges, and permissions assigned to the group determines the tasks that users in the group can perform within the Informatica domain.
- Privileges and roles. Privileges determine the actions that users can perform in application clients. A role is a collection of privileges that you can assign to users and groups. You assign roles or privileges to users and groups for the domain and for each application service in the domain.

- Operating system profiles. If you run the PowerCenter Integration Service on UNIX, you can configure the PowerCenter Integration Service to use operating system profiles when running workflows. You can create and manage operating system profiles on the Security tab of the Administrator tool.

Default Everyone Group

An Informatica domain includes a default group named Everyone. All users in the domain belong to the group.

You can assign privileges, roles, and permissions to the Everyone group to grant the same access to all users. You cannot complete the following tasks for the Everyone group:

- Edit or delete the Everyone group.
- Add users to or remove users from the Everyone group.
- Move a group to the Everyone group.

Understanding User Accounts

An Informatica domain can have the following types of accounts:

- Default administrator
- Domain administrator
- Application client administrator
- User

Default Administrator

When you install Informatica services, the installer creates the default administrator with a user name and password you provide. You can use the default administrator account to initially log in to the Administrator tool.

The default administrator has administrator permissions and privileges on the domain and all application services. The default administrator can perform the following tasks:

- Create, configure, and manage all objects in the domain, including nodes, application services, and administrator and user accounts.
- Configure and manage all objects and user accounts created by other domain administrators and application client administrators.
- Log in to any application client.

The default administrator is a user account in the native security domain. You cannot create a default administrator. You cannot disable or modify the user name or privileges of the default administrator. You can change the default administrator password.

Domain Administrator

A domain administrator can create and manage objects in the domain, including user accounts, nodes, grids, licenses, and application services.

The domain administrator can log in to the Administrator tool and create and configure application services in the domain. However, by default, the domain administrator cannot log in to application clients. The default

administrator must explicitly give a domain administrator full permissions and privileges to the application services so that they can log in and perform administrative tasks in the application clients.

To create a domain administrator, assign a user the Administrator role for a domain.

Application Client Administrator

An application client administrator can create and manage objects in an application client. You must create administrator accounts for the application clients. To limit administrator privileges and keep application clients secure, create a separate administrator account for each application client.

By default, the application client administrator does not have permissions or privileges on the domain. Without permissions or privileges on the domain, the application client administrator cannot log in to the Administrator tool to manage the application service.

You can set up the following application client administrators:

- Data Analyzer administrator. Has full permissions and privileges in Data Analyzer. The Data Analyzer administrator can log in to Data Analyzer to create and manage Data Analyzer objects and perform all tasks in the application client.

  To create a Data Analyzer administrator, assign a user the Administrator role for a Reporting Service.
- Informatica Analyst administrator. Has full permissions and privileges in Informatica Analyst. The Informatica Analyst administrator can log in to Informatica Analyst to create and manage projects and objects in projects and perform all tasks in the application client.

  To create an Informatica Analyst administrator, assign a user the Administrator role for an Analyst Service and for the associated Model Repository Service.
- Informatica Developer administrator. Has full permissions and privileges in Informatica Developer. The Informatica Developer administrator can log in to Informatica Developer to create and manage projects and objects in projects and perform all tasks in the application client.

  To create an Informatica Developer administrator, assign a user the Administrator role for a Model Repository Service.
- Metadata Manager administrator. Has full permissions and privileges in Metadata Manager. The Metadata Manager administrator can log in to Metadata Manager to create and manage Metadata Manager objects and perform all tasks in the application client.

  To create a Metadata Manager administrator, assign a user the Administrator role for a Metadata Manager Service.
- PowerCenter Client administrator. Has full permissions and privileges on all objects in the PowerCenter Client. The PowerCenter Client administrator can log in to the PowerCenter Client to manage the PowerCenter repository objects and perform all tasks in the PowerCenter Client. The PowerCenter Client administrator can also perform all tasks in the *pmrep* and *pmcmd* command line programs.

  To create a PowerCenter Client administrator, assign a user the Administrator role for a PowerCenter Repository Service.

User

A user with an account in the Informatica domain can perform tasks in the application clients.

Typically, the default administrator or a domain administrator creates and manages user accounts and assigns roles, permissions, and privileges in the Informatica domain. However, any user with the required domain privileges and permissions can create a user account and assign roles, permissions, and privileges.

Users can perform tasks in application clients based on the privileges and permissions assigned to them.

Understanding Authentication and Security Domains

When a user logs in to an application client, the Service Manager authenticates the user account in the Informatica domain and verifies that the user can use the application client. The Service Manager uses native and LDAP authentication to authenticate users logging in to the Informatica domain.

You can use more than one type of authentication in an Informatica domain. By default, the Informatica domain uses native authentication. You can configure the Informatica domain to use LDAP authentication in addition to native authentication.

The Service Manager organizes user accounts and groups by security domains. A security domain is a collection of user accounts and groups in an Informatica domain. The Service Manager stores user account information for each security domain in the domain configuration database.

The authentication method used by an Informatica domain determines the security domains available in an Informatica domain. An Informatica domain can have more than one security domain. The Service Manager authenticates users based on their security domain.

Native Authentication

For native authentication, the Service Manager stores all user account information and performs all user authentication within the Informatica domain. When a user logs in, the Service Manager uses the native security domain to authenticate the user name and password.

By default, the Informatica domain contains a native security domain. The native security domain is created at installation and cannot be deleted. An Informatica domain can have only one native security domain. You create and maintain user accounts of the native security domain in the Administrator tool. The Service Manager stores details of the user accounts, including passwords and groups, in the domain configuration database.

LDAP Authentication

To enable an Informatica domain to use LDAP authentication, you must set up a connection to an LDAP directory service and specify the users and groups that can have access to the Informatica domain. If the LDAP server uses the SSL protocol, you must also specify the location of the SSL certificate.

After you set up the connection to an LDAP directory service, you can import the user account information from the LDAP directory service into an LDAP security domain. Set a filter to specify the user accounts to be included in an LDAP security domain. An Informatica domain can have multiple LDAP security domains. When a user logs in, the Service Manager authenticates the user name and password against the LDAP directory service.

You can set up LDAP security domains in addition to the native security domain. For example, you use the Administrator tool to create users and groups in the native security domain. If you also have users in an LDAP directory service who use application clients, you can import the users and groups from the LDAP directory service and create an LDAP security domain. When users log in to application clients, the Service Manager authenticates them based on their security domain.

Note: The Service Manager requires that LDAP users log in to an application client using a password even though an LDAP directory service may allow a blank password for anonymous mode.

Setting Up LDAP Authentication

If you have user accounts in an enterprise LDAP directory service that you want to give access to application clients, you can configure the Informatica domain to use LDAP authentication. Create an LDAP security domain

and set up a filter to specify the users and groups in the LDAP directory service who can access application clients and be included in the security domain.

The Service Manager imports the users and groups from the LDAP directory service into an LDAP security domain. You can set up a schedule for the Service Manager to periodically synchronize the list of users and groups in the LDAP security domain with the list of users and groups in the LDAP directory service. During synchronization, the Service Manager imports users and groups from the LDAP directory service and deletes any user or group that no longer exists in the LDAP directory service.

When a user in an LDAP security domain logs in to an application client, the Service Manager passes the user account name and password to the LDAP directory service for authentication. If the LDAP server uses SSL security protocol, the Service Manager sends the user account name and password to the LDAP directory service using the appropriate SSL certificates.

You can use the following LDAP directory services for LDAP authentication:

- Microsoft Active Directory Service
- Sun Java System Directory Service
- Novell e-Directory Service
- IBM Tivoli Directory Service
- Open LDAP Directory Service

You create and manage LDAP users and groups in the LDAP directory service.

You can assign roles, privileges, and permissions to users and groups in an LDAP security domain. You can assign LDAP user accounts to native groups to organize them based on their roles in the Informatica domain. You cannot use the Administrator tool to create, edit, or delete users and groups in an LDAP security domain.

Use the LDAP Configuration dialog box to set up LDAP authentication for the Informatica domain.

To display the LDAP Configuration dialog box in the Security tab of the Administrator tool, click LDAP Configuration on the Security Actions menu.

To set up LDAP authentication for the domain, complete the following steps:

1. Set up the connection to the LDAP server.
2. Configure a security domain.
3. Schedule the synchronization times.

Step 1. Set Up the Connection to the LDAP Server

When you set up a connection to an LDAP server, the Service Manager imports the user accounts of all LDAP security domains from the LDAP server.

When you configure the LDAP server connection, indicate that the Service Manager must ignore case-sensitivity for distinguished name attributes when it assigns users to their corresponding groups. If the Service Manager does not ignore case sensitivity, the Service Manager may not assign all users to groups in the LDAP directory service.

If you modify the LDAP connection properties to connect to a different LDAP server, ensure that the user and group filters in the LDAP security domains are correct for the new LDAP server and include the users and groups that you want to use in the Informatica domain.

To set up a connection to the LDAP server:

1. In the LDAP Configuration dialog box, click the LDAP Connectivity tab.
2. Configure the LDAP server properties.

You may need to consult the LDAP administrator to get the information on the LDAP directory service.

The following table describes the LDAP server configuration properties:

Property	Description
Server name	Name of the machine hosting the LDAP directory service.
Port	Listening port for the LDAP server. This is the port number to communicate with the LDAP directory service. Typically, the LDAP server port number is 389. If the LDAP server uses SSL, the LDAP server port number is 636. The maximum port number is 65535.
LDAP Directory Service	Type of LDAP directory service. Select from the following directory services: - Microsoft Active Directory Service - Sun Java System Directory Service - Novell e-Directory Service - IBM Tivoli Directory Service - Open LDAP Directory Service
Name	Distinguished name (DN) for the principal user. The user name often consists of a common name (CN), an organization (O), and a country (C). The principal user name is an administrative user with access to the directory. Specify a user that has permission to read other user entries in the LDAP directory service. Leave blank for anonymous login. For more information, see the documentation for the LDAP directory service.
Password	Password for the principal user. Leave blank for anonymous login.
Use SSL Certificate	Indicates that the LDAP directory service uses Secure Socket Layer (SSL) protocol.
Trust LDAP Certificate	Determines whether the Service Manager can trust the SSL certificate of the LDAP server. If selected, the Service Manager connects to the LDAP server without verifying the SSL certificate. If not selected, the Service Manager verifies that the SSL certificate is signed by a certificate authority before connecting to the LDAP server. To enable the Service Manager to recognize a self-signed certificate as valid, specify the truststore file and password to use.
Not Case Sensitive	Indicates that the Service Manager must ignore case-sensitivity for distinguished name attributes when assigning users to groups. Enable this option.
Group Membership Attribute	Name of the attribute that contains group membership information for a user. This is the attribute in the LDAP group object that contains the DNs of the users or groups who are members of a group. For example, *member* or *memberof*.
Maximum Size	Maximum number of groups and user accounts to import into a security domain. For example, if the value is set to 100, you can import a maximum of 100 groups and 100 user accounts into the security domain. If the number of user and groups to be imported exceeds the value for this property, the Service Manager generates an error message and does not import any user. Set this property to a higher value if you have many users and groups to import. Default is 1000.

3. Click Test Connection to verify that the connection configuration is correct.

Step 2. Configure Security Domains

Create a security domain for each set of user accounts and groups you want to import from the LDAP server. Set up search bases and filters to define the set of user accounts and groups to include in a security domain. The

Service Manager uses the user search bases and filters to import user accounts and the group search bases and filters to import groups. The Service Manager imports groups and the list of users that belong to the groups. It imports the groups that are included in the group filter and the user accounts that are included in the user filter.

The names of users and groups to be imported from the LDAP directory service must conform to the same rules as the names of native users and groups. The Service Manager does not import LDAP users or groups if names do not conform to the rules of native user and group names.

Note: Unlike native user names, LDAP user names can be case-sensitive.

When you set up the LDAP directory service, you can use different attributes for the unique ID (UID). The Service Manager requires a particular UID to identify users in each LDAP directory service. Before you configure the security domain, verify that the LDAP directory service uses the required UID.

The following table provides the required UID for each LDAP directory service:

LDAP Directory Service	UID
IBMTivoliDirectory	uid
Microsoft Active Directory	sAMAccountName
NovellE	uid
OpenLDAP	uid
SunJavaSystemDirectory	uid

The Service Manager does not import the LDAP attribute that indicates that a user account is enabled or disabled. You must enable or disable an LDAP user account in the Administrator tool. The status of the user account in the LDAP directory service affects user authentication in application clients. For example, a user account is enabled in the Informatica domain but disabled in the LDAP directory service. If the LDAP directory service allows disabled user accounts to log in, then the user can log in to application clients. If the LDAP directory service does not allow disabled user accounts to log in, then the user cannot log in to application clients.

Note: If you modify the LDAP connection properties to connect to a different LDAP server, the Service Manager does not delete the existing security domains. You must ensure that the LDAP security domains are correct for the new LDAP server. Modify the user and group filters in the existing security domains or create security domains so that the Service Manager correctly imports the users and groups that you want to use in the Informatica domain.

Complete the following steps to add an LDAP security domain:

1. In the LDAP Configuration dialog box, click the Security Domains tab.
2. Click Add.
3. Use LDAP query syntax to create filters to specify the users and groups to be included in this security domain.

   You may need to consult the LDAP administrator to get the information on the users and groups available in the LDAP directory service.

   The following table describes the filter properties that you can set up for a security domain:

Property	Description
Security Domain	Name of the LDAP security domain. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or contain the following special characters: , + / < > @ ; \ % ?

Property	Description
	The name can contain an ASCII space character except for the first and last character. All other space characters are not allowed.
User search base	Distinguished name (DN) of the entry that serves as the starting point to search for user names in the LDAP directory service. The search finds an object in the directory according to the path in the distinguished name of the object. For example, in Microsoft Active Directory, the distinguished name of a user object might be cn=UserName,ou=OrganizationalUnit,dc=DomainName, where the series of relative distinguished names denoted by dc=DomainName identifies the DNS domain of the object.
User filter	An LDAP query string that specifies the criteria for searching for users in the directory service. The filter can specify attribute types, assertion values, and matching criteria. For example: `(objectclass=*)` searches all objects. `(&(objectClass=user)(!(cn=susan)))` searches all user objects except "susan." For more information about search filters, see the documentation for the LDAP directory service.
Group search base	Distinguished name (DN) of the entry that serves as the starting point to search for group names in the LDAP directory service.
Group filter	An LDAP query string that specifies the criteria for searching for groups in the directory service.

4. Click Preview to view a subset of the list of users and groups that fall within the filter parameters.

   If the preview does not display the correct set of users and groups, modify the user and group filters and search bases to get the correct users and groups.

5. To add another LDAP security domain, repeat steps 2 through 4.
6. To immediately synchronize the users and groups in the security domains with the users and groups in the LDAP directory service, click Synchronize Now.

   The Service Manager immediately synchronizes all LDAP security domains with the LDAP directory service. The time it takes for the synchronization process to complete depends on the number of users and groups to be imported.

7. Click OK to save the security domains.

Step 3. Schedule the Synchronization Times

By default, the Service Manager does not have a scheduled time to synchronize with the LDAP directory service. To ensure that the list of users and groups in the LDAP security domains is accurate, create a schedule for the Service Manager to synchronize the users and groups.

You can schedule the time of day when the Service Manager synchronizes the list of users and groups in the LDAP security domains with the LDAP directory service. The Service Manager synchronizes the LDAP security domains with the LDAP directory service every day during the times you set.

Note: During synchronization, the Service Manager locks the user account it synchronizes. Users might not be able to log in to application clients. If users are logged in to application clients when synchronization starts, they might not be able to perform tasks. The duration of the synchronization process depends on the number of users and groups to be synchronized. To avoid usage disruption, synchronize the security domains during times when most users are not logged in.

1. On the LDAP Configuration dialog box, click the Schedule tab.
2. Click the Add button (+) to add a time.

The synchronization schedule uses a 24-hour time format.

You can add as many synchronization times in the day as you require. If the list of users and groups in the LDAP directory service changes often, you can schedule the Service Manager to synchronize multiple times a day.

3. To immediately synchronize the users and groups in the security domains with the users and groups in the LDAP directory service, click Synchronize Now.
4. Click OK to save the synchronization schedule.

   Note: If you restart the Informatica domain before the Service Manager synchronizes with the LDAP directory service, the added times are lost.

Deleting an LDAP Security Domain

To permanently prohibit users in an LDAP security domain from accessing application clients, you can delete the LDAP security domain. When you delete an LDAP security domain, the Service Manager deletes all user accounts and groups in the LDAP security domain from the domain configuration database.

1. In the LDAP Configuration dialog box, click the Security Domains tab.

   The LDAP Configuration dialog box displays the list of security domains.
2. To ensure that you are deleting the correct security domain, click the security domain name to view the filter used to import the users and groups and verify that it is the security domain you want to delete.
3. Click the Delete button next to a security domain to delete the security domain.
4. Click OK to confirm that you want to delete the security domain.

Using a Self-Signed SSL Certificate

You can connect to an LDAP server that uses an SSL certificate signed by a certificate authority (CA). By default, the Service Manager does not connect to an LDAP server that uses a self-signed certificate.

To use a self-signed certificate, import the self-signed certificate into a truststore file and use the INFA_JAVA_OPTS environment variable to specify the truststore file and password:

```
setenv INFA_JAVA_OPTS -Djavax.net.ssl.trustStore=<TrustStoreFile>
-Djavax.net.ssl.trustStorePassword=<TrustStorePassword>
```

On Windows, configure INFA_JAVA_OPTS as a system variable.

Restart the node for the change to take effect. The Service Manager uses the truststore file to verify the SSL certificate.

keytool is a key and certificate management utility that allows you to generate and administer keys and certificates for use with the SSL security protocol. You can use keytool to create a truststore file or to import a certificate to an existing truststore file. You can find the keytool utility in the following directory:

```
<PowerCenterClientDir>\CMD_Utilities\PC\java\bin
```

For more information about using keytool, see the documentation on the Sun web site:

```
http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html
```

Using Nested Groups in the LDAP Directory Service

An LDAP security domain can contain nested LDAP groups. The Service Manager can import nested groups that are created in the following manner:

- Create the groups under the same organizational units (OU).
- Set the relationship between the groups.

For example, you want to create a nested grouping where GroupB is a member of GroupA and GroupD is a member of GroupC.

1. Create GroupA, GroupB, GroupC, and GroupD within the same OU.
2. Edit GroupA, and add GroupB as a member.
3. Edit GroupC, and add GroupD as a member.

You cannot import nested LDAP groups into an LDAP security domain that are created in a different way.

Managing Users

You can create, edit, and delete users in the native security domain. You cannot delete or modify the properties of user accounts in the LDAP security domains. You cannot modify the user assignments to LDAP groups.

You can assign roles, permissions, and privileges to a user account in the native security domain or an LDAP security domain. The roles, permissions, and privileges assigned to the user determines the tasks the user can perform within the Informatica domain.

Adding Native Users

Add, edit, or delete native users on the Security tab.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Create User.
3. Enter the following details for the user:

Property	Description
Login Name	Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? & The name can include an ASCII space character except for the first and last character. All other space characters are not allowed. **Note:** Data Analyzer uses the user account name and security domain in the format *UserName@SecurityDomain* to determine the length of the user login name. The combination of the user name, @ symbol, and security domain cannot exceed 128 characters.
Password	Password for the user account. The password can be from 1 through 80 characters long.
Confirm Password	Enter the password again to confirm. You must retype the password. Do not copy and paste the password.
Full Name	Full name for the user account. The full name cannot include the following special characters: < > “ **Note:** In Data Analyzer, the full name property is equivalent to three separate properties named first name, middle name, and last name.
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > “

Property	Description
Email	Email address for the user. The email address cannot include the following special characters: < > “ Enter the email address in the format UserName@Domain.
Phone	Telephone number for the user. The telephone number cannot include the following special characters: < > “

4. Click OK to save the user account.

   After you create a user account, the details panel displays the properties of the user account and the groups that the user is assigned to.

Editing General Properties of Native Users

You cannot change the login name of a native user. You can change the password and other details for a native user account.

1. In the Administrator tool, click the Security tab.
2. In the Users section of the Navigator, select a native user account and click Edit.
3. To change the password, select Change Password.

   The Security tab clears the Password and Confirm Password fields.
4. Enter a new password and confirm.
5. Modify the full name, description, email, and phone as necessary.
6. Click OK to save the changes.

Assigning Users to Native Groups

You can assign native or LDAP user accounts to native groups. You cannot change the assignment of LDAP user accounts to LDAP groups.

1. In the Administrator tool, click the Security tab.
2. In the Users section of the Navigator, select a native or LDAP user account and click Edit.
3. Click the Groups tab.
4. To assign a user to a group, select a group name in the All Groups column and click Add.

   If nested groups do not display in the All Groups column, expand each group to show all nested groups.

   You can assign a user to more than group. Use the Ctrl or Shift keys to select multiple groups at the same time.
5. To remove a user from a group, select a group in the Assigned Groups column and click Remove.
6. Click OK to save the group assignments.

Enabling and Disabling User Accounts

Users with active accounts can log in to application clients and perform tasks based on their permissions and privileges. If you do not want users to access application clients temporarily, you can disable their accounts. You can enable or disable user accounts in the native or an LDAP security domain. When you disable a user account, the user cannot log in to the application clients.

To disable a user account, select a user account in the Users section of the Navigator and click Disable. When you select a disabled user account, the Security tab displays a message that the user account is disabled. When a user account is disabled, the Enable button is available. To enable the user account, click Enable.

You cannot disable the default administrator account.

Note: When the Service Manager imports a user account from the LDAP directory service, it does not import the LDAP attribute that indicates that a user account is enabled or disabled. The Service Manager imports all user accounts as enabled user accounts. You must disable an LDAP user account in the Administrator tool if you do not want the user to access application clients. During subsequent synchronization with the LDAP server, the user account retains the enabled or disabled status set in the Administrator tool.

Deleting Native Users

To delete a native user account, right-click the user account name in the Users section of the Navigator and select Delete User. Confirm that you want to delete the user account.

You cannot delete the default administrator account. When you log in to the Administrator tool, you cannot delete your user account.

Deleting Users of PowerCenter

When you delete a user who owns objects in the PowerCenter repository, you remove any ownership that the user has over folders, connection objects, deployment groups, labels, or queries. After you delete a user, the default administrator becomes the owner of all objects owned by the deleted user.

When you view the history of a versioned object previously owned by a deleted user, the name of the deleted user appears prefixed by the word "deleted."

Deleting Users of Data Analyzer

When you delete a user, Data Analyzer deletes the alerts, alert email accounts, and personal folders and dashboards associated with the user.

Data Analyzer deletes all reports that a user subscribes to based on the security profile of the report. Data Analyzer keeps a security profile for each user who subscribes to the report. A report that uses user-based security uses the security profile of the user who accesses the report. A report that uses provider-based security uses the security profile of the user who owns the report.

When you delete a user, Data Analyzer does not delete any report in the public folder owned by the user. Data Analyzer can run a report with user-based security even if the report owner does not exist. However, Data Analyzer cannot determine the security profile for a report with provider-based security if the report owner does not exist. Before you delete a user, verify that the reports with provider-based security have a new owner.

For example, you want to delete UserA who has a report in the public folder with provider-based security. Create or select a user with the same security profile as UserA. Identify all the reports with provider-based security in the public folder owned by UserA. Then, have the other user with the same security profile log in and save those reports to the public folder, with provider-based security and the same report name. This ensures that after you delete the user, the reports stay in the public folder with the same security.

Deleting Users of Metadata Manager

When you delete a user who owns shortcuts and folders, Metadata Manager moves the user's personal folder to a folder named Deleted Users owned by the default administrator. The deleted user's personal folder contains all shortcuts and folders created by the user. Any shared folders remain shared after you delete the user.

If the Deleted Users folder contains a folder with the same user name, Metadata Manager names the additional folder "Copy (n) of <username>."

LDAP Users

You cannot add, edit, or delete LDAP users in the Administrator tool. You must manage the LDAP user accounts in the LDAP directory service.

Increasing System Memory for Many Users

Processing time for an Informatica domain restart and for LDAP user synchronization increases proportionally with the number of users in the Informatica domain.

The system memory used by the domain depends on the number of users in the domain. To increase the system memory, configure the INFA_JAVA_OPTS environment variable and specify the value in megabytes. For example, to configure 2048 MB of system memory on UNIX, use the following command:

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

On Windows, configure INFA_JAVA_OPTS as a system variable.

The following table provides the minimum system memory requirements for different amounts of users:

Number of Users	Minimum System Memory
1,000	512 MB (default)
5,000	1024 MB
10,000	1024 MB
20,000	2048 MB
30,000	3072 MB

After you configure the INFA_JAVA_OPTS system variable, restart the node for the changes to take effect.

Managing Groups

You can create, edit, and delete groups in the native security domain. You cannot delete or modify the properties of group accounts in the LDAP security domains.

You can assign roles, permissions, and privileges to a group in the native or an LDAP security domain. The roles, permissions, and privileges assigned to the group determines the tasks that users in the group can perform within the Informatica domain.

Adding a Native Group

Add, edit, or remove native groups on the Security tab.

A native group can contain native or LDAP user accounts or other native groups. You can create multiple levels of native groups. For example, the Finance group contains the AccountsPayable group which contains the OfficeSupplies group. The Finance group is the parent group of the AccountsPayable group and the

AccountsPayable group is the parent group of the OfficeSupplies group. Each group can contain other native groups.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Create Group.
3. Enter the following information for the group:

Property	Description
Name	Name of the group. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Parent Group	Group to which the new group belongs. If you select a native group before you click Create Group, the selected group is the parent group. Otherwise, Parent Group field displays Native indicating that the new group does not belong to a group.
Description	Description of the group. The group description cannot exceed 765 characters or include the following special characters: < > “

4. Click Browse to select a different parent group.

   You can create more than one level of groups and subgroups.
5. Click OK to save the group.

Editing Properties of a Native Group

After you create a group, you can change the description of the group and the list of users in the group. You cannot change the name of the group or the parent of the group. To change the parent of the group, you must move the group to another group.

1. In the Administrator tool, click the Security tab.
2. In the Groups section of the Navigator, select a native group and click Edit.
3. Change the description of the group.
4. To change the list of users in the group, click the Users tab.

   The Users tab displays the list of users in the domain and the list of users assigned to the group.
5. To assign users to the group, select a user account in the All Users column and click Add.
6. To remove a user from a group, select a user account in the Assigned Users column and click Remove.
7. Click OK to save the changes.

Moving a Native Group to Another Native Group

To organize the groups of users in the native security domain, you can set up nested groups and move a group to another group.

To move a native group to another native group, right-click the name of a native group in the Groups section of the Navigator and select Move Group.

Deleting a Native Group

To delete a native group, right-click the group name in the Groups section of the Navigator and select Delete Group.

When you delete a group, the users in the group lose their membership in the group and all permissions or privileges inherited from group.

When you delete a group, the Service Manager deletes all groups and subgroups that belong to the group.

LDAP Groups

You cannot add, edit, or delete LDAP groups or modify user assignments to LDAP groups in the Administrator tool. You must manage groups and user assignments in the LDAP directory service.

Managing Operating System Profiles

If the PowerCenter Integration Service uses operating system profiles, it runs workflows with the settings of the operating system profile assigned to the workflow or to the folder that contains the workflow.

You can create, edit, delete, and assign permissions to operating system profiles in the Operating System Profiles Configuration dialog box.

To display the Operating System Profiles Configuration dialog box, click Operating System Profiles Configuration on the Security Actions menu.

Complete the following steps to configure an operating system profile:

1. Create an operating system profile.
2. Configure the service process variables and environment variables in the operating system profile properties.
3. Assign permissions on operating system profiles.

Create Operating System Profiles

Create operating system profiles if the PowerCenter Integration Service uses operating system profiles.

The following table describes the properties you configure to create an operating system profile:

Property	Description
Name	Name of the operating system profile. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain the following special characters: % * + \ / . ? < > The name can contain an ASCII space character except for the first and last character. All other space characters are not allowed.
System User Name	Name of an operating system user that exists on the machines where the PowerCenter Integration Service runs. The PowerCenter Integration Service runs workflows using the system access of the system user defined for the operating system profile.
$PMRootDir	Root directory accessible by the node. This is the root directory for other service process variables. It cannot include the following special characters:

Property	Description
	* ? < > " | ,

You cannot edit the name or the system user name after you create an operating system profile. If you do not want to use the operating system user specified in the operating system profile, delete the operating system profile. After you delete an operating system profile, assign another operating system profile to the repository folders that the operating system profile was assigned to.

Properties of Operating System Profiles

After you create an operating system profile, configure the operating system profile properties. To edit the properties of an operating system profile, select the profile in the Operating System Profiles Configuration dialog box and then click Edit.

Note: Service process variables that are set in session properties and parameter files override the operating system profile settings.

The following table describes the properties of an operating system profile:

Property	Description
Name	Read-only name of the operating system profile. The name cannot exceed 128 characters. It cannot include spaces or the following special characters: \ / : * ? " < > | [ ] = + ; ,
System User Name	Read-only name of an operating system user that exists on the machines where the PowerCenter Integration Service runs. The PowerCenter Integration Service runs workflows using the system access of the system user defined for the operating system profile.
$PMRootDir	Root directory accessible by the node. This is the root directory for other service process variables. It cannot include the following special characters: * ? < > " | ,
$PMSessionLogDir	Directory for session logs. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SessLogs.
$PMBadFileDir	Directory for reject files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/BadFiles.
$PMCacheDir	Directory for index and data cache files. You can increase performance when the cache directory is a drive local to the PowerCenter Integration Service process. Do not use a mapped or mounted drive for cache files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Cache.
$PMTargetFileDir	Directory for target files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/TgtFiles.
$PMSourceFileDir	Directory for source files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SrcFiles.

Property	Description
$PmExtProcDir	Directory for external procedures. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/ExtProc.
$PMTempDir	Directory for temporary files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Temp.
$PMLookupFileDir	Directory for lookup files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/LkpFiles.
$PMStorageDir	Directory for run-time files. Workflow recovery files save to the $PMStorageDir configured in the PowerCenter Integration Service properties. Session recovery files save to the $PMStorageDir configured in the operating system profile. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Storage.
Environment Variables	Name and value of environment variables used by the PowerCenter Integration Service at workflow run time. **Note:** If you configure the LD_LIBRARY_PATH environment variable, the value is appended to the LD_LIBRARY_PATH variable of the PowerCenter Integration Service process.

Creating an Operating System Profile

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Operating System Profiles Configuration.

   The Operating System Profiles Configuration dialog box appears.
3. Click Create Profile.
4. Enter the User Name, System User Name, and $PMRootDir.
5. Click OK.

   After you create the profile, you must configure properties.
6. Click the operating system profile you want to configure.
7. Select the Properties tab and click Edit.
8. Edit the properties and click OK.
9. Select the Permissions tab.

   A list of all the users with permission on the operating system profile appears.
10. Click Edit.
11. Edit the permission and click OK.

CHAPTER 8

Privileges and Roles

This chapter includes the following topics:

- Privileges and Roles Overview, 74
- Domain Privileges, 75
- Analyst Service Privilege, 81
- Data Integration Service Privilege, 81
- Metadata Manager Service Privileges, 82
- Model Repository Service Privilege, 86
- PowerCenter Repository Service Privileges, 87
- PowerExchange Application Service Privileges, 96
- Reporting Service Privileges, 96
- Managing Roles, 103
- Assigning Privileges and Roles to Users and Groups, 106
- Viewing Users with Privileges for a Service, 108
- Troubleshooting Privileges and Roles, 108

Privileges and Roles Overview

You manage user security with privileges and roles.

Privileges

Privileges determine the actions that users can perform in application clients. Informatica includes the following privileges:

- Domain privileges. Determine actions on the Informatica domain that users can perform using the Administrator tool and the infacmd and pmrep command line programs.
- Analyst Service privilege. Determines actions that users can perform using Informatica Analyst.
- Data Integration Service privilege. Determines actions on applications that users can perform using the Administrator tool and the infacmd command line program. This privilege also determines whether users can drill down and export profile results.
- Metadata Manager Service privileges. Determine actions that users can perform using Metadata Manager.

- Model Repository Service privilege. Determines actions on projects that users can perform using Informatica Analyst and Informatica Developer.
- PowerCenter Repository Service privileges. Determine PowerCenter repository actions that users can perform using the Repository Manager, Designer, Workflow Manager, Workflow Monitor, and the pmrep and pmcmd command line programs.
- PowerExchange application service privileges. Determine actions that users can perform on the PowerExchange Listener Service and PowerExchange Logger Service using the infacmd pwx commands.
- Reporting Service privileges. Determine reporting actions that users can perform using Data Analyzer.

You assign privileges to users and groups and to application services. You can assign different privileges to a user for each application service of the same service type.

You assign privileges to users and groups on the Security tab of the Administrator tool.

The Administrator tool organizes privileges into levels. A privilege is listed below the privilege that it includes. Some privileges include other privileges. When you assign a privilege to users and groups, the Administrator tool also assigns any included privileges.

Privilege Groups

The domain and application service privileges are organized into privilege groups. A privilege group is an organization of privileges that define common user actions. For example, the domain privileges include the following privilege groups:

- Tools. Includes privileges to log in to the Administrator tool.
- Security Administration. Includes privileges to manage users, groups, roles, and privileges.
- Domain Administration. Includes privileges to manage the domain, folders, nodes, grids, licenses, and application services.

Tip: When you assign privileges to users and user groups, you can select a privilege group to assign all privileges in the group.

Roles

A role is a collection of privileges that you assign to a user or group. Each user within an organization has a specific role, whether the user is a developer, administrator, basic user, or advanced user. For example, the PowerCenter Developer role includes all the PowerCenter Repository Service privileges or actions that a developer performs.

You assign a role to users and groups for the domain or for each Data Integration Service, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service in the domain.

Tip: When you assign roles to groups, you can then move users in and out of groups without having to reassign privileges, roles, and permissions.

Domain Privileges

Domain privileges determine the actions that users can perform using the Administrator tool and the *infacmd* and *pmrep* command line programs.

The following table describes each domain privilege:

Privilege Group	Privilege Name	Description
Security Administration	Grant Privileges and Roles	Assign privileges and roles to users and groups for the domain or application services. Includes the Manage Users, Groups, and Roles privilege.
	Manage Users, Groups, and Roles	Create, edit, and delete users, groups, and roles. Configure LDAP authentication. Import LDAP users and groups.
Domain Administratoin	Manage Service Execution	Enable and disable application services and service processes. Receive application service alerts. Includes the Manage Services privilege.
	Manage Services	Create, configure, move, remove, and grant permission on application services and license objects.
	Manage Nodes and Grids	Create, configure, move, remove, shut down, and grant permission on nodes and grids.
	Manage Domain Folders	Create, edit, move, remove, and grant permission on folders.
	Manage Connections	Create, edit, and remove connections.
Monitoring	Monitoring	Includes the following privileges: - Configure Global Settings - Configure Statistics and Reports
	Configure Global Settings	Configure the global settings.
	Configure Statistics and Reports	Configure preferences for monitoring statistics and reports.
	View	Includes the following privileges: - View Jobs of Other Users - View Statistics - View Reports
	View Jobs of Other Users	Displays jobs of other users. If you disable this option, you can only view your own jobs.
	View Statistics	View statistics for domain objects.
	View Reports	View reports for domain objects.
	Access Monitoring	Includes the following privileges: - Access from Analyst Tool - Access from Developer Tool - Access from Administrator Tool
	Access from Analyst Tool	Access the monitoring feature from the Analyst tool.
	Access from Developer Tool	Access the monitoring feature from the Developer tool.
	Access from Administrator Tool	Access the monitoring feature from the Administration tool.

Privilege Group	Privilege Name	Description
	Allow Actions for Jobs	Abort jobs, reissue mapping jobs, and view logs about a job.
Tools	Access Informatica Administrator	Log in to the Administrator tool.

Security Administration Privilege Group

Privileges in the Security Administration privilege group and domain object permissions determine the security management tasks users can complete.

Some security management tasks are determined by the Administrator role, not by privileges or permissions. A user assigned the Administrator role for the domain can complete the following tasks:

- Create operating system profiles.
- Grant permission on operating system profiles.
- Delete operating system profiles.

The following table lists the privileges and permissions required to administer domain security:

Privilege	Permission On...	Grants Users the Ability To...
Grant Privileges and Roles	Domain Metadata Manager Service Model Repository Service PowerCenter Repository Service Reporting Service	- Assign privileges and roles to users and groups for the domain or application service. - Edit and remove the privileges and roles assigned to users and groups.
Manage Users, Groups, and Roles (includes Grant Privileges and Roles privilege)	n/a	- Configure LDAP authentication for the domain. - Create, edit, and delete users, groups, and roles. - Import LDAP users and groups.
	Operating system profile	Edit operating system profile properties.

Note: To complete security management tasks in the Administrator tool, users must also have the Access Informatica Administrator privilege.

Domain Administration Privilege Group

Domain management tasks that users can perform depend on privileges in the Domain Administration group and permissions on domain objects.

Some domain management tasks are determined by the Administrator role, not by privileges or permissions. A user assigned the Administrator role for the domain can complete the following tasks:

- Configure domain properties.
- Grant permission on the domain.
- Manage and purge log events.
- Receive domain alerts.
- Run the License Report.
- View user activity log events.
- Shut down the domain.

The following table lists the privileges and permissions required to administer the domain:

Privilege	Permission On...	Grants Users the Ability To...
n/a	Domain	- View domain properties and log events. - Configure the global settings.
n/a	Folder	View folder properties.
n/a	Application service	View application service properties and log events.
n/a	License object	View license object properties.
n/a	Grid	View grid properties.
n/a	Node	View node properties.
n/a	Web Services Hub	Run a Web Services Report.
Manage Service Execution	Application service	- Enable and disable application services and service processes. To enable and disable a Metadata Manager Service, users must also have permission on the associated PowerCenter Integration Service and PowerCenter Repository Service. - Receive application service alerts.
Manage Services (includes Manage Service Execution privilege)	Domain or parent folder	Create license objects.
	Domain or parent folder, node or grid where application service runs, license object, and any associated application service	Create application services.
	Application service	- Configure application services. - Grant permission on application services.
	Original and destination folders	Move application services or license objects from one folder to another.
	Domain or parent folder and application service	Remove application services.
	Analyst Service	Create and delete audit trail tables.
	Metadata Manager Service	- Create and delete Metadata Manager repository content. - Upgrade the content of the Metadata Manager Service.
	Metadata Manager Service Repository Service	Restore the PowerCenter repository for Metadata Manager.

Privilege	Permission On...	Grants Users the Ability To...
	Model Repository Service	- Create and delete model repository content. - Create, delete, and re-index the search index. - Change the source analyzer.
	PowerCenter Integration Service	Run the PowerCenter Integration Service in safe mode.
Manage Services (includes Manage Service Execution privilege)	PowerCenter Repository Service	- Back up, restore, and upgrade the PowerCenter repository. - Configure data lineage for the PowerCenter repository. - Copy content from another PowerCenter repository. - Close user connections and release PowerCenter repository locks. - Create and delete PowerCenter repository content. - Create, edit, and delete reusable metadata extensions in the PowerCenter Repository Manager. - Enable version control for the PowerCenter repository. - Manage a PowerCenter repository domain. - Perform an advanced purge of object versions at the repository level in the PowerCenter Repository Manager. - Register and unregister PowerCenter repository plug-ins. - Run the PowerCenter repository in exclusive mode. - Send PowerCenter repository notifications to users. - Update PowerCenter repository statistics.
	Reporting Service	- Back up, restore, and upgrade the content of the Data Analyzer repository. - Create and delete the content of the Data Analyzer repository.
	License object	- Edit license objects. - Grant permission on license objects.
	License object and application service	Assign a license to an application service.
	Domain or parent folder and license object	Remove license objects.
Manage Nodes and Grids	Domain or parent folder	Create nodes.

Privilege	Permission On...	Grants Users the Ability To...
	Domain or parent folder and nodes assigned to the grid	Create grids.
	Node or grid	- Configure and shut down nodes and grids. - Grant permission on nodes and grids.
	Original and destination folders	Move nodes and grids from one folder to another.
	Domain or parent folder and node or grid	Remove nodes and grids.
Manage Domain Folders	Domain or parent folder	Create folders.
	Folder	- Edit folders. - Grant permission on folders.
	Original and destination folders	Move folders from one parent folder to another.
	Domain or parent folder and folder being removed	Remove folders.
Manage Connections	Connection	Edit and remove connections.

Note: To complete domain management tasks in the Administrator tool, users must also have the Access Informatica Administrator privilege.

Monitoring Privilege Group

The privileges in the Monitoring group determine which users can view and configure monitoring.

The following table lists the actions that users can perform for the privileges in the Monitoring group:

Privilege	Permission On...	Grants Users the Ability To...
Configure Global Settings	Domain	Configure the global settings.
Configure Statistics and Reports	Domain	Configure preferences for monitoring statistics and reports.
View Jobs of Other Users	n/a	Displays jobs of other users.
View Statistics	n/a	View statistics for domain objects.
View Reports	n/a	View reports for domain objects.
Access from Analyst Tool	n/a	Access the monitoring feature from the Analyst tool.
Access from Developer Tool	n/a	Access the monitoring feature from the Developer tool.

Privilege	Permission On...	Grants Users the Ability To...
Access from Administrator Tool	n/a	Access the monitoring feature from the Administration tool.
Allow Actions for Jobs	n/a	- Abort jobs. - Reissue mapping jobs. - View logs about a job.

To run *infacmd* commands or to access the read-only view of the Monitoring tab, users do not need the Access Informatica Administrator privilege.

Tools Privilege Group

The privileges in the domain Tools group determine which users can access the Administrator tool or the read-only view of the Monitoring tab.

The following table lists the actions that users can perform for the privileges in the Tools group:

Privilege	Permission On...	Grants Users the Ability To...
Access Informatica Administrator	At least one domain object	- Log in to the Administrator tool. - Manage their own user account in the Administrator tool. - Export log events.

To complete tasks in the Administrator tool, users must have the Access Informatica Administrator privilege.

To run *infacmd* commands or to access the read-only view of the Monitoring tab, users do not need the Access Informatica Administrator privilege.

Analyst Service Privilege

The Analyst Service privilege determines actions that licensed users can perform on projects using the Analyst tool.

The following table lists the privileges and permissions required to manage projects and objects in projects:

Privilege	Permission	Grants Users the Ability to
License access for Informatica Analyst	n/a	Run profiles and scorecards for licensed users in the Analyst tool.

Data Integration Service Privilege

The Data Integration Service privilege determines actions that users can perform on applications using the Administrator tool and the infacmd command line program. It also determines whether users can drill down and export profile results.

The following table describes each Data Integration Service privilege:

Privilege Group	Privilege Name	Description
Application Administration	Manage Applications	Grants users the ability to: - Backup and restore an application to a file. - Deploy an application to a Data Integration Service and resolve name conflicts. - Start an application after deployment. - Find an application. - Start or stop SQL data services. - Configure application properties.
Profiling Administration	Drilldown and Export Results	Grants users the ability to: - Drill down profling results - Export profiling results Access permission required on the project. For a relational data source, you need the Execute permission to query the source.

To complete these tasks in the Administrator tool, users must also have permission on the Data Integration Service.

Metadata Manager Service Privileges

Metadata Manager Service privileges determine the Metadata Manager actions that users can perform using Metadata Manager.

The following table describes each Metadata Manager Service privilege:

Privilege Group	Privilege Name	Description
Catalog	Share Shortcuts	Share a folder that contains a shortcut.
	View Lineage	Run lineage analysis on metadata objects in the catalog.
	View Related Catalogs	View related catalogs.
	View Reports	View Metadata Manager reports in Data Analyzer.
	View Profile Results	View profiling information for metadata objects in the catalog from a relational source.
	View Catalog	View and export metadata catalog objects.
	View Relationships	View relationships for metadata objects, categories, and business terms.
	Manage Relationships	Create, edit, and delete relationships for custom metadata objects, categories, and business terms.
	View Comments	View comments for metadata objects, categories, and business terms.

Privilege Group	Privilege Name	Description
	Post Comments	Add comments for metadata objects, categories, and business terms.
	Delete Comments	Delete comments for metadata objects, categories, and business terms.
	View Links	View links for metadata objects, categories, and business terms.
	Manage Links	Create, edit, and delete links for metadata objects, categories, and business terms.
	View Glossary	View business glossaries in the Business Glossary view. Export a business glossary.
	Draft/Propose Business Terms	Draft and propose business terms.
	Manage Glossary	Create, edit, and delete a business glossary, including categories and business terms. Import a business glossary.
	Manage Objects	Create, edit, and delete metadata objects in the catalog.
Load	View Resource	View resources and resource properties.
	Load Resource	Load metadata for a resource into the Metadata Manager warehouse.
	Manage Schedules	Create and edit schedules, and add schedules to resources.
	Purge Metadata	Remove metadata for a resource from the Metadata Manager warehouse.
	Manage Resource	Create, edit, and delete resources.
Model	View Model	Open models and classes, and view model and class properties. View relationships and attributes for classes.
	Manage Model	Create, edit, and delete custom models. Add attributes to packaged models.
	Export/Import Models	Import and export custom models and modified packaged models.
Security	Manage Catalog Permissions	Assign users and groups permissions on metadata objects and edit permissions on metadata objects in the catalog.

Catalog Privilege Group

The privileges in the Catalog privilege group determine the tasks that users can perform in the Browse page of the Metadata Manager interface. A user with the privilege to perform certain actions requires permissions to perform the action on a particular object. Configure permissions on the Security tab of the Metadata Manager application.

The following table lists the privileges in the Catalog privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Grants Users the Ability to
Share Shortcuts	n/a	Write	Share a folder that contains a shortcut with other users and groups.
View Lineage	n/a	Read	- Run data lineage analysis on metadata objects, categories, and business terms. - Run data lineage analysis from the PowerCenter Designer. Users must also have read permission on the PowerCenter repository folder.
View Related Catalogs	n/a	Read	View related catalogs.
View Reports	n/a	Read	View Metadata Manager reports in Data Analyzer.
View Profile Results	n/a	Read	View profiling information for metadata objects in the catalog from a relational source.
View Catalog	n/a	Read	- View resources and metadata objects in the metadata catalog. - Search the metadata catalog.
View Relationships	n/a	Read	View relationships for metadata objects, categories, and business terms.
Manage Relationships	View Relationships	Write	Create, edit, and delete relationships for custom metadata objects, categories, and business terms. Import related catalog objects and related terms for a business glossary.
View Comments	n/a	Read	View comments for metadata objects, categories, and business terms.
Post Comments	View Comments	Write	Add comments for metadata objects, categories, and business terms.
Delete Comments	- Post Comments - View Comments	Write	Delete comments for metadata objects, categories, and business terms.
View Links	n/a	Read	View links for metadata objects, categories, and business terms.
Manage Links	View Links	Write	Create, edit, and delete links for metadata objects, categories, and business terms.
View Glossary	n/a	Read	- View business glossaries in the Business Glossary view. - Search business glossaries.
Draft/Propose Business Terms	View Glossary	Write	Draft and propose business terms.

Privilege	Includes Privileges	Permission	Grants Users the Ability to
Manage Glossary	- Draft/Propose Business Terms - View Glossary	Write	Create, edit, and delete a business glossary, including categories and business terms. Import and export a business glossary.
Manage Objects	n/a	Write	- Edit metadata objects in the catalog. - Create, edit, and delete custom metadata objects. Users must also have the View Model privilege. - Create, edit, and delete custom metadata resources. Users must also have the Manage Resource privilege.

Load Privilege Group

The privileges in the Load privilege group determine the tasks users can perform in the Load page of the Metadata Manager interface. You cannot configure permissions on resources.

The following table lists the privileges required to manage an instance of a resource in the Metadata Manager warehouse:

Privilege	Includes Privileges	Permission	Grants Users the Ability to
View Resource	n/a	n/a	- View resources and resource properties in the Metadata Manager warehouse. - Download Metadata Manager agent installer.
Load Resource	View Resource	n/a	- Load metadata for a resource into the Metadata Manager warehouse. - Create links between objects in connected resources for data lineage. - Configure search indexing for resources.
Manage Schedules	View Resource	n/a	Create and edit schedules, and add schedules to resources.
Purge Metadata	View Resource	n/a	Remove metadata for a resource from the Metadata Manager warehouse.
Manage Resource	- Purge Metadata - View Resource	n/a	Create, edit, and delete resources.

Model Privilege Group

The privileges in the Model privilege group determine the tasks users can perform in the Model page of the Metadata Manager interface. You cannot configure permissions on a model.

The following table lists the privileges required to manage models:

Privilege	Includes Privileges	Permission	Grants Users the Ability to
View Model	n/a	n/a	Open models and classes, and view model and class properties. View relationships and attributes for classes.
Manage Model	View Model	n/a	Create, edit, and delete custom models. Add attributes to packaged models.
Export/Import Models	View Model	n/a	Import and export custom models and modified packaged models.

Security Privilege Group

The privilege in the Security privilege group determines the tasks users can perform on the Security tab of the Metadata Manager interface.

By default, the Manage Catalog Permissions privilege in the Security privilege group is assigned to the Administrator, or a user with the Administrator role on the Metadata Manager Service. You can assign the Manage Catalog Permissions privilege to other users.

The following table lists the privilege required to manage Metadata Manager security:

Privilege	Includes Privileges	Permission	Grants Users the Ability to
Manage Catalog Permissions	n/a	Full control	- Assign users and groups permissions on resources, metadata objects, categories, and business terms. - Edit permissions on resources, metadata objects, categories, and business terms.

Model Repository Service Privilege

The Model Repository Service privilege determines actions that users can perform on projects using Informatica Analyst and Informatica Developer.

The Model Repository Service privilege and model repository object permissions determine the tasks that users can complete on projects and objects in projects.

The following table lists the privileges and permissions required to manage projects and objects in projects:

Privilege	Permission	Grants Users the Ability To
n/a	Read on project	View projects and objects in projects.
n/a	Write on project	- Edit projects. - Create, edit, and delete objects in projects. - Delete projects.

Privilege	Permission	Grants Users the Ability To
n/a	Grant on project	Grant and revoke permissions on projects for users and groups.
Create Project	n/a	- Create projects. - Upgrade the Model Repository Service using the Actions menu.

PowerCenter Repository Service Privileges

PowerCenter Repository Service privileges determine PowerCenter repository actions that users can perform using the PowerCenter Repository Manager, Designer, Workflow Manager, Workflow Monitor, and the *pmrep* and *pmcmd* command line programs.

The following table describes each PowerCenter Repository Service privilege:

Privilege Group	Privilege Name	Description
Tools	Access Designer	Connect to the PowerCenter repository using the Designer.
	Access Repository Manager	Connect to the PowerCenter repository using the Repository Manager. Run *pmrep* commands.
	Access Workflow Manager	Connect to the PowerCenter repository using the Workflow Manager.
	Access Workflow Monitor	Connect to the PowerCenter repository and PowerCenter Integration Service using the Workflow Monitor.
Folders	Create	Create PowerCenter repository folders.
	Copy	Copy folders within a PowerCenter repository or to another PowerCenter repository.
	Manage Versions	In a versioned PowerCenter repository, change the status of folders and perform an advanced purge of object versions at the folder level.
Design Objects	Create, Edit, and Delete	Create, edit, and delete business components, mapping parameters and variables, mappings, mapplets, transformations, and user-defined functions.
	Manage Versions	In a versioned PowerCenter repository, change the status, recover, and purge design object versions. Check in and undo checkouts made by other users. Includes the Create, Edit, and Delete privilege.
Sources and Targets	Create, Edit, and Delete	Create, edit, and delete cubes, dimensions, source definitions, and target definitions.
	Manage Versions	In a versioned PowerCenter repository, change the status, recover, and purge versions of source and target objects. Check in and undo checkouts made by other users. Includes the Create, Edit, and Delete privilege.

Privilege Group	Privilege Name	Description
Run-time Objects	Create, Edit, and Delete	Create, edit, and delete session configuration objects, tasks, workflows, and worklets.
	Manage Versions	In a versioned PowerCenter repository, change the status, recover, and purge run-time object versions. Check in and undo checkouts made by other users. Includes the Create, Edit, and Delete privilege.
	Monitor	Monitor workflows and tasks in the Workflow Monitor.
	Execute	Start, cold start, and recover tasks and workflows. Includes the Monitor privilege.
	Manage Execution	Schedule and unschedule workflows. Stop, abort, and recover tasks and workflows started by other users. Includes the Execute and Monitor privileges.
Global Objects	Create Connections	Create connection objects.
	Manage Deployment Groups	In a versioned PowerCenter repository, create, edit, copy, and roll back deployment groups. In a non-versioned repository, create, edit, and copy deployment groups.
	Execute Deployment Groups	Copy a deployment group without write permission on target folders. Requires read permission on source folders and execute permission on the deployment group.
	Create Labels	In a versioned PowerCenter repository, create labels.
	Create Queries	Create object queries.

Users must have the Manage Services domain privilege and permission on the PowerCenter Repository Service to perform the following actions in the Repository Manager:

- Perform an advanced purge of object versions at the PowerCenter repository level.
- Create, edit, and delete reusable metadata extensions.

Tools Privilege Group

The privileges in the PowerCenter Repository Service Tools privilege group determine the PowerCenter Client tools and command line programs that users can access.

The following table lists the actions that users can perform for the privileges in the Tools group:

Privilege	Permission	Grants Users the Ability To
Access Designer	n/a	Connect to the PowerCenter repository using the Designer.
Access Repository Manager	n/a	- Connect to the PowerCenter repository using the Repository Manager. - Run *pmrep* commands.
Access Workflow Manager	n/a	- Connect to the PowerCenter repository using the Workflow Manager. - Remove a PowerCenter Integration Service from the Workflow Manager.

Privilege	Permission	Grants Users the Ability To
Access Workflow Monitor	n/a	- Connect to the PowerCenter repository using the Workflow Monitor. - Connect to the PowerCenter Integration Service in the Workflow Monitor.
Note: When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter Repository Service.		

The appropriate privilege in the Tools privilege group is required for all users completing tasks in PowerCenter Client tools and command line programs. For example, to create folders in the Repository Manager, a user must have the Create Folders and Access Repository Manager privileges.

If users have a privilege in the Tools privilege group and permission on a PowerCenter repository object but not the privilege to modify the object type, they can still perform some actions on the object. For example, a user has the Access Repository Manager privilege and read permission on some folders. The user does not have any of the privileges in the Folders privilege group. The user can view objects in the folders and compare the folders.

Folders Privilege Group

Folder management tasks are determined by privileges in the Folders privilege group, PowerCenter repository object permissions, and domain object permissions. Users complete folder management tasks in the Repository Manager and with the *pmrep* command line program.

Some folder management tasks are determined by folder ownership and the Administrator role, not by privileges or permissions. The folder owner or a user assigned the Administrator role for the PowerCenter Repository Service can complete the following folder management tasks:

- Assign operating system profiles to folders if the PowerCenter Integration Service uses operating system profiles. Requires permission on the operating system profile.
- Change the folder owner.
- Configure folder permissions.
- Delete the folder.
- Designate the folder to be shared.
- Edit the folder name and description.

The following table lists the privileges and permissions required to manage folders:

Privilege	Permission	Grants Users the Ability To
n/a	Read on folder	- Compare folders. - View objects in folders.
Create	n/a	Create folders.
Copy	Read on folder	Copy folders within the same PowerCenter repository or to another PowerCenter repository. Users must also have the Create Folders privilege in the destination repository.
Manage Versions	Read and Write on folder	- Change the status of folders. - Perform an advanced purge of object versions at the folder level.

Note: To perform actions on folders, users must also have the Access Repository Manager privilege.

Design Objects Privilege Group

Privileges in the Design Objects privilege group and PowerCenter repository object permissions determine tasks users can complete on the following design objects:

- Business components
- Mapping parameters and variables
- Mappings
- Mapplets
- Transformations
- User-defined functions

The following table lists the privileges and permissions required to manage design objects:

Privilege	Permission	Grants Users the Ability To
n/a	Read on folder	- Compare design objects. - Copy design objects as an image. - Export design objects. - Generate code for Custom transformation and external procedures. - Receive PowerCenter repository notification messages. - Run data lineage on design objects. Users must also have the View Lineage privilege for the Metadata Manager Service and read permission on the metadata objects in the Metadata Manager catalog. - Search for design objects. - View design objects, design object dependencies, and design object history.
n/a	Read on shared folder Read and Write on destination folder	Create shortcuts.
Create, Edit, and Delete	Read on original folder Read and Write on destination folder	- Copy design objects from one folder to another. - Copy design objects to another PowerCenter repository. Users must also have the Create, Edit, and Delete Design Objects privilege in the destination repository.
	Read and Write on folder	- Change comments for a versioned design object. - Check in and undo a checkout of design objects checked out by their own user account. - Check out design objects. - Copy and paste design objects in the same folder. - Create, edit, and delete data profiles and launch the Profile Manager. Users must also have the Create, Edit, and Delete Run-time Objects privilege. - Create, edit, and delete design objects. - Generate and clean SAP ABAP programs. - Generate business content integration mappings. Users must also have the Create, Edit, and Delete Sources and Targets privilege. - Import design objects using the Designer. Users must also have the Create, Edit, and Delete Sources and Targets privilege. - Import design objects using the Repository Manager. Users must also have the Create, Edit, and Delete Run-

Privilege	Permission	Grants Users the Ability To
		time Objects and Create, Edit, and Delete Sources and Targets privileges. - Revert to a previous design object version. - Validate mappings, mapplets, and user-defined functions.
Manage Versions (includes Create, Edit, and Delete privilege)	Read and Write on folder	- Change the status of design objects. - Check in and undo checkouts of design objects checked out by other users. - Purge versions of design objects. - Recover deleted design objects.

Note: To perform actions on design objects, users must also have the appropriate privilege in the Tools privilege group.

Sources and Targets Privilege Group

Privileges in the Sources and Targets privilege group and PowerCenter repository object permissions determine tasks users can complete on the following source and target objects:

- Cubes
- Dimensions
- Source definitions
- Target definitions

The following table lists the privileges and permissions required to manage source and target objects:

Privilege	Permission	Grants Users the Ability To
n/a	Read on folder	- Compare source and target objects. - Export source and target objects. - Preview source and target data. - Receive PowerCenter repository notification messages. - Run data lineage on source and target objects. Users must also have the View Lineage privilege for the Metadata Manager Service and read permission on the metadata objects in the Metadata Manager catalog. - Search for source and target objects. - View source and target objects, source and target object dependencies, and source and target object history.
n/a	Read on shared folder Read and Write on destination folder	Create shortcuts.
Create, Edit, and Delete	Read on original folder Read and Write on destination folder	- Copy source and target objects to another folder. - Copy source and target objects to another PowerCenter repository. Users must also have the Create, Edit, and Delete Sources and Targets privilege in the destination repository.

Privilege	Permission	Grants Users the Ability To
	Read and Write on folder	- Change comments for a versioned source or target object. - Check in and undo a checkout of source and target objects checked out by their own user account. - Check out source and target objects. - Copy and paste source and target objects in the same folder. - Create, edit, and delete source and target objects. - Import SAP functions. - Import source and target objects using the Designer. Users must also have the Create, Edit, and Delete Design Objects privilege. - Import source and target objects using the Repository Manager. Users must also have the Create, Edit, and Delete Design Objects and Create, Edit, and Delete Run-time Objects privileges. - Generate and execute SQL to create targets in a relational database. - Revert to a previous source or target object version.
Manage Versions (includes Create, Edit, and Delete privilege)	Read and Write on folder	- Change the status of source and target objects. - Check in and undo checkouts of source and target objects checked out by other users. - Purge versions of source and target objects. - Recover deleted source and target objects.

Note: To perform actions on source and target objects, users must also have the appropriate privilege in the Tools privilege group.

Run-time Objects Privilege Group

Privileges in the Run-time Objects privilege group, PowerCenter repository object permissions, and domain object permissions determine tasks users can complete on the following run-time objects:

- Session configuration objects
- Tasks
- Workflows
- Worklets

Some run-time object tasks are determined by the Administrator role, not by privileges or permissions. A user assigned the Administrator role for the PowerCenter Repository Service can delete a PowerCenter Integration Service from the Navigator of the Workflow Manager.

The following table lists the privileges and permissions required to manage run-time objects:

Privilege	Permission	Grants Users the Ability To
n/a	Read on folder	- Compare run-time objects. - Export run-time objects. - Receive PowerCenter repository notification messages. - Search for run-time objects. - Use mapping parameters and variables in a session. - View run-time objects, run-time object dependencies, and run-time object history.
Create, Edit, and Delete	Read on original folder Read and Write on destination folder	- Copy tasks, workflows, or worklets from one folder to another. - Copy tasks, workflows, or worklets to another PowerCenter repository. Users must also have the Create, Edit, and Delete Run-time Objects privilege in the destination repository.
	Read and Write on folder	- Assign a PowerCenter Integration Service to a workflow in the workflow properties. - Assign a service level to a workflow. - Change comments for a versioned run-time object. - Check in and undo a checkout of run-time objects checked out by their own user account. - Check out run-time objects. - Copy and paste tasks, workflows, and worklets in the same folder. - Create, edit, and delete data profiles and launch the Profile Manager. Users must also have the Create, Edit, and Delete Design Objects privilege. - Create, edit, and delete session configuration objects. - Delete and validate tasks, workflows, and worklets. - Import run-time objects using the Repository Manager. Users must also have the Create, Edit, and Delete Design Objects and Create, Edit, and Delete Sources and Targets privileges. - Import run-time objects using the Workflow Manager. - Revert to a previous object version.
	Read and Write on folder Read on connection object	- Create and edit tasks, workflows, and worklets. - Replace a relational database connection for all sessions that use the connection.
Manage Versions (includes Create, Edit, and Delete privilege)	Read and Write on folder	- Change the status of run-time objects. - Check in and undo checkouts of run-time objects checked out by other users. - Purge versions of run-time objects. - Recover deleted run-time objects.
Monitor	Read on folder	- View properties of run-time objects in the Workflow Monitor.* - View session and workflow logs in the Workflow Monitor.* - View run-time object and performance details in the Workflow Monitor.*
n/a	Read and Execute on folder	Stop and abort tasks and workflows started by their own user account.*

Privilege	Permission	Grants Users the Ability To
Execute (includes Monitor privilege)	Read and Execute on folder	Assign a PowerCenter Integration Service to a workflow using the Service menu or the Navigator.
	Read, Write, and Execute on folder Read and Execute on connection object	Debug a mapping by creating a debug session instance or by using an existing reusable session. Users must also have the Create, Edit, and Delete Run-time Objects privilege.*
	Read and Execute on folder Read and Execute on connection object	Debug a mapping by using an existing non-reusable session.*
	Read and Execute on folder Read and Execute on connection object Permission on operating system profile	- Start, cold start, and restart tasks and workflows.* - Recover tasks and workflows started by their own user account.*
Manage Execution (includes Execute and Monitor privileges)	Read and Execute on folder	- Stop and abort tasks and workflows started by other users.* - Stop and abort tasks that were recovered automatically.* - Truncate workflow and session log entries. - Unschedule workflows.*
	Read and Execute on folder Read and Execute on connection object Permission on operating system profile	- Recover tasks and workflows started by other users.* - Recover tasks that were recovered automatically.*
	Read, Write, and Execute on folder Read and Execute on connection object Permission on operating system profile	- Create and edit a reusable scheduler from the Workflows > Schedulers menu.* - Edit a non-reusable scheduler from the workflow properties.* - Edit a reusable scheduler from the workflow properties. Users must also have the Create, Edit, and Delete Run-time Objects privilege.*
*When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter Repository Service.		

Note: To perform actions on run-time objects, users must also have the appropriate privilege in the Tools privilege group.

Global Objects Privilege Group

Privileges in the Global Objects privilege group and PowerCenter repository object permissions determine the tasks users can complete on the following global objects:

- Connection objects
- Deployment groups
- Labels
- Queries

Some global object tasks are determined by global object ownership and the Administrator role, not by privileges or permissions. The global object owner or a user assigned the Administrator role for the PowerCenter Repository Service can complete the following global object tasks:

- Configure global object permissions.
- Change the global object owner.
- Delete the global object.

The following table lists the privileges and permissions required to manage global objects:

Privilege	Permission	Grants Users the Ability To
n/a	Read on connection object	View connection objects.
n/a	Read on deployment group	View deployment groups.
n/a	Read on label	View labels.
n/a	Read on query	View object queries.
n/a	Read and Write on connection object	Edit connection objects.
n/a	Read and Write on label	Edit and lock labels.
n/a	Read and Write on query	Edit and validate object queries.
n/a	Read and Execute on query	Run object queries.
n/a	Read on folder Read and Execute on label	Apply labels and remove label references.
Create Connections	n/a	Create and copy connection objects.
Manage Deployment Groups	n/a	Create deployment groups.
	Read and Write on deployment group	- Edit deployment groups. - Remove objects from a deployment group.
	Read on original folder Read and Write on deployment group	Add objects to a deployment group.
	Read on original folder Read and Write on destination folder Read and Execute on deployment group	Copy deployment groups.
	Read and Write on destination folder	Roll back deployment groups.
Execute Deployment Groups	Read on original folder Execute on deployment group	Copy deployment groups.
Create Labels	n/a	Create labels.
Create Queries	n/a	Create object queries.

Note: To perform actions on global objects, users must also have the appropriate privilege in the Tools privilege group.

PowerExchange Application Service Privileges

The PowerExchange Listener Service and PowerExchange Logger Service privileges determine the infacmd pwx commands that users can run.

The following table describes each PowerExchange Listener Service privilege:

Privilege Group	Privilege Name	Description
Informational Commands	listtask	Run the infacmd pwx ListTaskListener command.
Management Commands	close	Run the infacmd pwx CloseListener command.
	closeforce	Run the infacmd pwx CloseForceListener command.
	stoptask	Run the infacmd pwx StopTaskListener command.

The following table describes each PowerExchange Logger Service privilege:

Privilege Group	Privilege Name	Description
Informational Commands	displayall	Run the infacmd pwx DisplayAllLogger command.
	displaycpu	Run the infacmd pwx DisplayCPULogger command.
	displaycheckpoints	Run the infacmd pwx DisplayCheckpointsLogger command.
	displayevents	Run the infacmd pwx DisplayEventsLogger command.
	displaymemory	Run the infacmd pwx DisplayMemoryLogger command.
	displayrecords	Run the infacmd pwx DisplayRecordsLogger command.
	displaystatus	Run the infacmd pwx DisplayStatusLogger command.
Management Commands	condense	Run the infacmd pwx CondenseLogger command.
	fileswitch	Run the infacmd pwx FileSwitchLogger command.
	shutdown	Run the infacmd pwx ShutDownLogger command.

Reporting Service Privileges

Reporting Service privileges determine the actions that users can perform using Data Analyzer.

The following table describes each Reporting Service privilege:

Privilege Group	Privilege Name	Description
Administration	Maintain Schema	Create, edit, and delete schema tables.
	Export/Import XML Files	Export and import metadata as XML files.
	Manage User Access	Manage user and group properties in Data Analyzer. Set data restrictions for users and groups.
	Set Up Schedules and Tasks	Create and manage schedules and tasks.
	Manage System Properties	Manage system settings and properties.
	Set Up Query Limits	Access query governing settings.
	Configure Real-Time Message Streams	Add, edit, and remove real-time message streams.
Alerts	Receive Alerts	Receive and view triggered alerts.
	Create Real-time Alerts	Create an alert for a real-time report.
	Set Up Delivery Option	Configure alert delivery options.
Communication	Print	Print reports and dashboards.
	Email Object Links	Send links to reports or dashboards in an email.
	Email Object Contents	Send the contents of a report or dashboard in an email.
	Export	Export reports and dashboards.
	Export to Excel or CSV	Export reports to Excel or comma-separated values files.
	Export to Pivot Table	Export reports to Excel pivot tables.
	View Discussions	Read discussions.
	Add Discussions	Add messages to discussions.
	Manage Discussions	Delete messages from discussions.
	Give Feedback	Create feedback messages.
Content Directory	Access Content Directory	Access folders and content on the Find tab.
	Access Advanced Search	Search for advanced items.
	Manage Content Directory	Manage folders in the content directory.
	Manage Shared Documents	Manage shared documents.
Dashboards	View Dashboards	View contents of personal and public dashboards.
	Manage Personal Dashboard	Manage your own personal dashboard.

Privilege Group	Privilege Name	Description
	Create, Edit, and Delete Dashboards	Create, edit, and delete dashboards.
	Access Basic Dashboard Creation	Use basic dashboard configuration options. Broadcast dashboards as links.
	Access Advanced Dashboard Creation	Use all dashboard configuration options.
Indicators	Interact with Indicators	Use and interact with indicators.
	Create Real-time Indicator	Create an indicator on a real-time report.
	Get Continuous, Automatic Real-time Indicator Updates	View continuous, automatic, and animated real-time updates to indicators.
Manage Account	Manage Personal Settings	Configure personal account preferences.
Reports	View Reports	View reports and related metadata.
	Analyze Report	Analyze reports.
	Interact with Data	Access the toolbar on the Analyze tab and perform data-level tasks on the report table and charts.
	Drill Anywhere	Choose any attribute to drill into reports.
	Create Filtersets	Create and save filtersets in reports.
	Promote Custom Metric	Promote custom metrics from reports to schemas.
	View Query	View report queries.
	View Life Cycle Metadata	Edit time keys on the Time tab.
	Create and Delete Reports	Create and delete reports.
	Access Basic Report Creation	Create reports using basic report options.
	Access Advanced Report Creation	Create reports using all available report options.
	Save Copy of Reports	Use the Save As function to save the report with another name.
	Edit Reports	Edit reports.

Administration Privilege Group

Privileges in the Administration privilege group determine the tasks that users can perform in the Administration tab of Data Analyzer.

The following table lists the privileges and permissions in the Administration privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
Maintain Schema	n/a	Read, Write, and Delete on: - Metric folder - Attribute folder - Template dimension folder - Metric - Attribute - Template dimension	Create, edit, and delete schema tables.
Export/Import XML Files	n/a	n/a	Export or import metadata as XML files.
Manage User Access	n/a	n/a	Manage users, groups, and roles.
Set Up Schedules and Tasks	n/a	Read, Write, and Delete on time-based and event-based schedules	Create and manage schedules and tasks.
Manage System Properties		n/a	Manage system settings and properties.
Set Up Query Limits	- Manage System Properties	n/a	Access query governing settings.
Configure Real-Time Message Streams	n/a	n/a	Add, edit, and remove real-time message streams.

Alerts Privilege Group

Privileges in the Alerts privilege group determine the tasks users can perform in the Alerts tab of Data Analyzer.

The following table lists the privileges and permissions in the Alerts privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
Receive Alerts	n/a	n/a	Receive and view triggered alerts.
Create Real-time Alerts	- Receive Alerts	n/a	Create an alert for a real-time report.
Set Up Delivery Options	- Receive Alerts	n/a	Configure alert delivery options.

Communication Privilege Group

Privileges in the Communication privilege group determine the tasks users can perform to share dashboard or report information with other users.

The following table lists the privileges and permissions in the Communication privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
Print	n/a	Read on report Read on dashboard	Print reports and dashboards.
Email Object Links	n/a	Read on report Read on dashboard	Send links to reports or dashboards in an email.
Email Object Contents	- Email Object Links	Read on report Read on dashboard	Send the contents of a report or dashboard in an email.
Export	n/a	Read on report Read on dashboard	Export reports and dashboards.
Export to Excel or CSV	- Export	Read on report Read on dashboard	Export reports to Excel or comma-separated values files.
Export to Pivot Table	- Export - Export to Excel or CSV	Read on report Read on dashboard	Export reports to Excel pivot tables.
View Discussions	n/a	Read on report Read on dashboard	Read discussions.
Add Discussions	- View Discussions	Read on report Read on dashboard	Add messages to discussions.
Manage Discussions	- View Discussions	Read on report Read on dashboard	Delete messages from discussions. Delete Comment.
Give Feedback	n/a	Read on report Read on dashboard	Create feedback messages.

Content Directory Privilege Group

Privileges in the Content Directory privilege group determine the tasks users can perform in the Find tab of Data Analyzer.

The following table lists the privileges and permissions in the Content Directory privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
Access Content Directory	n/a	Read on folders	- Access folders and content on the Find tab. - Access personal folders. - Search for items available to users with the Basic Consumer role. - Search for reports by name or search for reports you use frequently. - View reports from the PowerCenter Designer or Workflow Manager.
Access Advanced Search	- Access Content Directory	Read on folders	- Search for advanced items. - Search for reports you create or reports used by a specific user.

Privilege	Includes Privileges	Permission	Grants Users the Ability To
Manage Content Directory	- Access Content Directory	Read and Write on folders	- Create folders. - Copy folder. - Cut and paste folders. - Rename folders.
		Delete on folders	Delete folders.
Manage Shared Documents	- Access Content Directory - Manage Content Directory	Read on folders Write on folders	Manage shared documents in the folders.

Dashboards Privilege Group

Privileges in the Dashboards privilege group determine the tasks users can perform on dashboards in Data Analyzer.

The following table lists the privileges and permissions in the Dashboards privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
View Dashboards	n/a	Read on dashboards	View contents of personal dashboards and public dashboards.
Manage Personal Dashboard	- View Dashboards	Read and Write on dashboards	Manage your own personal dashboard.
Create, Edit, and Delete Dashboards	- View Dashboards	Read and Write on dashboards	- Create dashboards. - Edit dashboards.
		Delete on dashboards	Delete dashboards.
Access Basic Dashboard Creation	- View Dashboards - Create, Edit, and Delete Dashboards	Read and Write on dashboards	- Use basic dashboard configuration options. - Broadcast dashboards as links.
Access Advanced Dashboard Creation	- View Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation	Read and Write on dashboards	Use all dashboard configuration options.

Indicators Privilege Group

Privileges in the Indicators privilege group determine the tasks users can perform with indicators.

The following table lists the privileges and permissions in the Indicators privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
Interact with Indicators	n/a	Read on report	Use and interact with indicators.

Privilege	Includes Privileges	Permission	Grants Users the Ability To
		Write on dashboard	
Create Real-time Indicator	n/a	Read and Write on report Write on dashboard	- Create an indicator on a real-time report. - Create gauge indicator.
Get Continuous, Automatic Real-time Indicator Updates	n/a	Read on report	View continuous, automatic, and animated real-time updates to indicators.

Manage Account Privilege Group

The privilege in the Manage Account privilege group determines the task users can perform in the Manage Account tab of Data Analyzer.

The following table lists the privilege and permission in the Manage Account privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
Manage Personal Settings	n/a	n/a	Configure personal account preferences.

Reports Privilege Group

Privileges in the Reports privilege group determine the tasks users can perform with reports in Data Analyzer.

The following table lists the privileges and permissions in the Reports privilege group:

Privilege	Includes Privileges	Permission	Grants Users the Ability To
View Reports	n/a	Read on report	View reports and related metadata.
Analyze Reports	- View Reports	Read on report	- Analyze reports. - View report data, metadata, and charts.
Interact with Data	- View Reports - Analyze Reports	Read and Write on report	- Access the toolbar on the Analyze tab and perform data-level tasks on the report table and charts. - Right-click on items on the Analyze tab.
Drill Anywhere	- View Reports - Analyze Reports - Interact with Data	Read on report	Choose any attribute to drill into reports.
Create Filtersets	- View Reports - Analyze Reports - Interact with Data	Read and Write on report	Create and save filtersets in reports.
Promote Custom Metric	- View Reports - Analyze Reports - Interact with Data	Write on report	Promote custom metrics from reports to schemas.

Privilege	Includes Privileges	Permission	Grants Users the Ability To
View Query	- View Reports - Analyze Reports - Interact with Data	Read on report	View report queries.
View Life Cycle Metadata	- View Reports - Analyze Reports - Interact with Data	Write on report	Edit time keys on the Time tab.
Create and Delete Reports	- View Reports	Write and Delete on report	Create or delete reports.
Access Basic Report Creation	- View Reports - Create and Delete Reports	Write on report	- Create reports using basic report options. - Broadcast the link to a report in Data Analyzer and edit the SQL query for the report.
Access Advanced Report Creation	- View Reports - Create and Delete Reports - Access Basic Report Creation	Write on report	- Create reports using all available report options. - Broadcast report content as an email attachment and link. - Archive reports. - Create and manage Excel templates. - Set provider-based security for a report.
Save Copy of Reports	- View Reports	Write on report	Use the Save As function to save the with another name.
Edit Reports	- View Reports	Write on report	Edit reports.

Managing Roles

A role is a collection of privileges that you can assign to users and groups. You can assign the following types of roles:

- System-defined. Roles that you cannot edit or delete.
- Custom. Roles that you can create, edit, and delete.

A role includes privileges for the domain or an application service type. You assign roles to users or groups for the domain or for each application service in the domain. For example, you can create a Developer role that includes privileges for the PowerCenter Repository Service. A domain can contain multiple PowerCenter Repository Services. You can assign the Developer role to a user for the Development PowerCenter Repository Service. You can assign a different role to that user for the Production PowerCenter Repository Service.

When you select a role in the Roles section of the Navigator, you can view all users and groups that have been directly assigned the role for the domain and application services. You can view the role assignments by users and groups or by services. To navigate to a user or group listed in the Assignments section, right-click the user or group and select Navigate to Item.

You can search for system-defined and custom roles.

System-Defined Roles

A system-defined role is a role that you cannot edit or delete. The Administrator role is a system-defined role.

When you assign the Administrator role to a user or group for the domain, Analyst Service, Data Integration Service, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service, the user or group is granted all privileges for the service. The Administrator role bypasses permission checking. Users with the Administrator role can access all objects managed by the service.

Administrator Role

When you assign the Administrator role to a user or group for the domain, Data Integration Service, or PowerCenter Repository Service, the user or group can complete some tasks that are determined by the Administrator role, not by privileges or permissions.

You can assign a user or group all privileges for the domain, Data Integration Service, or PowerCenter Repository Service and then grant the user or group full permissions on all domain or PowerCenter repository objects. However, this user or group cannot complete the tasks determined by the Administrator role.

For example, a user assigned the Administrator role for the domain can configure domain properties in the Administrator tool. A user assigned all domain privileges and permission on the domain cannot configure domain properties.

The following table lists the tasks determined by the Administrator role for the domain, Data Integration Service, and PowerCenter Repository Service:

Service	Tasks
Domain	- Configure domain properties. - Create operating system profiles. - Delete operating system profiles. - Grant permission on the domain and operating system profiles. - Manage and purge log events. - Receive domain alerts. - Run the License Report. - View user activity log events. - Shut down the domain. - Upgrade services using the service upgrade wizard.
Data Integration Service	- Upgrade the Data Integration Service using the Actions menu.
PowerCenter Repository Service	- Assign operating system profiles to repository folders if the PowerCenter Integration Service uses operating system profiles.* - Change the owner of folders and global objects.* - Configure folder and global object permissions.* - Connect to the PowerCenter Integration Service from the PowerCenter Client when running the PowerCenter Integration Service in safe mode. - Delete a PowerCenter Integration Service from the Navigator of the Workflow Manager. - Delete folders and global objects.* - Designate folders to be shared.* - Edit the name and description of folders.* *The PowerCenter repository folder owner or global object owner can also complete these tasks.

Custom Roles

A custom role is a role that you can create, edit, and delete. The Administrator tool includes custom roles for the Metadata Manager Service, PowerCenter Repository Service, and Reporting Service. You can edit the privileges belonging to these roles and can assign these roles to users and groups.

Or you can create custom roles and assign these roles to users and groups.

Managing Custom Roles

You can create, edit, and delete custom roles.

Creating Custom Roles

When you create a custom role, you assign privileges to the role for the domain or for an application service type. A role can include privileges for one or more services.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Create Role.

   The Create Role dialog box appears.
3. Enter the following properties for the role:

Property	Description
Name	Name of the role. The role name is case insensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Description	Description of the role. The description cannot exceed 765 characters or include a tab, newline character, or the following special characters: < > "

4. Click the Privileges tab.
5. Expand the domain or an application service type.
6. Select the privileges to assign to the role for the domain or application service type.
7. Click OK.

Editing Properties for Custom Roles

When you edit a custom role, you can change the description of the role. You cannot change the name of the role.

1. In the Administrator tool, click the Security tab.
2. In the Roles section of the Navigator, select a role.
3. Click Edit.
4. Change the description of the role and click OK.

Editing Privileges Assigned to Custom Roles

You can change the privileges assigned to a custom role for the domain and for each application service type.

1. In the Administrator tool, click the Security tab.
2. In the Roles section of the Navigator, select a role.

3. Click the Privileges tab.
4. Click Edit.

   The Edit Roles and Privileges dialog box appears.
5. Expand the domain or an application service type.
6. To assign privileges to the role, select the privileges for the domain or application service type.
7. To remove privileges from the role, clear the privileges for the domain or application service type.
8. Repeat the steps to change the privileges for each service type.
9. Click OK.

Deleting Custom Roles

When you delete a custom role, the custom role and all privileges that it included are removed from any user or group assigned the role.

To delete a custom role, right-click the role in the Roles section of the Navigator and select Delete Role. Confirm that you want to delete the role.

Assigning Privileges and Roles to Users and Groups

You determine the actions that users can perform by assigning the following items to users and groups:

- Privileges. A privilege determines the actions that users can perform in application clients.
- Roles. A role is a collection of privileges. When you assign a role to a user or group, you assign the collection of privileges belonging to the role.

Use the following rules and guidelines when you assign privileges and roles to users and groups:

- You assign privileges and roles to users and groups for the domain and for each application service that is running in the domain.

  You cannot assign privileges and roles to users and groups for a Metadata Manager Service, PowerCenter Repository Service, or Reporting Service in the following situations:

  - The application service is disabled.

  - The PowerCenter Repository Service is running in exclusive mode.
- You can assign different privileges and roles to a user or group for each application service of the same service type.
- A role can include privileges for the domain and multiple application service types. When you assign the role to a user or group for one application service, privileges for that application service type are assigned to the user or group.

If you change the privileges or roles assigned to a user, the changed privileges or roles take affect the next time the user logs in.

Note: You cannot edit the privileges or roles assigned to the default Administrator user account.

Inherited Privileges

A user or group can inherit privileges from the following objects:

- Group. When you assign privileges to a group, all subgroups and users belonging to the group inherit the privileges.
- Role. When you assign a role to a user, the user inherits the privileges belonging to the role. When you assign a role to a group, the group and all subgroups and users belonging to the group inherit the privileges belonging to the role. The subgroups and users do not inherit the role.

You cannot revoke privileges inherited from a group or role. You can assign additional privileges to a user or group that are not inherited from a group or role.

The Privileges tab for a user or group displays all the roles and privileges assigned to the user or group for the domain and for each application service. Expand the domain or application service to view the roles and privileges assigned for the domain or service. Click the following items to display additional information about the assigned roles and privileges:

- Name of an assigned role. Displays the role details on the details panel.
- Information icon for an assigned role. Highlights all privileges inherited with that role.

Privileges that are inherited from a role or group display an inheritance icon. The tooltip for an inherited privilege displays which role or group the user inherited the privilege from.

Steps to Assign Privileges and Roles to Users and Groups

You can assign privileges and roles to users and groups in the following ways:

- Navigate to a user or group and edit the privilege and role assignments.
- Drag roles to a user or group.

Assigning Privileges and Roles to a User or Group by Navigation

1. In the Administrator tool, click the Security tab.
2. In the Navigator, select a user or group.
3. Click the Privileges tab.
4. Click Edit.

   The Edit Roles and Privileges dialog box appears.
5. To assign roles, expand the domain or an application service on the Roles tab.
6. To grant roles, select the roles to assign to the user or group for the domain or application service.

   You can select any role that includes privileges for the selected domain or application service type.
7. To revoke roles, clear the roles assigned to the user or group.
8. Repeat steps 5 through 7 to assign roles for another service.
9. To assign privileges, click the Privileges tab.
10. Expand the domain or an application service.
11. To grant privileges, select the privileges to assign to the user or group for the domain or application service.
12. To revoke privileges, clear the privileges assigned to the user or group.

    You cannot revoke privileges inherited from a role or group.
13. Repeat steps 10 through 12 to assign privileges for another service.
14. Click OK.

Assigning Roles to a User or Group by Dragging

1. In the Administrator tool, click the Security tab.
2. In the Roles section of the Navigator, select the folder containing the roles you want to assign.
3. In the details panel, select the role you want to assign.

   You can use the Ctrl or Shift keys to select multiple roles.
4. Drag the selected roles to a user or group in the Users or Groups sections of the Navigator.

   The Assign Roles dialog box appears.
5. Select the domain or application services to which you want to assign the role.
6. Click OK.

Viewing Users with Privileges for a Service

You can view all users that have privileges for the domain or an application service. For example, you might want to view all users that have privileges on the Development PowerCenter Repository Service.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Service User Privileges.

   The Services dialog box appears.
3. Select the domain or an application service.

   The details panel displays all users that have privileges for the domain or application service.
4. Right-click a user name and click Navigate to Item to navigate to the user.

Troubleshooting Privileges and Roles

I cannot assign privileges or roles to users for an existing Metadata Manager Service, PowerCenter Repository Service, or Reporting Service.

You cannot assign privileges and roles to users and groups for an existing Metadata Manager Service, PowerCenter Repository Service, or Reporting Service in the following situations:

- The application service is disabled.
- The PowerCenter Repository Service is running in exclusive mode.

I cannot assign privileges to a user for an enabled Reporting Service.

Data Analyzer uses the user account name and security domain name in the format *UserName@SecurityDomain* to determine the length of the user login name. You cannot assign privileges or roles to a user for a Reporting Service when the combination of the user name, @ symbol, and security domain name exceeds 128 characters.

I removed a privilege from a group. Why do some users in the group still have that privilege?

You can use any of the following methods to assign privileges to a user:

- Assign a privilege directly to a user.
- Assign a privilege to a role, and then assign the role to a user.
- Assign a privilege to a group that the user belongs to.

If you remove a privilege from a group, users that belong to that group can be directly assigned the privilege or can inherit the privilege from an assigned role.

I am assigned all domain privileges and permission on all domain objects, but I cannot complete all tasks in the Administrator tool.

Some of the Administrator tool tasks are determined by the Administrator role, not by privileges or permissions. You can be assigned all privileges for the domain and granted full permissions on all domain objects. However, you cannot complete the tasks determined by the Administrator role.

I am assigned the Administrator role for an application service, but I cannot configure the application service in the Administrator tool.

When you have the Administrator role for an application service, you are an application client administrator. An application client administrator has full permissions and privileges in an application client.

However, an application client administrator does not have permissions or privileges on the Informatica domain. An application client administrator cannot log in to the Administrator tool to manage the service for the application client for which it has administrator privileges.

To manage an application service in the Administrator tool, you must have the appropriate domain privileges and permissions.

I am assigned the Administrator role for the PowerCenter Repository Service, but I cannot use the Repository Manager to perform an advanced purge of objects or to create reusable metadata extensions.

You must have the Manage Services domain privilege and permission on the PowerCenter Repository Service in the Administrator tool to perform the following actions in the Repository Manager:

- Perform an advanced purge of object versions at the PowerCenter repository level.
- Create, edit, and delete reusable metadata extensions.

My privileges indicate that I should be able to edit objects in an application client, but I cannot edit any metadata.

You might not have the required object permissions in the application client. Even if you have the privilege to perform certain actions, you may also require permission to perform the action on a particular object.

I cannot use pmrep to connect to a new PowerCenter Repository Service running in exclusive mode.

The Service Manager might not have synchronized the list of users and groups in the PowerCenter repository with the list in the domain configuration database. To synchronize the list of users and groups, restart the PowerCenter Repository Service.

I am assigned all privileges in the Folders privilege group for the PowerCenter Repository Service and have read, write, and execute permission on a folder. However, I cannot configure the permissions for the folder.

Only the folder owner or a user assigned the Administrator role for the PowerCenter Repository Service can complete the following folder management tasks:

- Assign operating system profiles to folders if the PowerCenter Integration Service uses operating system profiles. Requires permission on the operating system profile.
- Change the folder owner.
- Configure folder permissions.
- Delete the folder.
- Designate the folder to be shared.
- Edit the folder name and description.

CHAPTER 9

Permissions

This chapter includes the following topics:

- Permissions Overview, 111
- Domain Object Permissions, 113
- Connection Permissions, 117
- SQL Data Service Permissions, 119
- Web Service Permissions, 123

Permissions Overview

You manage user security with privileges and permissions. Permissions define the level of access that users and groups have to an object. Even if a user has the privilege to perform certain actions, the user may also require permission to perform the action on a particular object.

For example, a user has the Manage Services domain privilege and permission on the Development PowerCenter Repository Service, but not on the Production PowerCenter Repository Service. The user can edit or remove the Development PowerCenter Repository Service, but not the Production PowerCenter Repository Service. To manage an application service, a user must have the Manage Services domain privilege and permission on the application service.

You use different tools to configure permissions on the following objects:

Object Type	Tool	Description
Connection objects	Administrator tool Analyst tool Developer tool	You can assign permissions on connections defined in the Administrator tool, Analyst tool, or Developer tool. These tools share the connection permissions.
Data Analyzer objects	Data Analyzer	You can assign permissions on Data Analyzer folders, reports, dashboards, attributes, metrics, template dimensions, and schedules.
Domain objects	Administrator tool	You can assign permissions on the following domain objects: domain, folders, nodes, grids, licenses,

Object Type	Tool	Description
		application services, and operating system profiles.
Metadata Manager catalog objects	Metadata Manager	You can assign permissions on Metadata Manager folders and catalog objects.
Model repository projects	Analyst tool Developer tool	You can assign permissions on projects defined in the Analyst tool and Developer tool. These tools share project permissions.
PowerCenter repository objects	PowerCenter Client	You can assign permissions on PowerCenter folders, deployment groups, labels, queries, and connection objects.
SQL data service objects	Administrator tool	You can assign permissions on SQL data objects, such as SQL data services, virtual schemas, virtual tables, and virtual stored procedures.
Web service objects	Administrator tool	You can assign permissions on web services or web service operations.

Types of Permissions

Users and groups can have the following types of permissions in a domain:

Direct permissions

Permissions that are assigned directly to a user or group. When users and groups have permission on an object, they can perform administrative tasks on that object if they also have the appropriate privilege. You can edit direct permissions.

Inherited permissions

Permissions that users inherit. When users have permission on a domain or a folder, they inherit permission on all objects in the domain or the folder. When groups have permission on a domain object, all subgroups and users belonging to the group inherit permission on the domain object. For example, a domain has a folder named Nodes that contains multiple nodes. If you assign a group permission on the folder, all subgroups and users belonging to the group inherit permission on the folder and on all nodes in the folder.

You cannot revoke inherited permissions. You also cannot revoke permissions from users or groups assigned the Administrator role. The Administrator role bypasses permission checking. Users with the Administrator role can access all objects.

You can deny inherited permissions on some object types. When you deny permissions, you configure exceptions to the permissions that users and groups might already have.

Effective permissions

Superset of all permissions for a user or group. Includes direct permissions and inherited permissions.

When you view permission details, you can view the origin of effective permissions. Permission details display direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.

Permission Search Filters

When you assign permissions, view permission details, or edit permissions for a user or group, you can use search filters to search for a user or group.

When you manage permissions for a user or group, you can use the following search filters:

Security domain

Select the security domain to search for users or groups.

Pattern string

Enter a string to search for users or groups. The Administrator tool returns all names that contain the search string. The string is not case sensitive. For example, the string "DA" can return "iasdaemon," "daphne," and "DA_AdminGroup."

You can also sort the list of users or groups. Right-click a column name to sort the column in ascending or descending order.

Domain Object Permissions

You configure privileges and permissions to manage user security within the domain. Permissions define the level of access a user has to a domain object. To log in to the Administrator tool, a user must have permission on at least one domain object. If a user has permission on an object, but does not have the domain privilege that grants the ability to modify the object type, then the user can only view the object. For example, if a user has permission on a node, but does not have the Manage Nodes and Grids privilege, the user can view the node properties, but cannot configure, shut down, or remove the node.

You can configure permissions on the following types of domain objects:

Domain Object Type	Description of Permission
Domain	Enables Administrator tool users to access all objects in the domain. When users have permission on a domain, they inherit permission on all objects in the domain.
Folder	Enables Administrator tool users to access all objects in the folder in the Administrator tool. When users have permission on a folder, they inherit permission on all objects in the folder.
Node	Enables Administrator tool users to view and edit the node properties. Without permission, a user cannot use the node when defining an application service or creating a grid.
Grid	Enables Administrator tool users to view and edit the grid properties. Without permission, a user cannot assign the grid to a PowerCenter Integration Service.
License	Enables Administrator tool users to view and edit the license properties. Without permission, a user cannot use the license when creating an application service.

Domain Object Type	Description of Permission
Application Service	Enables Administrator tool users to view and edit the application service properties.
Operating System Profile	Enables PowerCenter users to run workflows associated with the operating system profile. If the user that runs a workflow does not have permission on the operating system profile assigned to the workflow, the workflow fails.

You can use the following methods to manage domain object permissions:

- Manage permissions by domain object. Use the Permissions view of a domain object to assign and edit permissions on the object for multiple users or groups.
- Manage permissions by user or group. Use the Manage Permissions dialog box to assign and edit permissions on domain objects for a specific user or group.

Note: You configure permissions on an operating system profile differently than you configure permissions on other domain objects.

Permissions by Domain Object

Use the **Permissions** view of a domain object to assign, view, and edit permissions on the domain object for multiple users or groups.

Assigning Permissions on a Domain Object

When you assign permissions on a domain object, you grant users and groups access to the object.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select the domain object.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Click **Actions** > **Assign Permission**.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the object.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group, and click **Next**.
8. Select **Allow**, and click **Finish**.

Viewing Permission Details on a Domain Object

When you view permission details, you can view the origin of effective permissions.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select the domain object.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Enter the filter conditions to search for users and groups, and click the **Filter** button.
6. Select a user or group and click **Actions** > **View Permission Details**.

The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.

7. Click **Close**.
8. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on a Domain Object

You can edit direct permissions on a domain object for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select the domain object.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Enter the filter conditions to search for users and groups, and click the **Filter** button.
6. Select a user or group and click **Actions** > **Edit Direct Permissions**.

   The **Edit Direct Permissions** dialog box appears.
7. To assign permission on the object, select **Allow**.
8. To revoke permission on the object, select **Revoke**.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.
9. Click **OK**.

Permissions by User or Group

Use the **Manage Permissions** dialog box to view, assign, and edit domain object permissions for a specific user or group.

Viewing Permission Details for a User or Group

When you view permission details, you can view the origin of effective permissions.

1. In the header of Infomatica Administrator, click **Manage** > **Permissions**.

   The **Manage Permissions** dialog box appears.
2. Click the **Groups** or **Users** tab.
3. Enter a string to search for users and groups, and click the **Filter** button.
4. Select a user or group.
5. Select a domain object and click the **View Permission Details** button.

   The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.
6. Click **Close**.
7. Or, click **Edit Permissions** to edit direct permissions.

Assigning and Editing Permissions for a User or Group

When you edit domain object permissions for a user or group, you can assign permissions and edit existing direct permissions. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. In the header of Infomatica Administrator, click **Manage** > **Permissions**.

   The **Manage Permissions** dialog box appears.
2. Click the **Groups** or **Users** tab.
3. Enter a string to search for users and groups and click the **Filter** button.
4. Select a user or group.
5. Select a domain object and click the **Edit Direct Permissions** button.

   The **Edit Direct Permissions** dialog box appears.
6. To assign permission on the object, select **Allow**.
7. To revoke permission on the object, select **Revoke**.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.
8. Click **OK**.
9. Click **Close**.

Operating System Profile Permissions

Use the **Configure Operating System Profiles** dialog box to assign, view, and edit permissions on operating system profiles.

Assigning Permissions on an Operating System Profile

When you assign permissions on an operating system profile, PowerCenter users can run workflows assigned to the operating system profile.

1. On the **Security** tab, click **Actions** > **Configure Operating System Profiles**.

   The **Configure Operating System Profiles** dialog box appears.
2. Select the operating system profile, and click the **Permissions** tab.
3. Select the **Groups** or **Users** view, and click the **Assign Permission** button.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the operating system profile.
4. Enter the filter conditions to search for users and groups, and click the **Filter** button.
5. Select a user or group, and click **Next**.
6. Select **Allow**, and click **Finish**.

Viewing Permission Details on an Operating System Profile

When you view permission details, you can view the origin of effective permissions.

1. On the **Security** tab, click **Actions** > **Configure Operating System Profiles**.

   The **Configure Operating System Profiles** dialog box appears.
2. Select the operating system profile, and click the **Permissions** tab.

3. Select the **Groups** or **Users** view.
4. Enter the filter conditions to search for users and groups, and click the **Filter** button.
5. Select a user or group and click **Actions** > **View Permission Details**.

   The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.
6. Click **Close**.
7. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on an Operating System Profile

You can edit direct permissions on an operating system profile for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the **Security** tab, click **Actions** > **Configure Operating System Profiles**.

   The **Configure Operating System Profiles** dialog box appears.
2. Select the operating system profile, and click the **Permissions** tab.
3. Select the **Groups** or **Users** view.
4. Enter the filter conditions to search for users and groups, and click the **Filter** button.
5. Select a user or group and click **Actions** > **Edit Direct Permissions**.

   The **Edit Direct Permissions** dialog box appears.
6. To assign permission on the operating system profile, select **Allow**.
7. To revoke permission on the operating system profile, select **Revoke**.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.
8. Click **OK**.

Connection Permissions

Permissions control the level of access that a user or group has on the connection.

You can configure permissions on a connection in the Analyst tool, Developer tool, or Administrator tool.

Any connection permission that is assigned to a user or group in one tool also applies in other tools. For example, you grant GroupA permission on ConnectionA in the Developer tool. GroupA has permission on ConnectionA in the Analyst tool and Administrator tool also.

The following Informatica components use the connection permissions:

- Administrator tool. Enforces read, write, and execute permissions on connections.
- Analyst tool. Does not enforce connection permissions because analysts cannot edit or delete connections. Analysts can view basic connection metadata, such as connection name, description, and type.
- Informatica command line interface. Enforces read, write, and grant permissions on connections.

- Developer tool. Enforces read, write, and execute permissions on connections. For SQL data services, the Developer tool does not enforce connection permissions. Instead, it enforces column-level and pass-through security to restrict access to data.
- Data Integration Service. Enforces execute permissions when a user tries to preview data or run a mapping, scorecard, or profile.

Note: You cannot assign permissions on the following connections: profiling warehouse, staging database, data object cache database, or Model repository.

Related Topics:

- "Column Level Security" on page 122
- " Pass-through Security" on page 170

Types of Connection Permissions

You can assign different permission types to users to perform the following actions:

Action	Permission Types
View all connection metadata, except passwords, such as connection name, type, description, connection strings, and user names.	Read
Write all connection metadata, such as connection strings. Users with Write permission inherit Read permission.	Write
Access to all physical data in the tables in the connection. Users can preview data or run a mapping, scorecard, or profile.	Execute
Grant and revoke permissions on connections.	Grant

Default Connection Permissions

The domain administrator has all permissions on all connections. The user that creates a connection has read, write, and execute permission on the connection. By default, all users have permission to perform the following actions on connections:

- View basic connection metadata, such as connection name, type, and description.
- Use the connection in mappings in the Developer tool.
- Create profiles in the Analyst tool on objects in the connection.

Assigning Permissions on a Connection

When you assign permissions on a connection, you define the level of access a user or group has to the connection.

1. On the Domain tab, select the **Connections** view.
2. In the Navigator, select the connection.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.

5. Click **Actions** > **Assign Permission**.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the connection.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group, and click **Next**.
8. Select **Allow** for each permission type that you want to assign.
9. Click **Finish**.

Editing Permissions on a Connection

You can edit direct permissions on a connection for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the Domain tab, select the **Connections** view.
2. In the Navigator, select the connection.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Enter the filter conditions to search for users and groups, and click the **Filter** button.
6. Select a user or group and click **Actions** > **Edit Direct Permissions**.

   The **Edit Direct Permissions** dialog box appears.
7. Choose to allow or revoke permissions.
   - Select **Allow** to assign a permission.
   - Clear **Allow** to revoke a single permission.
   - Select **Revoke** to revoke all permissions.
8. Click **OK**.

SQL Data Service Permissions

End users can connect to an SQL data service through a JDBC or ODBC client tool. After connecting, users can run SQL queries against virtual tables in an SQL data service, or users can run a virtual stored procedure in an SQL data service. Permissions control the level of access that a user has to an SQL data service.

You can assign permissions to users and groups on the following SQL data service objects:

- SQL data service
- Virtual table
- Virtual stored procedure

When you assign permissions on an SQL data service object, the user or group inherits the same permissions on all objects that belong to the SQL data service object. For example, you assign a user select permission on an SQL data service. The user inherits select permission on all virtual tables in the SQL data service.

You can deny permissions to users and groups on some SQL data service objects. When you deny permissions, you configure exceptions to the permissions that users and groups might already have. For example, you cannot

assign permissions to a column in a virtual table, but you can deny a user from running an SQL SELECT statement that includes the column.

Types of SQL Data Service Permissions

You can assign the following permissions to users and groups:

- Grant permission. Users can grant and revoke permissions on the SQL data service objects using the Administrator tool or using the *infacmd* command line program.
- Execute permission. Users can run virtual stored procedures in the SQL data service using a JDBC or ODBC client tool.
- Select permission. Users can run SQL SELECT statements on virtual tables in the SQL data service using a JDBC or ODBC client tool.

Some permissions are not applicable for all SQL data service objects.

The following table describes the permissions for each SQL data service object:

Object	Grant Permission	Execute Permission	Select Permission
SQL data service	Grant and revoke permission on the SQL data service and all objects within the SQL data service.	Run all virtual stored procedures in the SQL data service.	Run SQL SELECT statements on all virtual tables in the SQL data service.
Virtual table	Grant and revoke permission on the virtual table.	n/a	Run SQL SELECT statements on the virtual table.
Virtual stored procedure	Grant and revoke permission on the virtual stored procedure.	Run the virtual stored procedure.	n/a

Assigning Permissions on an SQL Data Service

When you assign permissions on an SQL data service object, you define the level of access a user or group has to the object.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the SQL data service object.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Click the **Assign Permission** button.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the SQL data service object.
7. Enter the filter conditions to search for users and groups, and click the **Filter** button.
8. Select a user or group, and click **Next**.
9. Select **Allow** for each permission type that you want to assign.
10. Click **Finish**.

Viewing Permission Details on an SQL Data Service

When you view permission details, you can view the origin of effective permissions.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the SQL data service object.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group and click the **View Permission Details** button.

   The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.
8. Click **Close**.
9. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on an SQL Data Service

You can edit direct permissions on an SQL data service for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the SQL data service object.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group and click the **Edit Direct Permissions** button.

   The **Edit Direct Permissions** dialog box appears.
8. Choose to allow or revoke permissions.
   - Select **Allow** to assign a permission.
   - Clear **Allow** to revoke a single permission.
   - Select **Revoke** to revoke all permissions.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.
9. Click **OK**.

Denying Permissions on an SQL Data Service

You can explicitly deny permissions on some SQL data service objects. When you deny a permission on an object in an SQL data service, you are applying an exception to the effective permission.

To deny permissions use one of the following infacmd commands:

- infacmd sql SetStoredProcedurePermissions. Denies Execute or Grant permissions at the stored procedure level.
- infacmd sql SetTablePermissions. Denies Select and Grant permissions at the virtual table level.
- infacmd sql SetColumnPermissions. Denies Select permission at the column level.

Each command has options to apply permissions (-ap) and deny permissions (-dp). The SetColumnPermissions command does not include the apply permissions option.

Note: You cannot deny permissions from the Administrator tool.

The Data Integration Service verifies permissions before running SQL queries and stored procedures against the virtual database. The Data Integration Service validates the permissions for users or groups starting at the SQL data service level. When permissions apply to a parent object in an SQL data service, the child objects inherit the permission. The Data Integration Service checks for denied permissions at the column level.

Column Level Security

An Administrator can deny access to columns in a virtual table of an SQL data object. The Administrator can configure the Data Integration Service behavior for queries against a restricted column.

The following results might occur when the user queries a column that the user does not have permissions for:

- The query returns a substitute value instead of the data. The query returns a substitute value in each row that it returns. The substitute value replaces the column value through the query. If the query includes filters or joins, the results substitute appears in the results.
- The query fails with an insufficient permission error.

For more information about configuring security for SQL data services, see the Informatica How-To Library article "How to Configure Security for SQL Data Services": http://communities.informatica.com/docs/DOC-4507.

Related Topics:

- “ Connection Permissions” on page 117

Restricted Columns

When you configure column level security, set a column option that determines what happens when a user selects the restricted column in a query. You can substitute the restricted data with a default value. Or, you can fail the query if a user selects the restricted column.

For example, an Administrator denies a user access to the salary column in the Employee table. The Administrator configures a substitute value of 100,000 for the salary column. When the user selects the salary column in an SQL query, the Data Integration Service returns 100,000 for the salary in each row.

Run the infacmd sql UpdateColumnOptions command to configure the column options. You cannot set column options in the Administrator tool.

When you run infacmd sql UpdateColumnOptions, enter the following options:

ColumnOptions.DenyWith=*option*

Determines whether to substitute the restricted column value or to fail the query. If you substitute the column value, you can choose to substitute the value with NULL or with a constant value. Enter one of the following options:

- ERROR. Fails the query and returns an error when an SQL query selects a restricted column.
- NULL. Returns null values for a restricted column in each row.
- VALUE. Returns a constant value in place of the restricted column in each row. Configure the constant value in the ColumnOptions.InsufficientPermissionValue option.

ColumnOptions.InsufficientPermissionValue=*value*

Substitutes the restricted column value with a constant. The default is an empty string. If the Data Integration Service substitutes the column with an empty string, but the column is a number or a date, the query returns errors. If you do not configure a value for the DenyWith option, the Data Integration Service ignores the InsufficientPermissionValue option.

To configure a substitute value for a column, enter the command with the following syntax:

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sqlds
employee_APP.employees_SQL -t Employee -c Salary -o ColumnOptions.DenyWith=VALUE
ColumnOptions.InsufficientPermissionValue=100000
```

If you do not configure either option for a restricted column, default is not to fail the query. The query runs and the Data Integration Service substitutes the column value with NULL.

Adding Column Level Security

Configure column level security with the infacmd sql SetColumnPermissions command. You cannot set column level security from the Administrator tool.

An Employee table contains FirstName, LastName, Dept, and Salary columns. You enable a user to access the Employee table but restrict the user from accessing the salary column.

To restrict the user from the salary column, disable the Data Integration Service and enter an infacmd similar to the following command:

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sqlds
employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

The following SQL statements return NULL in the salary column:

```
Select * from Employee
Select LastName, Salary from Employee
```

The default behavior is to return null values.

Web Service Permissions

End users can send web service requests and receive web service responses through a web service client. Permissions control the level of access that a user has to a web service.

You can assign permissions to users and groups on the following web service objects:

- Web service
- Web service operation

When you assign permissions on a web service object, the user or group inherits the same permissions on all objects that belong to the web service object. For example, you assign a user execute permission on a web service. The user inherits execute permission on web service operations in the web service.

You can deny permissions to users and groups on a web service operation. When you deny permissions, you configure exceptions to the permissions that users and groups might already have. For example, a user has execute permissions on a web service which has three operations. You can deny a user from running one web service operation that belongs to the web service.

Types of Web Service Permissions

You can assign the following permissions to users and groups:

- Grant permission. Users can manage permissions on the web service objects using the Administrator tool or using the *infacmd* command line program.
- Execute permission. Users can send web service requests and receive web service responses.

The following table describes the permissions for each web service object:

Object	Grant Permission	Execute Permission
Web service	Grant and revoke permission on the web service and all web service operations within the web service.	Send web service requests and receive web service responses from all web service operations within the web service.
Web service operation	Grant, revoke, and deny permission on the web service operation.	Send web service requests and receive web service responses from the web service operation.

Assigning Permissions on a Web Service

When you assign permissions on a web service object, you define the level of access a user or group has to the object.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the web service object.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Click the **Assign Permission** button.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the SQL data service object.
7. Enter the filter conditions to search for users and groups, and click the **Filter** button.
8. Select a user or group, and click **Next**.
9. Select **Allow** for each permission type that you want to assign.
10. Click **Finish**.

Viewing Permission Details on a Web Service

When you view permission details, you can view the origin of effective permissions.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the web service object.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group and click the **View Permission Details** button.

   The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.
8. Click **Close**.
9. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on a Web Service

You can edit direct permissions on a web service for a user or group. When you edit permissions on a web service object, you can deny permissions on the object. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the web service object.
5. In the details panel, select the **Group Permissions** or **User Permissions**view.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group and click the **Edit Direct Permissions** button.

   The **Edit Direct Permissions** dialog box appears.
8. Choose to allow or revoke permissions.
   - Select **Allow** to assign a permission.
   - Select **Deny** to deny a permission on a web service object.
   - Clear **Allow** to revoke a single permission.
   - Select **Revoke** to revoke all permissions.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.
9. Click **OK**.

CHAPTER 10

High Availability

This chapter includes the following topics:

- High Availability Overview, 126
- High Availability in the Base Product, 129
- Achieving High Availability, 131
- Managing Resilience, 133
- Managing High Availability for the PowerCenter Repository Service, 136
- Managing High Availability for the PowerCenter Integration Service, 137
- Troubleshooting High Availability, 142

High Availability Overview

The term *high availability* refers to the uninterrupted availability of computer system resources. In an Informatica domain, high availability eliminates a single point of failure in a domain and provides minimal service interruption in the event of failure. When you configure high availability for a domain, the domain can continue running despite temporary network, hardware, or service failures.

The following high availability components make services highly available in a Informatica domain:

- Resilience. The ability of an Informatica domain to tolerate temporary connection failures until either the resilience timeout expires or the failure is fixed.
- Restart and failover. The restart of a service or task or the migration to a backup node after the service becomes unavailable on the primary node.
- Recovery. The completion of operations after a service is interrupted. After a service process restarts or fails over, it restores the service state and recovers operations.

When you plan a highly available Informatica environment, consider the differences between internal Informatica components and systems that are external to Informatica. Internal components include Service Manager, application services, the PowerCenter Client, and command line programs. External systems include the network, hardware, database management systems, FTP servers, message queues, and shared storage.

If you have the high availability option, you can achieve full high availability of internal Informatica components. You can achieve high availability with external components based on the availability of those components. If you do not have the high availability option, you can achieve some high availability of internal components.

Example

While you are fetching a mapping into the PowerCenter Designer workspace, the PowerCenter Repository Service becomes unavailable, and the request fails. The PowerCenter Repository Service fails over to another node because it cannot restart on the same node.

The PowerCenter Designer is resilient to temporary failures and tries to establish a connection to the PowerCenter Repository Service. The PowerCenter Repository Service starts within the resilience timeout period, and the PowerCenter Designer reestablishes the connection.

After the PowerCenter Designer reestablishes the connection, the PowerCenter Repository Service recovers from the failed operation and fetches the mapping into the PowerCenter Designer workspace.

Resilience

Resilience is the ability of application service clients to tolerate temporary network failures until the timeout period expires or the system failure is resolved. Clients that are resilient to a temporary failure can maintain connection to a service for the duration of the timeout.

All clients of PowerCenter components are resilient to service failures. A client of a service can be any PowerCenter Client tool or PowerCenter service that depends on the service. For example, the PowerCenter Integration Service is a client of the PowerCenter Repository Service. If the PowerCenter Repository Service becomes unavailable, the PowerCenter Integration Service tries to reestablish the connection. If the PowerCenter Repository Service becomes available within the timeout period, the PowerCenter Integration Service is able to connect. If the PowerCenter Repository Service is not available within the timeout period, the request fails.

PowerCenter services may also be resilient to temporary failures of external systems, such as database systems, FTP servers, and message queue sources. For this type of resilience to work, the external systems must be highly available. You need the high availability option or the real-time option to configure resilience to external system failures.

Internal Resilience

Internal resilience occurs within the Informatica environment among application services, the Informatica client tools, and other client applications such as *pmrep* and *pmcmd*. You can configure internal resilience at the following levels:

- Domain. You configure application service connection resilience at the domain level in the general properties for the domain. The domain resilience timeout determines how long application services try to connect as clients to application services or the Service Manager. The domain resilience properties are the default values for all application services that have internal resilience.
- Application service. You can also configure service connection resilience in the advanced properties for an application service. When you configure connection resilience for an application service, you override the resilience values from the domain settings.
- Gateway. The master gateway node maintains a connection to the domain configuration repository. If the domain configuration repository becomes unavailable, the master gateway node tries to reconnect. The resilience timeout period depends on user activity and the number of gateway nodes:
  - Single gateway node. If the domain has one gateway node, the gateway node tries to reconnect until a user or service tries to perform a domain operation. When a user tries to perform a domain operation, the master gateway node shuts down.

- Multiple gateway nodes. If the domain has multiple gateway nodes and the master gateway node cannot reconnect, then the master gateway node shuts down. If a user tries to perform a domain operation while the master gateway node is trying to connect, the master gateway node shuts down. If another gateway node is available, the domain elects a new master gateway node. The domain tries to connect to the domain configuration repository with each gateway node. If none of the gateway nodes can connect, the domain shuts down and all domain operations fail.

  When a master gateway fails over, the client tools retrieve information about the alternate domain gateways from the domains.infa file.

Note: The Model Repository, Data Integration Service, and Analyst Service do not have internal resilience. If the master gateway node becomes unavailable and fails over to another gateway node, you must restart these services. After the restart, the services do not restore the state of operation and do not recover from the point of interruption. You must restart jobs that were previously running during the interruption.

External Resilience

Services in the domain can also be resilient to the temporary unavailability of systems that are external to Informatica, such as FTP servers and database management systems.

You can configure the following types of external resilience for application services:

- Database connection resilience for PowerCenter Integration Service. The PowerCenter Integration Service depends on external database systems to run sessions and workflows. If a database is temporarily unavailable, the PowerCenter Integration Service tries to connect for a specified amount of time. The PowerCenter Integration Service is resilient when connecting to a database when a session starts, when the PowerCenter Integration Services fetches data from a relational source or uncached lookup, or it writes data to a relational target.

  The PowerCenter Integration Service is resilient if the database supports resilience. You configure the connection retry period in the relational connection object for a database.
- Database connection resilience for PowerCenter Repository Service. The PowerCenter Repository Service can be resilient to temporary unavailability of the repository database system. A client request to the PowerCenter Repository Service does not necessarily fail if the database system becomes temporarily unavailable. The PowerCenter Repository Service tries to reestablish connections to the database system and complete the interrupted request. You configure the repository database resilience timeout in the database properties of a PowerCenter Repository Service.
- Database connection resilience for master gateway node. The master gateway node can be resilient to temporary unavailability of the domain configuration database. The master gateway node maintains a connection to the domain configuration database. If the domain configuration database becomes unavailable, the master gateway node tries to reconnect. The timeout period depends on whether the domain has one or multiple gateway nodes.
- FTP connection resilience. If a connection is lost while the PowerCenter Integration Service is transferring files to or from an FTP server, the PowerCenter Integration Service tries to reconnect for the amount of time configured in the FTP connection object. The PowerCenter Integration Service is resilient to interruptions if the FTP server supports resilience.
- Client connection resilience. You can configure connection resilience for PowerCenter Integration Service clients that are external applications using C/Java LMAPI. You configure this type of resilience in the Application connection object.

Restart and Failover

If a service process becomes unavailable, the Service Manager can restart the process or fail it over to a backup node based on the availability of the node. When a PowerCenter service process restarts or fails over, the service

restores the state of operation and begins recovery from the point of interruption. When a PowerExchange service process restarts or fails over, the service process restarts on the same node or on the backup node.

You can configure backup nodes for PowerCenter application services and PowerExchange application services if you have the high availability option. If you configure an application service to run on primary and backup nodes, one service process can run at a time. The following situations describe restart and failover for an application service:

- If the primary node running the service process becomes unavailable, the service fails over to a backup node. The primary node might be unavailable if it shuts down or if the connection to the node becomes unavailable.
- If the primary node running the service process is available, the domain tries to restart the process based on the restart options configured in the domain properties. If the process does not restart, the Service Manager may mark the process as failed. The service then fails over to a backup node and starts another process. If the Service Manager marks the process as failed, the administrator must enable the process after addressing any configuration problem.

If a service process fails over to a backup node, it does not fail back to the primary node when the node becomes available. You can disable the service process on the backup node to cause it to fail back to the primary node.

Recovery

Recovery is the completion of operations after an interrupted service is restored. When a service recovers, it restores the state of operation and continues processing the job from the point of interruption.

The state of operation for a service contains information about the service process. The PowerCenter services include the following states of operation:

- Service Manager. The Service Manager for each node in the domain maintains the state of service processes running on that node. If the master gateway shuts down, the newly elected master gateway collects the state information from each node to restore the state of the domain.
- PowerCenter Repository Service. The PowerCenter Repository Service maintains the state of operation in the repository. This includes information about repository locks, requests in progress, and connected clients.
- PowerCenter Integration Service. The PowerCenter Integration Service maintains the state of operation in the shared storage configured for the service. This includes information about scheduled, running, and completed tasks for the service. The PowerCenter Integration Service maintains PowerCenter session and workflow state of operation based on the recovery strategy you configure for the session and workflow.

High Availability in the Base Product

Informatica provides some high availability functionality that does not require the high availability option. The base product provides the following high availability functionality:

- Internal PowerCenter resilience. The Service Manager, application services, PowerCenter Client, and command line programs are resilient to temporary unavailability of other PowerCenter internal components.
- PowerCenter Repository database resilience. The PowerCenter Repository Service is resilient to temporary unavailability of the repository database.
- Restart services. The Service Manager can restart application services after a failure.
- Manual recovery of PowerCenter workflows and sessions. You can manually recover PowerCenter workflows and sessions.
- Multiple gateway nodes. You can configure multiple nodes as gateway.

Note: You must have the high availability option for failover and automatic recovery.

Internal PowerCenter Resilience

Internal PowerCenter components are resilient to temporary unavailability of other PowerCenter components. PowerCenter components include the Service Manager, application services, the PowerCenter Client, and command line programs. You can configure the resilience timeout and the limit on resilience timeout for the domain, application services, and command line programs.

The PowerCenter Client is resilient to temporary unavailability of the application services. For example, temporary network failure can cause the PowerCenter Integration Service to be unavailable to the PowerCenter Client. The PowerCenter Client tries to reconnect to the PowerCenter Integration Service during the resilience timeout period.

PowerCenter Repository Service Resilience to PowerCenter Repository Database

The PowerCenter Repository Service is resilient to temporary unavailability of the repository database. If the repository database becomes unavailable, the PowerCenter Repository Service tries to reconnect within the database connection timeout period. If the database becomes available and the PowerCenter Repository Service reconnects, the PowerCenter Repository Service can continue processing repository requests. You configure the database connection timeout in the PowerCenter Repository Service database properties.

Restart Services

If an application service process fails, the Service Manager restarts the process on the same node.

On Windows, you can configure Informatica services to restart when the Service Manager fails or the operating system starts.

The PowerCenter Integration Service cannot automatically recover failed operations without the high availability option.

Manual PowerCenter Workflow and Session Recovery

You can manually recover a workflow and all tasks in the workflow without the high availability option. To recover a workflow, you must configure the workflow for recovery. When you configure a workflow for recovery, the PowerCenter Integration Service stores the state of operation that it uses to begin processing from the point of interruption.

You can manually recover a session without the high availability option. To recover a PowerCenter session, you must configure the recovery strategy for the session. If you have the high availability option, the PowerCenter Integration Service can automatically recover PowerCenter workflows.

Multiple Gateway Nodes

You can define multiple gateway nodes to achieve some resilience between the domain and the master gateway node without the high availability option. If you have multiple gateway nodes and the master gateway node becomes unavailable, the Service Managers on the other gateway nodes elect another master gateway node to accept service requests. Without the high availability option, you cannot configure an application service to run on a multiple nodes. Therefore, application services running on the master gateway node will not fail over when another master gateway node is elected.

If you have one gateway node and it becomes unavailable, the domain cannot accept service requests. If none of the gateway nodes can connect, the domain shuts down and all domain operations fail.

Achieving High Availability

You can achieve different degrees of availability depending on factors that are internal and external to the Informatica environment. For example, you can achieve a greater degree of availability when you configure more than one node to serve as a gateway and when you configure backup nodes for application services.

Consider internal components and external systems when you are designing a highly available PowerCenter environment:

- PowerCenter internal components. Configure nodes and services for high availability.
- External systems. Use highly available external systems for hardware, shared storage, database systems, networks, message queues, and FTP servers.

Note: The Analyst Service, Data Integration Service, Metadata Manager Service, Model Repository Service, Listener Service, Logger Service, Reporting Service, SAP BW Service, and Web Services Hub are not highly available.

Configuring PowerCenter Internal Components for High Availability

PowerCenter internal components include the Service Manager, nodes, and PowerCenter services within the Informatica environment. You can configure nodes and services to enhance availability:

- Configure more than one gateway. You can configure multiple nodes in a domain to serve as the gateway. Only one node serves as the gateway at any given time. That node is called the master gateway. If the master gateway becomes unavailable, the Service Manager elects another master gateway node. If you configure only one gateway node, the gateway is a single point of failure. If the gateway node becomes unavailable, the Service Manager cannot accept service requests.
- Configure application services to run on multiple nodes. You can configure the application services to run on multiple nodes in a domain. A service is available if at least one designated node is available.
- Configure access to shared storage. You need to configure access to shared storage when you configure multiple gateway nodes and multiple backup nodes for the PowerCenter Integration Service. When you configure more than one gateway node, each gateway node must have access to the domain configuration database. When you configure the PowerCenter Integration Service to run on more than one node, each node must have access to the run-time files used to process a session or workflow.

When you design a highly available PowerCenter environment, you can configure the nodes and services to minimize failover or to optimize performance:

- Minimize service failover. Configure two nodes as gateway. Configure different primary nodes for each application service.
- Optimize performance. Configure gateway nodes on machines that are dedicated to serve as a gateway. Configure backup nodes for the PowerCenter Integration Service and the PowerCenter Repository Service.

Minimizing Service Failover

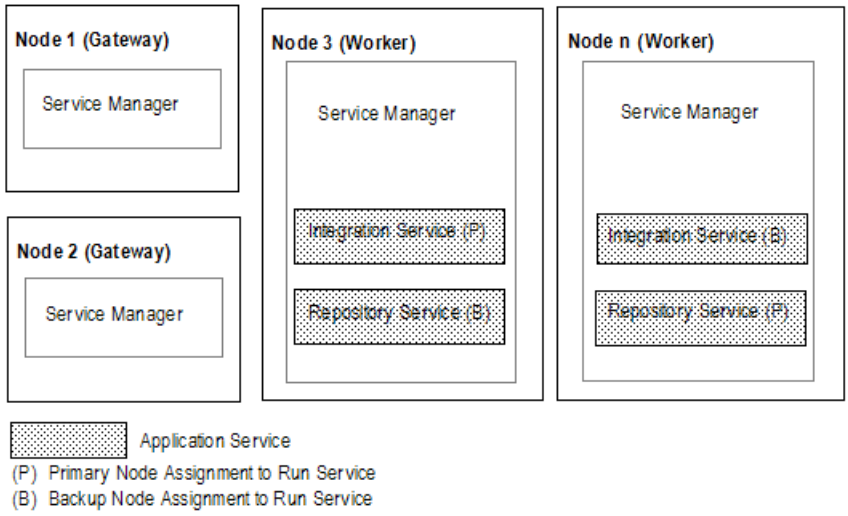
To minimize service failover in a domain with two nodes, configure the PowerCenter Integration Service and PowerCenter Repository Service to run on opposite primary nodes. Configure one node as the primary node for the PowerCenter Integration Service, and configure the other node as the primary node for the PowerCenter Repository Service.

Optimizing Performance

To optimize performance in a domain, configure gateway operations and applications services to run on separate nodes. Configure the PowerCenter Integration Service and the PowerCenter Repository Service to run on multiple

worker nodes. When you separate the gateway operations from the application services, the application services do not interfere with gateway operations when they consume a high level of CPUs.

The following figure shows a configuration with two gateway nodes and multiple backup nodes for the PowerCenter Integration Service and PowerCenter Repository Service:



Using Highly Available External Systems

Informatica depends on external systems such as file systems and databases for repositories, sources, and targets. To optimize Informatica availability, ensure that external systems are also highly available. Use the following rules and guidelines to configure external systems:

- Use a highly available database management system for the repository and domain configuration database. Follow the guidelines of the database system when you plan redundant components and backup and restore policies.
- Use highly available versions of other external systems, such as source and target database systems, message queues, and FTP servers.
- Use a highly available POSIX compliant shared file system for the shared storage used by services in the domain.
- Make the network highly available by configuring redundant components such as routers, cables, and network adapter cards.

Rules and Guidelines for Configuring for High Availability

Use the following rules and guidelines when you set up high availability for the PowerCenter environment:

- Install and configure PowerCenter services on multiple nodes.
- For each node, configure Informatica Services to restart if it terminates unexpectedly.
- In the Administrator tool, configure at least two nodes to serve as gateway nodes.
- Configure the PowerCenter Repository Services to run on at least two nodes.
- Configure the PowerCenter Integration Services to run on multiple nodes. Configure primary and backup nodes or a grid. If you configure the PowerCenter Integration Services to run on a grid, make resources available to more than one node.

- Use highly available database management systems for the repository databases associated with PowerCenter Repository Services and the domain configuration database.
- Use a highly available POSIX compliant shared file system that is configured for I/O fencing in order to ensure PowerCenter Integration Service failover and recovery. To be highly available, the shared file system must be configured for I/O fencing. The hardware requirements and configuration of an I/O fencing solution are different for each file system. When possible, it is recommended to use hardware I/O fencing. PowerCenter nodes need to be on the same shared file system so that they can share resources. For example, the PowerCenter Integration Service on each node needs to be able to access the log and recovery files within the shared file system. Also, all PowerCenter nodes within a cluster must be on the cluster file system's heartbeat network. The following shared file systems are certified by Informatica for use in PowerCenter Integration Service failover and session recovery:

  Storage Array Network

  Veritas Cluster Files System (VxFS)

  IBM General Parallel File System (GPFS)

  Network Attached Storage using NFS v3 protocol

  EMC UxFS hosted on an EMV Celerra NAS appliance

  NetApp WAFL hosted on a NetApp NAS appliance

  Informatica recommends that customers contact the file system vendors directly to evaluate which file system matches their requirements.

Tip: To perform maintenance on a node without service interruption, disable the service process on the node so that the service fails over to a backup node.

Managing Resilience

Resilience is the ability of PowerCenter Service clients to tolerate temporary network failures until the resilience timeout period expires or the external system failure is fixed. A client of a service can be any PowerCenter Client or PowerCenter service that depends on the service. Clients that are resilient to a temporary failure can try to reconnect to a service for the duration of the timeout.

For example, the PowerCenter Integration Service is a client of the PowerCenter Repository Service. If the PowerCenter Repository Service becomes unavailable, the PowerCenter Integration Service tries to reestablish the connection. If the PowerCenter Repository Service becomes available within the timeout period, the PowerCenter Integration Service is able to connect. If the PowerCenter Repository Service is not available within the timeout period, the request fails.

You can configure the following resilience properties for the domain, application services, and command line programs:

- Resilience timeout. The amount of time a client tries to connect or reconnect to a service. A limit on resilience timeouts can override the timeout.
- Limit on resilience timeout. The amount of time a service waits for a client to connect or reconnect to the service. This limit can override the client resilience timeouts configured for a connecting client. This is available for the domain and application services.

Note: The Model Repository, Data Integration Service, Analyst Service, Logger Service, and Listener Service are not resilient.

Configuring Service Resilience for the Domain

The domain resilience timeout determines how long services try to connect as clients to other services. The default value is 30 seconds.

The limit on resilience timeout is the maximum amount of time that a service allows another service to connect as a client. This limit overrides the resilience timeout for the connecting service if the resilience timeout is a greater value. The default value is 180 seconds.

You can configure resilience properties for each service or you can configure each service to use the domain values.

Configuring Application Service Resilience

When an application service connects to another service in the domain, the connecting service is a client of the other service. When an application service connects to another application service, the resilience timeout is determined by one of the following values:

- Configured value. You can configure the resilience timeout for the service in the service properties. To disable resilience for a service, set the resilience timeout to 0. The default is 180 seconds.
- Domain resilience timeout. To use the resilience timeout configured for the domain, set the service resilience timeout to blank.
- Limit on timeout. If the limit on resilience timeout for the service is smaller than the resilience timeout for the connecting client, the client uses the limit as the resilience timeout. To use the limit on resilience timeout configured for the domain, set the service limit to blank. The default is 180 seconds.

You configure the resilience timeout and resilience timeout limits for the PowerCenter Integration Service and the PowerCenter Repository Service in the advanced properties for the service. You configure the resilience timeout for the SAP BW Service in the general properties for the service. The property for the SAP BW Service is called the retry period.

Note: A client cannot be resilient to service interruptions if you disable the service in the Administrator tool. If you disable the service process, the client is resilient to the interruption in service.

Understanding PowerCenter Client Resilience

PowerCenter Client resilience timeout determines the amount of time the PowerCenter Client tries to connect or reconnect to the PowerCenter Repository Service or the PowerCenter Integration Service. The PowerCenter Client resilience timeout is 180 seconds and is not configurable. This resilience timeout is bound by the service limit on resilience timeout.

If you perform a PowerCenter Client action that requires connection to the repository while the PowerCenter Client is trying to reestablish the connection, the PowerCenter Client prompts you to try the operation again after the PowerCenter Client reestablishes the connection. If the PowerCenter Client is unable to reestablish the connection during the resilience timeout period, the PowerCenter Client prompts you to reconnect to the repository manually.

Configuring Command Line Program Resilience

When you use a command line program to connect to the domain or an application service, the resilience timeout is determined by one of the following values:

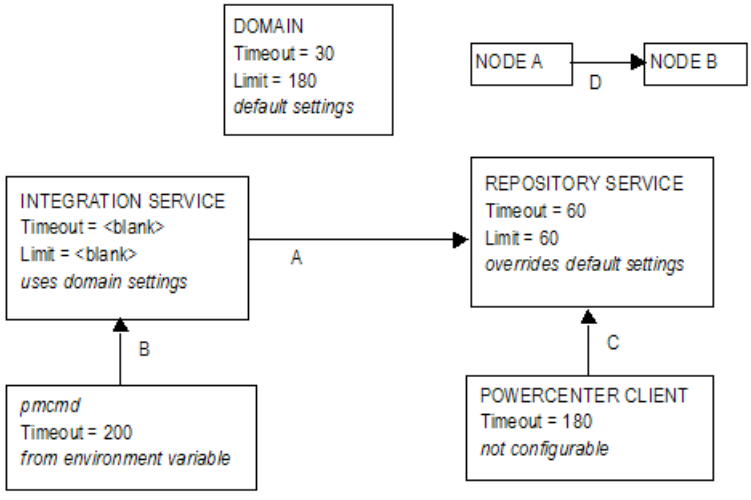
- Command line option. You can determine the resilience timeout for command line programs by using a command line option, -timeout or -t, each time you run a command.

- Environment variable. If you do not use the timeout option in the command line syntax, the command line program uses the value of the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT that is configured on the client machine.
- Default value. If you do not use the command line option or the environment variable, the command line program uses the default resilience timeout of 180 seconds.
- Limit on timeout. If the limit on resilience timeout for the service is smaller than the command line resilience timeout, the command line program uses the limit as the resilience timeout.

Note: PowerCenter does not provide resilience for a repository client when the PowerCenter Repository Service is running in exclusive mode.

Example

The following figure shows some sample connections and resilience configurations in a domain:



The following table describes the resilience timeout and the limits shown in the preceding figure:

	Connect From	Connect To	Description
A	PowerCenter Integration Service	PowerCenter Repository Service	The PowerCenter Integration Service can spend up to 30 seconds to connect to the PowerCenter Repository Service, based on the domain resilience timeout. It is not bound by the PowerCenter Repository Service limit on resilience timeout of 60 seconds.
B	*pmcmd*	PowerCenter Integration Service	*pmcmd* is bound by the PowerCenter Integration Service limit on resilience timeout of 180 seconds, and it cannot use the 200 second resilience timeout configured in INFA_CLIENT_RESILIENCE_TIMEOUT.
C	PowerCenter Client	PowerCenter Repository Service	The PowerCenter Client is bound by the PowerCenter Repository Service limit on resilience timeout of 60 seconds. It cannot use the default resilience timeout of 180 seconds.
D	Node A	Node B	Node A can spend up to 30 seconds to connect to Node B. The Service Manager on Node A uses the domain configuration for resilience timeout. The Service Manager on Node B uses the domain configuration for limit on resilience timeout.

Managing High Availability for the PowerCenter Repository Service

High availability for the PowerCenter Repository Service includes the following behavior:

- Resilience. The PowerCenter Repository Service is resilient to temporary unavailability of other services and the repository database. PowerCenter Repository Service clients are resilient to connections with the PowerCenter Repository Service.
- Restart and failover. If the PowerCenter Repository Service fails, the Service Manager can restart the service or fail it over to another node, based on node availability.
- Recovery. After restart or failover, the PowerCenter Repository Service can recover operations from the point of interruption.

Resilience

The PowerCenter Repository Service is resilient to temporary unavailability of other services. Services can be unavailable because of network failure or because a service process fails. The PowerCenter Repository Service is also resilient to temporary unavailability of the repository database. This can occur because of network failure or because the repository database system becomes unavailable.

PowerCenter Repository Service clients are resilient to temporary unavailability of the PowerCenter Repository Service. A PowerCenter Repository Service client is any PowerCenter Client or PowerCenter service that depends on the PowerCenter Repository Service. For example, the PowerCenter Integration Service is a PowerCenter Repository Service client because it depends on the PowerCenter Repository Service for a connection to the repository.

You can configure the PowerCenter Repository Service to be resilient to temporary unavailability of the repository database. The repository database may become unavailable because of network failure or because the repository database system becomes unavailable. If the repository database becomes unavailable, the PowerCenter Repository Service tries to reconnect to the repository database within the period specified by the database connection timeout configured in the PowerCenter Repository Service properties.

Tip: If the repository database system has high availability features, set the database connection timeout to allow the repository database system enough time to become available before the PowerCenter Repository Service tries to reconnect to it. Test the database system features that you plan to use to determine the optimum database connection timeout.

You can configure some PowerCenter Repository Service clients to be resilient to connections with the PowerCenter Repository Service. You configure the resilience timeout and the limit on resilience timeout for the PowerCenter Repository Service in the advanced properties when you create the PowerCenter Repository Service. PowerCenter Client resilience timeout is 180 seconds and is not configurable.

Restart and Failover

If the PowerCenter Repository Service process fails, the Service Manager can restart the process on the same node. If the node is not available, the PowerCenter Repository Service process fails over to the backup node. The PowerCenter Repository Service process fails over to a backup node in the following situations:

- The PowerCenter Repository Service process fails and the primary node is not available.
- The PowerCenter Repository Service process is running on a node that fails.
- You disable the PowerCenter Repository Service process.

After failover, PowerCenter Repository Service clients synchronize and connect to the PowerCenter Repository Service process without loss of service.

You may want to disable a PowerCenter Repository Service process to shut down a node for maintenance. If you disable a PowerCenter Repository Service process in complete or abort mode, the PowerCenter Repository Service process fails over to another node.

Recovery

The PowerCenter Repository Service maintains the state of operation in the repository. This includes information about repository locks, requests in progress, and connected clients. After a PowerCenter Repository Service restarts or fails over, it restores the state of operation from the repository and recovers operations from the point of interruption.

The PowerCenter Repository Service performs the following tasks to recover operations:

- Gets locks on repository objects, such as mappings and sessions
- Reconnects to clients, such as the PowerCenter Designer and the PowerCenter Integration Service
- Completes requests in progress, such as saving a mapping
- Sends outstanding notifications about metadata changes, such as workflow schedule changes

Managing High Availability for the PowerCenter Integration Service

High availability for the PowerCenter Integration Service includes the following behavior:

- Resilience. A PowerCenter Integration Service process is resilient to connections with PowerCenter Integration Service clients and with external components.
- Restart and failover If the PowerCenter Integration Service process becomes unavailable, the Service Manager can restart the process or fail it over to another node.
- Recovery. When the PowerCenter Integration Service restarts or fails over a service process, it can automatically recover interrupted workflows that are configured for recovery.

Resilience

The PowerCenter Integration Service is resilient to temporary unavailability of other services, PowerCenter Integration Service clients, and external components such databases and FTP servers. If the PowerCenter Integration Service loses connectivity to other services and PowerCenter Integration Service clients within the PowerCenter Integration Service resilience timeout period. The PowerCenter Integration Service tries to reconnect to external components within the resilience timeout for the database or FTP connection object.

Note: You must have the high availability option for resilience when the PowerCenter Integration Service loses connection to an external component. All other PowerCenter Integration Service resilience is part of the base product.

Service and Client Resilience

PowerCenter Integration Service clients are resilient to temporary unavailability of the PowerCenter Integration Service. This can occur because of network failure or because a PowerCenter Integration Service process fails. PowerCenter Integration Service clients include the PowerCenter Client, the Service Manager, the Web Services Hub, and *pmcmd*. PowerCenter Integration Service clients also include applications developed using LMAPI.

You configure the resilience timeout and the limit on resilience timeout in the PowerCenter Integration Service advanced properties.

External Component Resilience

A PowerCenter Integration Service process is resilient to temporary unavailability of external components. External components can be temporarily unavailable because of network failure or the component experiences a failure. If the PowerCenter Integration Service process loses connection to an external component, it tries to reconnect to the component within the retry period for the connection object.

If the PowerCenter Integration Service loses the connection when it transfers files to or from an FTP server, the PowerCenter Integration Service tries to reconnect for the amount of time configured in the FTP connection object. The PowerCenter Integration Service is resilient to interruptions if the FTP server supports resilience.

If the PowerCenter Integration Service loses the connection when it connects or retrieves data from a database for sources or Lookup transformations, it tries to reconnect for the amount of time configured in the database connection object. If a connection is lost when the PowerCenter Integration Service writes data to a target database, it tries to reconnect for the amount of time configured in the database connection object.

For example, you configure a retry period of 180 for a database connection object. If PowerCenter Integration Service connectivity to a database fails during the initial connection to the database, or connectivity fails when the PowerCenter Integration Service reads data from the database, it tries to reconnect for 180 seconds. If it cannot reconnect to the database and you configure the workflow for automatic recovery, the PowerCenter Integration Service recovers the session. Otherwise, the session fails.

You can configure the retry period when you create or edit the database or FTP server connection object.

Restart and Failover

If a PowerCenter Integration Service process becomes unavailable, the Service Manager tries to restart it or fails it over to another node based on the shutdown mode, the service configuration, and the operating mode for the service. Restart and failover behavior is different for services that run on a single node, primary and backup nodes, or on a grid.

When the PowerCenter Integration Service fails over, the behavior of completed tasks depends on the following situations:

- If a completed task reported a completed status to the PowerCenter Integration Service process prior to the PowerCenter Integration Service failure, the task will not restart.
- If a completed task did not report a completed status to the PowerCenter Integration Service process prior to the PowerCenter Integration Service failure, the task will restart.

Running on a Single Node

The following table describes the failover behavior for a PowerCenter Integration Service if only one service process is running:

Source of Shutdown	Restart and Failover Behavior
Service Process	If the service process shuts down unexpectedly, the Service Manager tries to restart the service process. If it cannot restart the process, the process stops or fails. When you restart the process, the PowerCenter Integration Service restores the state of operation for the service and restores workflow schedules, service requests, and workflows.

Source of Shutdown	Restart and Failover Behavior
	The failover and recovery behavior of the PowerCenter Integration Service after a service process fails depends on the operating mode: - Normal. When you restart the process, the workflow fails over on the same node. The PowerCenter Integration Service can recover the workflow based on the workflow state and recovery strategy. If the workflow is enabled for HA recovery, the PowerCenter Integration Service restores the state of operation for the workflow and recovers the workflow from the point of interruption. The PowerCenter Integration Service performs failover and recovers the schedules, requests, and workflows. If a scheduled workflow is not enabled for HA recovery, the PowerCenter Integration Service removes the workflow from the schedule. - Safe. When you restart the process, the workflow does not fail over and the PowerCenter Integration Service does not recover the workflow. It performs failover and recovers the schedules, requests, and workflows when you enable the service in normal mode.
Service	When the PowerCenter Integration Service becomes unavailable, you must enable the service and start the service processes. You can manually recover workflows and sessions based on the state and the configured recovery strategy. The workflows that run after you start the service processes depend on the operating mode: - Normal. Workflows configured to run continuously or on initialization will start. You must reschedule all other workflows. - Safe. Scheduled workflows do not start. You must enable the service in normal mode for the scheduled workflows to run.
Node	When the node becomes unavailable, the restart and failover behavior is the same as restart and failover for the service process, based on the operating mode.

Running on a Primary Node

The following table describes the failover behavior for a PowerCenter Integration Service configured to run on primary and backup nodes:

Source of Shutdown	Restart and Failover Behavior
Service Process	When you disable the service process on a primary node, the service process fails over to a backup node. When the service process on a primary node shuts down unexpectedly, the Service Manager tries to restart the service process before failing it over to a backup node. After the service process fails over to a backup node, the PowerCenter Integration Service restores the state of operation for the service and restores workflow schedules, service requests, and workflows. The failover and recovery behavior of the PowerCenter Integration Service after a service process fails depends on the operating mode: - Normal. The PowerCenter Integration Service can recover the workflow based on the workflow state and recovery strategy. If the workflow was enabled for HA recovery, the PowerCenter Integration Service restores the state of operation for the workflow and recovers the workflow from the point of interruption. The PowerCenter Integration Service performs failover and recovers the schedules, requests, and workflows. If a scheduled workflow is not enabled for HA recovery, the PowerCenter Integration Service removes the workflow from the schedule. - Safe. The PowerCenter Integration Service does not run scheduled workflows and it disables schedule failover, automatic workflow recovery, workflow failover, and client request recovery. It performs failover and recovers the schedules, requests, and workflows when you enable the service in normal mode.
Service	When the PowerCenter Integration Service becomes unavailable, you must enable the service and start the service processes. You can manually recover workflows and sessions based on the state and the configured recovery strategy. Workflows configured to run continuously or on initialization will start. You must reschedule all other workflows.

Source of Shutdown	Restart and Failover Behavior
	The workflows that run after you start the service processes depend on the operating mode: - Normal. Workflows configured to run continuously or on initialization will start. You must reschedule all other workflows. - Safe. Scheduled workflows do not start. You must enable the service in normal mode to run the scheduled workflows.
Node	When the node becomes unavailable, the failover behavior is the same as the failover for the service process, based on the operating mode.

Running on a Grid

The following table describes the failover behavior for a PowerCenter Integration Service configured to run on a grid:

Source of Shutdown	Restart and Failover Behavior
Master Service Process	If you disable the master service process, the Service Manager elects another node to run the master service process. If the master service process shuts down unexpectedly, the Service Manager tries to restart the process before electing another node to run the master service process. The master service process then reconfigures the grid to run on one less node. The PowerCenter Integration Service restores the state of operation, and the workflow fails over to the newly elected master service process. The PowerCenter Integration Service can recover the workflow based on the workflow state and recovery strategy. If the workflow was enabled for HA recovery, the PowerCenter Integration Service restores the state of operation for the workflow and recovers the workflow from the point of interruption. When the PowerCenter Integration Service restores the state of operation for the service, it restores workflow schedules, service requests, and workflows. The PowerCenter Integration Service performs failover and recovers the schedules, requests, and workflows. If a scheduled workflow is not enabled for HA recovery, the PowerCenter Integration Service removes the workflow from the schedule.
Worker Service Process	If you disable a worker service process, the master service process reconfigures the grid to run on one less node. If the worker service process shuts down unexpectedly, the Service Manager tries to restart the process before the master service process reconfigures the grid. After the master service process reconfigures the grid, it can recover tasks based on task state and recovery strategy. Since workflows do not run on the worker service process, workflow failover is not applicable.
Service	When the PowerCenter Integration Service becomes unavailable, you must enable the service and start the service processes. You can manually recover workflows and sessions based on the state and the configured recovery strategy. Workflows configured to run continuously or on initialization will start. You must reschedule all other workflows.
Node	When the node running the master service process becomes unavailable, the failover behavior is the same as the failover for the master service process. When the node running the worker service process becomes unavailable, the failover behavior is the same as the failover for the worker service process.
Note: You cannot configure a PowerCenter Integration Service to fail over in safe mode when it runs on a grid.	

Recovery

When you have the high availability option, the PowerCenter Integration Service can automatically recover workflows and tasks based on the recovery strategy, the state of the workflows and tasks, and the PowerCenter Integration Service operating mode:

- Stopped, aborted, or terminated workflows. In normal mode, the PowerCenter Integration Service can recover stopped, aborted, or terminated workflows from the point of interruption. In safe mode, automatic recovery is disabled until you enable the service in normal mode. After you enable normal mode, the PowerCenter Integration Service automatically recovers the workflow.
- Running workflows. In normal and safe mode, the PowerCenter Integration Service can recover terminated tasks while the workflow is running.
- Suspended workflows. The PowerCenter Integration Service can restore the workflow state after the workflow fails over to another node if you enable recovery in the workflow properties.

Stopped, Aborted, or Terminated Workflows

When the PowerCenter Integration Service restarts or fails over a service process, it can automatically recover interrupted workflows that are configured for recovery, based on the operating mode. When you run a workflow that is enabled for HA recovery, the PowerCenter Integration Service stores the state of operation in the $PMStorageDir directory. When the PowerCenter Integration Service recovers a workflow, it restores the state of operation and begins recovery from the point of interruption. The PowerCenter Integration Service can recover a workflow with a stopped, aborted, or terminated status.

In normal mode, the PowerCenter Integration Service can automatically recover the workflow. In safe mode, the PowerCenter Integration Service does not recover the workflow until you enable the service in normal mode

When the PowerCenter Integration Service recovers a workflow that failed over, it begins recovery at the point of interruption. The PowerCenter Integration Service can recover a task with a stopped, aborted, or terminated status according to the recovery strategy for the task. The PowerCenter Integration Service behavior for task recovery does not depend on the operating mode.

Note: The PowerCenter Integration Service does not automatically recover a workflow or task that you stop or abort through the PowerCenter Workflow Monitor or *pmcmd*.

Running Workflows

You can configure automatic task recovery in the workflow properties. When you configure automatic task recovery, the PowerCenter Integration Service can recover terminated tasks while the workflow is running. You can also configure the number of times that the PowerCenter Integration Service tries to recover the task. If the PowerCenter Integration Service cannot recover the task in the configured number of times for recovery, the task and the workflow are terminated.

The PowerCenter Integration Service behavior for task recovery does not depend on the operating mode.

Suspended Workflows

If a service process shuts down while a workflow is suspended, the PowerCenter Integration Service marks the workflow as terminated. It fails the workflow over to another node, and changes the workflow state to terminated. The PowerCenter Integration Service does not recover any workflow task. You can fix the errors that caused the workflow to suspend, and manually recover the workflow.

Troubleshooting High Availability

The solutions to the following situations might help you with high availability.

I am not sure where to look for status information regarding client connections to the repository.

In PowerCenter Client applications such as the PowerCenter Designer and the PowerCenter Workflow Manager, an error message appears if the connection cannot be established during the timeout period. Detailed information about the connection failure appears in the Output window. If you are using *pmrep*, the connection error information appears at the command line. If the PowerCenter Integration Service cannot establish a connection to the repository, the error appears in the PowerCenter Integration Service log, the workflow log, and the session log.

I entered the wrong connection string for an Oracle database. Now I cannot enable the PowerCenter Repository Service even though I edited the PowerCenter Repository Service properties to use the right connection string.

You need to wait for the database resilience timeout to expire before you can enable the PowerCenter Repository Service with the updated connection string.

I have the high availability option, but my FTP server is not resilient when the network connection fails.

The FTP server is an external system. To achieve high availability for FTP transmissions, you must use a highly available FTP server. For example, Microsoft IIS 6.0 does not natively support the restart of file uploads or file downloads. File restarts must be managed by the client connecting to the IIS server. If the transfer of a file to or from the IIS 6.0 server is interrupted and then reestablished within the client resilience timeout period, the transfer does not necessarily continue as expected. If the write process is more than half complete, the target file may be rejected.

I have the high availability option, but the Informatica domain is not resilient when machines are connected through a network switch.

If you are using a network switch to connect machines in the domain, use the auto-select option for the switch.

CHAPTER 11

Analyst Service

This chapter includes the following topics:

- Analyst Service Overview, 143
- Analyst Service Architecture, 144
- Configuration Prerequisites, 144
- Configure the TLS Protocol, 146
- Recycling and Disabling the Analyst Service, 147
- Properties for the Analyst Service, 147
- Process Properties for the Analyst Service, 149
- Creating and Deleting Audit Trail Tables, 151
- Creating and Configuring the Analyst Service, 152
- Creating an Analyst Service, 152

Analyst Service Overview

The Analyst Service is an application service that runs Informatica Analyst in the Informatica domain. The Analyst Service manages the connections between service components and the users that have access to the Analyst tool.

The Analyst Service connects to a Data Integration Service, Model Repository Service, the Analyst tool, staging database, and a flat file cache location.

You can use the Administrator tool to administer the Analyst Service. You can create and recycle an Analyst Service in the Informatica domain to access the Analyst tool. When you recycle the Analyst Service, the Service Manager restarts the Analyst Service.

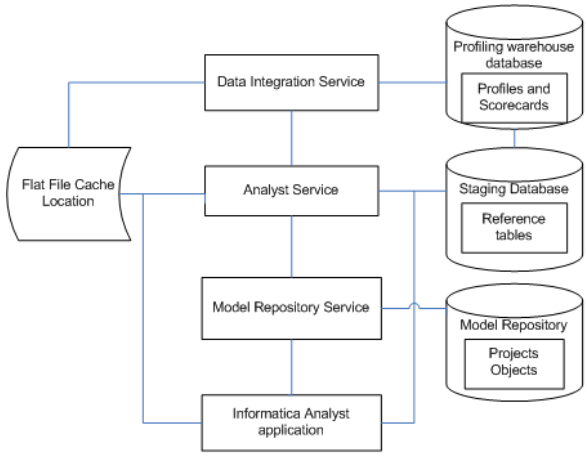
You manage users, groups, privileges, and roles on the Security tab of the Administrator tool. You manage permissions for projects and objects in the Analyst tool.

You can run more than one Analyst Service on the same node. You can associate one Model Repository Service with an Analyst Service. You can associate one Data Integration Service with more than one Analyst Service.

Analyst Service Architecture

The Analyst Service is an application service that runs the Analyst tool and manages connections between service components and Analyst tool users.

The following figure shows the Analyst tool components that the Analyst Service manages on a node in the Informatica domain:



The Analyst Service manages the connections between the following components:

- Data Integration Service. The Analyst Service manages the connection to a Data Integration Service for the Analyst tool to run or preview project components in the Analyst tool.
- Model Repository Service. The Analyst Service manages the connection to a Model Repository Service for the Analyst tool. The Analyst tool connects to the model repository database to create, update, and delete projects and objects in the Analyst tool.
- Staging database. The Analyst Service manages the connection to a database that stores reference tables that you create or import in the Analyst tool. The associated Data Integration Service also uses a staging database to store reference tables.
- Flat file cache location. The Analyst Service manages the connection to the directory that stores uploaded flat files that you use as imported reference tables and flat file sources in the Analyst tool.
- Informatica Analyst. The Analyst Service manages the Analyst tool. Use the Analyst tool to analyze, cleanse, and standardize data in an enterprise. Use the Analyst tool to collaborate with data quality and data integration developers on data quality integration solutions. You can perform column and rule profiling, manage scorecards, and manage bad records and duplicate records in the Analyst tool. You can also manage and provide reference data to developers in a data quality solution.

Configuration Prerequisites

Before you configure the Analyst Service, you need to complete the prerequisite tasks for the service. The Data Integration Service and the Model Repository Service must be enabled. You need a database to store the reference tables you create or import in the Analyst tool, and a directory to upload flat files that the Data Integration Service can access. You need a keystore file if you configure the Transport Layer Security protocol for the Analyst Service.

The Analyst Service requires the following prerequisite tasks:

- Create associated services.
- Create a staging database.
- Specify a location for the flat file cache.

Associated Services

Before you configure the Analyst Service, the associated Data Integration Service and the Model Repository Service must be enabled. When you create the Analyst Service, you can specify an existing Data Integration Service and Model Repository Service.

The Analyst Service requires the following associated services:

- Data Integration Service. When you create a Data Integration Service you also create a profiling warehouse database to store profiling information and scorecard results. When you create the database connection for the database, you must also create content if no content exists for the database.
- Model Repository Service. Before you create a Model Repository Service you must create a database to store the model repository. When you create the Model Repository Service, you must also create repository content if no content exists for the model repository.

Staging Databases

The Analyst Service uses a staging database to store reference tables that you create or import in the Analyst tool. The associated Data Integration Service also uses a staging database to store reference tables. You can use the same database connection for the staging database that the Analyst Service uses and the database that the Data Integration Service uses.

You can use Oracle, Microsoft SQL Server, or IBM DB2 as staging databases.

After you create a database, you create a database connection that the Data Integration Service uses to connect to the database. When you create the Analyst Service, you select an existing database connection or create a database connection.

The following table describes the database connection options if you create a database:

Option	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the connection. The description cannot exceed 765 characters.
Database Type	Type of relational database. You can select Oracle, Microsoft SQL Server, or IBM DB2.
Username	Database user name.
Password	Password for the database user name.
Connection String	Connection string used to access data from the database. - IBM DB2: <database name> - Microsoft SQL Server: <server name>@<database name> - Oracle: <database name listed in TNSNAMES entry>

Option	Description
JDBC URL	JDBC connection URL used to access metadata from the database. - IBM DB2: jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name> - Oracle: jdbc:informatica:oracle://<host_name>:<port>;SID=<database name> - Microsoft SQL Server: jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name>
Code Page	Code page use to read from a source database or write to a target database or file.

Flat File Cache

Create a directory to store uploaded flat files from a local machine to a location in the Informatica services installation directory that the Data Integration Service can access. When you import a reference table or flat file source, Informatica Analyst uses the files from this directory to create a reference table or file object.

For example, you can create a directory named "flatfilecache" in the following location:

```
<Informatica_services_installation_directory>\server\
```

Keystore File

A keystore file contains the keys and certificates required if you enable Transport Layer Security (TLS) and use the HTTPS protocol for the Analyst Service. You can create the keystore file when you install Informatica services or you can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a file called a “keystore.” When you generate a public or private key pair, keytool wraps the public key into a self-signed certificate. You can use the self-signed certificate or use a certificate signed by a certificate authority.

Note: You must use a certified keystore file. If you do not use a certified keystore file, security warnings and error messages for the browser appear when you access the Analyst tool.

Configure the TLS Protocol

For greater security, you can configure the Transport Layer Security (TLS) protocol mode for the Analyst Service. You can configure the TLS protocol when you create the Analyst Service.

The following table describes the TLS protocol properties that you can configure when you create the Analyst Service:

Property	Description
HTTPS Port	HTTPS port number that the Informatica Analyst application runs on when you enable the Transport Layer Security (TLS) protocol. Use a different port number than the HTTP port number.
Keystore File	Location of the file that includes private or public key pairs and associated certificates.

Property	Description
Keystore Password	Plain-text password for the keystore file. Default is "changeit."
SSL Protocol	Secure Sockets Layer Protocol for security.

Recycling and Disabling the Analyst Service

Use the Administrator tool to recycle and disable the Analyst Service. Disable an Analyst Service to perform maintenance or temporarily restrict users from accessing Informatica Analyst. When you disable the Analyst Service, you also stop the Analyst tool. When you recycle the Analyst Service, you stop and start the service to make the Analyst tool available again.

In the Navigator, select the Analyst Service and click the Disable button to stop the service. Click the Recycle button to start the service.

When you disable the Analyst Service, you must choose the mode to disable it in. You can choose one of the following options:

- Complete. Allows the jobs to run to completion before disabling the service.
- Abort. Tries to stop all jobs before aborting them and disabling the service.

Note: The Model Repository Service and the Data Integration Service must be running before you recycle the Analyst Service.

Properties for the Analyst Service

After you create an Analyst Service, you can configure the Analyst Service properties. You can configure Analyst Service properties on the Properties tab in the Administrator tool.

For each service properties section, click Edit to modify the service properties.

You can configure the following types of Analyst Service properties:

- General Properties
- Model Repository Service Options
- Data Integration Service Options
- Staging Database
- Logging Options
- Custom Properties

General Properties for the Analyst Service

General properties for the Analyst Service include the name and description of the Analyst Service, and the node in the Informatica domain that the Analyst Service runs on. You can configure these properties when you create the Analyst Service.

The following table describes the general properties for the Analyst Service:

Property	Description
Name	Name of the Analyst Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the Analyst Service. The description cannot exceed 765 characters.
Node	Node in the Informatica domain on which the Analyst Service runs. If you change the node, you must recycle the Analyst Service.
License	License assigned to the Analyst Service.

Model Repository Service Options

Model Repository Service property includes the Model Repository Service that is associated with the Analyst Service.

The following table describes the Model Repository Service properties for the Analyst Service:

Property	Description
Model Repository Service	Model Repository Service associated with the Analyst Service. The Analyst Service manages the connections to the Model Repository Service for Informatica Analyst. You must recycle the Analyst Service if you associate another Model Repository Service with the Analyst Service.
Username	The database user name for the Model repository.
Password	An encrypted version of the database password for the Model repository.
Security Domain	LDAP Security domain for the user who manages the Model Repository Service.

Data Integration Service Options

Data Integration Service properties include the Data Integration Service associated with the Analyst Service and the flat file cache location.

The following table describes the Data Integration Service properties for the Analyst Service:

Property	Description
Data Integration Service Name	Data Integration Service name associated with the Analyst Service. The Analyst Service manages the connection to a Data Integration Service for Informatica Analyst. You must recycle the Analyst Service if you associate another Data Integration Service with the Analyst Service.
Flat File Cache Location	Location of the flat file cache where Informatica Analyst stores uploaded flat files. When you import a reference table or flat file source, Informatica Analyst uses the files from this directory to create a reference table or file object. Restart the Analyst Service if you change the flat file location.

Property	Description
Username	User name for a Data Integration Service administrator.
Password	Password for the administrator user name.
Security Domain	Name of the security domain that the user belongs to.

Staging Database

The Staging Database properties include the database connection name and properties for an IBM DB2 EEE database or a Microsoft SQL Server database.

The following table describes the staging database properties for the Analyst Service:

Property	Description
Resource Name	Database connection name for the staging database. You must recycle the Analyst Service if you use another database connection name.
Tablespace Name	Tablespace name for an IBM DB2 EEE database with multiple partitions.
Schema Name	The schema name for a Microsoft SQL Server database.
Owner Name	Database schema owner name for a Microsoft SQL Server database.

Note: IBM DB2 EEE databases use tablespaces as a container for tablespace pages. If you use an IBM DB2 EEE database as the staging database, you must set the tablespace page size to a minimum of 8 KB. If the tablespace page size is less than 8 KB, the Analyst tool cannot create all the reference tables in the staging database.

Logging Options

The logging options include properties for the severity level for Analyst Service Logs. Valid values are Info, Error, Warning, Trace, Debug, Fatal. Default is Info.

Custom Properties

Custom properties include properties that are unique to your environment or that apply in special cases.

An Analyst Service does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Process Properties for the Analyst Service

The Analyst Service runs the Analyst Service process on a node. When you select the Analyst Service in the Administrator tool, you can view the service processes for the Analyst Service on the **Processes** tab. You can view the node properties for the service process in the service panel. You can view the service process properties in the Service Process Properties panel.

Note: You must select the node to view the service process properties in the Service Process Properties panel.

You can configure the following types of Analyst Service process properties:

- Analyst Security Options
- Advanced Properties
- Custom Properties
- Environment Variables

Node Properties for the Analyst Service Process

The following table describes the node properties for the Analyst Service process:

Property	Description
Node	Node that the service process runs on.
Node Status	Status of the node. Status can be enabled or disabled.
Process Configuration	Status of the process configured to run on the node.
Process State	State of the service process running on the node. The state can be enabled or disabled.

Analyst Security Options for the Analyst Service Process

The Analyst Service Options include security properties for the Analyst Service process.

The following table describes the security properties for the Analyst Service process:

Property	Description
HTTP Port	HTTP port number on which the Analyst tool runs. Use a port number that is different from the HTTP port number for the Data Integration Service. Default is 8085. You must recycle the service if you change the HTTP port number.
HTTPS Port	HTTPS port number that the Analyst tool runs on when you enable the Transport Layer Security (TLS) protocol. Use a differnet port number than the HTTP port number. You must recycle the service if you change the HTTPS port number.
Keystore File	Location of the file that includes private or public key pairs and associated certificates.
Keystore Password	Plain-text password for the keystore file. Default is "changeit."
SSL Protocol	Secure Sockets Layer Protocol for Security.

Advanced Properties for the Analyst Service Process

Advanced properties include properties for the maximum heap size and the Java Virtual Manager (JVM) memory settings.

The following table describes the advanced properties for the Analyst Service process:

Property	Description
Maximum Heap Size	Amount of RAM allocated to the Java Virtual Machine (JVM) that runs the Analyst Service. Use this property to increase the performance. Append one of the following letters to the value to specify the units: - b for bytes. - k for kilobytes. - m for megabytes. - g for gigabytes. Default is 512 megabytes.
JVM Command Line Options	Java Virtual Machine (JVM) command line options to run Java-based programs. When you configure the JVM options, you must set the Java SDK classpath, Java SDK minimum memory, and Java SDK maximum memory properties.

Custom Properties for the Analyst Service Process

Custom properties include properties that are unique to your environment or that apply in special cases.

An Analyst Service does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Environment Variables for the Analyst Service Process

You can edit environment variables for the Analyst Service process.

The following table describes the environment variables for the Analyst Service process:

Property	Description
Environment Variables	Environment variables defined for the Analyst Service process.

Creating and Deleting Audit Trail Tables

Audit trail tables store the audit trail log events that provide information about the reference tables you manage in the Analyst tool.

Create audit trail tables in the Administrator tool to view the audit trail log events for reference tables in the Analyst tool. Delete audit trail tables after an upgrade, or to use another database connection for a different reference table.

1. In the Navigator, select the Analyst Service.
2. To create audit trail tables, click **Actions** > **Audit Trail tables** > **Create**.
3. Optionally, to delete the tables, click **Delete**.

Creating and Configuring the Analyst Service

Use the Administrator tool to create and configure the Analyst Service. After you create the Analyst Service, you can configure the service properties and service process properties. You can enable the Analyst Service to make the Analyst tool accessible to users.

1. Complete the prerequisite tasks for configuring the Analyst Service.
2. Create the Analyst Service.
3. Configure the Analyst Service properties.
4. Configure the Analyst Service process properties.
5. Recycle the Analyst Service.

Creating an Analyst Service

Create an Analyst Service to manage the Informatica Analyst application and to grant users access to Informatica Analyst.

1. In the Administrator tool, click the **Domain** tab.
2. On the Domain Actions menu, click **New** > **Analyst Service.**

   The **New Analyst Service** window appears.
3. Enter the general properties for the service and the location and HTTP port number for the service.

   Optionally, click Browse in the **Location** field to enter the location for the domain and folder where you want to create the service. Optionally, click Create Folder to create another folder.
4. Enter the **Model Repository Service** name and the user name and password to connect to the Model Repository Service.
5. Click **Next**.
6. Enter the Data Integration Service Options properties.
7. Enter the staging database name.

   Optionally, click **Select** to select a staging database. You can select an existing database connection. Optionally, click **New** to create another database connection. In the **New Database Connection** dialog box, enter the database connection options, test the connection, and click OK.
8. Optionally, choose to create content if no content exists under the specified database connection string. Default selects the option to not create content.
9. Click **Next**.
10. Optionally, select **Enable Transport Layer Security (TLS)** and enter the TLS protocol properties.
11. Optionally, select **Enable Service** to enable the service after you create it.
12. Click **Finish**.

If you did not choose to enable the service earlier, you must recycle the service to start it.

Related Topics:

- “Properties for the Analyst Service” on page 147

CHAPTER 12

Content Management Service

This chapter includes the following topics:

- Content Management Service Overview, 153
- Content Management Service Architecture, 154
- Recycling and Disabling the Content Management Service, 154
- Content Management Service Properties, 155
- Content Management Service Process Properties, 156
- Creating a Content Management Service, 158

Content Management Service Overview

The Content Management Service is an application service that manages reference data. It provides reference data information to the Data Integration Service and to the Developer tool.

The Content Management Service provides reference data properties to the Data Integration Service. The Content Management Service also provides Developer tool transformations with information about installed reference data. The Content Management Service reads the following types of reference data:

Address reference data

You use address reference data when you create a mapping to validate the postal accuracy of an address or to fix errors or omissions in an address. Use the Address Validator transformation in a mapping to perform address validation.

Identity populations

You use identity population data when you create a mapping to perform duplicate analysis on identity data. An identity is a set of values within a record that collectively identify a person or business. Use a Match transformation or Comparison transformation in a mapping to perform identity duplicate analysis.

You use the Administrator tool to administer the Content Management Service. To update the Data Integration Service with address reference data properties or to provide the Developer tool with information about installed reference data, you must create a Content Management Service in the Informatica domain. Recycle the Content Management Service to start it.

Content Management Service Architecture

You can create one Content Management Service for each node in the domain. You associate each Content Management Service with a Data Integration Service.

You must associate a Content Management Service with each Data Integration Service that runs address validation mappings or identity duplicate analysis mappings. A Data Integration Service cannot be associated with more than one Content Management Service.

The Content Management Service receives requests from the following components:

Data Integration Service

When you update address reference data properties in the Content Management Service, the Content Management Service connects to the Data Integration Service. The Content Management Service writes the properties to the Data Integration Service storage area in the domain repository. The Data Integration Service uses these properties when it runs mappings that require address reference data.

Informatica Developer

When you connect the Developer tool to a domain, it connects to the Content Management Service and caches information about installed reference data files. The Developer tool displays the installed address reference datasets in the Content Status view within application preferences. The Developer tool also displays the installed identity populations in the Match transformation and Comparison transformation.

Recycling and Disabling the Content Management Service

Recycle the Content Management Service to refresh the list of available address reference data. Disable the Content Management Service to restrict users from accessing information about reference data in the Developer tool.

In the Navigator, select the Content Management Service and click the Disable button to stop the service. When you disable the Content Management Service, you must choose the mode to disable it in. You can choose one of the following options:

- Complete. Allows the jobs to run to completion before disabling the service.
- Abort. Tries to stop all jobs before aborting them and disabling the service.

Click the Recycle button to restart the service. The Data Integration Service must be running before you recycle the Content Management Service. You must recycle the Content Management Service after you add address reference data or update existing address reference data. If you update the address validation properties in the service process properties, you must recycle the Content Management service and the associated Data Integration Service.

Note: If you add identity populations or update existing identity populations, users must restart the Developer tool to access the latest identity population details.

Content Management Service Properties

After you create a Content Management Service, you can configure the Content Management Service properties on the Properties tab in the Administrator tool.

You can configure the following types of Content Management Service properties:

- General Properties
- Data Integration Service Property
- Logging Options
- Custom Properties

General Properties

General properties for the Content Management Service include the name and description of the Content Management Service, and the node in the Informatica domain that the Content Management Service runs on. You configure these properties when you create the Content Management Service.

The following table describes the general properties for the Content Management Service:

Property	Description
Name	Name of the Content Management Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the domain repository. The name cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the Content Management Service. The description cannot exceed 765 characters.
Node	Node in the Informatica domain on which the Content Management Service runs. If you change the node, you must recycle the Content Management Service.
License	License assigned to the Content Management Service.

Data Integration Service Property

The Data Integration Service property for the Content Management Service specifies the name of the Data Integration Service. You can configure this property when you create the Content Management Service.

The following table describes the Data Integration Service property for the Content Management Service:

Property	Description
Data Integration Service Name	Data Integration Service name associated with the Content Management Service. You must recycle the Content Management Service if you associate another Data Integration Service with the Content Management Service.

Logging Options

The logging options include properties for the severity level for Content Management Service logs. Valid values are Info, Error, Warning, Trace, Debug, Fatal. Default is Info.

Custom Properties

Custom properties include properties that are unique to your environment or that apply in special cases.

A Content Management Service does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Content Management Service Process Properties

The Content Management Service runs the Content Management Service process on the same node as the service. When you select the Content Management Service in the Administrator tool, you can view the service process for the Content Management Service on the **Processes** tab.

You can view the node properties for the service process on the **Processes** tab. Select the node to view the service process properties.

You can configure the following types of Content Management Service process properties:

- Content Management Service Security Options
- Address Validation Properties
- Custom Properties

Note: The Content Management Service does not currently use the Content Management Service Security Options properties.

Content Management Service Security Options

Reserved for future use.

Address Validation Properties

Configure address validation properties to determine how the Data Integration Service and the Developer tool read address reference data files. After you update address validation properties, you must recycle the Content Management Service and the Data Integration Service.

The following table describes the address validation properties for the Content Management Service process:

Property	Description
License	License key to activate validation reference data. You may have more than one key, for example, if you use general address reference data and Geocoding reference data. Enter keys as a comma-delimited list.
Reference Data Location	Location of the Address Doctor reference data. Enter the full path where you installed the reference data. Install all Address Doctor data to a single location.
Full Pre-Load Countries	List of countries for which all available address reference data will be loaded into memory before address validation begins. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to load all data sets. Load the full reference database to increase performance. Some countries, such as the United States, have large databases that require significant amounts of memory.

Property	Description
Partial Pre-Load Countries	List of countries for which the address reference metadata and indexing structures will be loaded into memory before address validation begins. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to partially load all data sets. Partial preloading increases performance when not enough memory is available to load the complete databases into memory.
No Pre-Load Countries	List of countries for which no address reference data will be loaded into memory before address validation begins. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to load no datasets.
Full Pre-Load Geocoding Countries	List of countries for which all geocoding reference data will be loaded into memory before address validation begins. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to load all data sets. Load all reference data for a country to increase performance when processing addresses from that country. Some countries, such as the United States, have large data sets that require significant amounts of memory.
Partial Pre-Load Geocoding Countries	List of countries for which geocoding metadata and indexing structures will be loaded into memory before address validation begins. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to partially load all data sets.
No Pre-Load Geocoding Countries	List of countries for which no geocoding reference data will be loaded into memory before address validation begins. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to load no datasets.
Full Pre-Load Suggestion List Countries	List of countries for which all reference data will be loaded into memory before address validation begins. Applies when the Address Validator transformation uses Suggestion List mode, which generates a list of valid addresses that are possible matches for an input address. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to load all data sets. Load the full reference database to increase performance. Some countries, such as the United States, have large databases that require significant amounts of memory.
Partial Pre-Load Suggestion List Countries	List of countries for which the address reference metadata and indexing structures will be loaded into memory before address validation begins. Applies when the Address Validator transformation uses Suggestion List mode, which generates a list of valid addresses that are possible matches for an input address. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to partially load all data sets. Partial preloading increases performance when not enough memory is available to load the complete databases into memory.
No Pre-Load Suggestion List Countries	List of countries for which no address reference data will be loaded into memory before address validation begins. Applies when the Address Validator transformation uses Suggestion List mode, which generates a list of valid addresses that are possible matches for an input address. Enter the three-character ISO country codes in a comma-separated list. For example, enter DEU,FRA,USA. Enter ALL to load no datasets.
Memory Usage	Number of megabytes of memory that Address Doctor can allocate. Default is 4096.
Max Address Object count	Maximum number of Address Doctor instances to run at the same time. Default is 3.

Property	Description
Max Thread Count	Maximum number of threads that the Address Doctor can use. Set to the total number of cores or threads available on a machine. Default is 2.
Cache Size	Size of cache for databases that are not preloaded. Caching reserves memory to increase lookup performance in reference data that has not been preloaded. Set the cache size to LARGE unless all the reference data is preloaded or you need to reduce the amount of memory usage. Enter one of the following options for the cache size in uppercase letters: - NONE. No cache. Enter NONE if all reference databases are preloaded. - SMALL. Reduced cache size. - LARGE. Standard cache size. Default is LARGE.

Note: If the Data Integration Service runs mappings that read address reference data, you must enter a value for at least one of the following properties: Full Pre-Load Countries, Partial Pre-Load Countries, No Pre-Load Countries.

Custom Properties for the Content Management Service Process

Custom properties include properties that are unique to your environment or that apply in special cases.

A Content Management Service does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Creating a Content Management Service

Before you create a Content Management Service, verify that a Data Integration Service is present in the domain.

Create a Content Management Service to manage reference data properties and to provide the Developer tool with information about installed reference data.

1. On the Domain tab, select the **Services and Nodes** view.
2. Click **Actions** > **New** > **Content Management Service**.

   The **New Content Management Service** window appears.
3. Enter the general properties for the service and the location for the service.

   Optionally, click **Browse** in the **Location** field to enter the location for the domain and folder where you want to create the service. Optionally, click **Create Folder** to create another folder.
4. Specify a Data Integration Service to associate with the Content Management Service.
5. Click **Next**.
6. Optionally, select **Enable Service** to enable the service after you create it.

   Note: Do not configure the Transport Layer Security properties. These are reserved for future use.
7. Click **Finish**.

If you did not choose to enable the service, you must recycle the service to start it.

CHAPTER 13

Data Integration Service

This chapter includes the following topics:

- Data Integration Service Overview, 159
- Data Integration Service Components, 160
- Data Integration Service Architecture, 163
- Data and File Caching, 163
- Data Integration Service Logs, 164
- Data Integration Service Properties, 164
- Data Integration Service Management, 169
- Creating a Data Integration Service, 175
- Application Management, 176

Data Integration Service Overview

The Data Integration Service is an application service in the Informatica domain that performs data integration tasks for the Analyst tool, the Developer tool, and external clients. When you preview or run mappings, profiles, SQL data services, and web services in Informatica Analyst or Informatica Developer, the application sends requests to the Data Integration Service to perform the data integration tasks. When you start a command from the command line or an external client to run mappings, SQL data services, and web services in an application, the command sends the request to the Data Integration Service.

The Data Integration Service performs the following tasks:

- Runs mappings and generates mapping previews in the Developer tool.
- Runs profiles and generates previews for profiles in the Analyst tool and the Developer tool.
- Runs scorecards for the profiles in the Analyst tool and the Developer tool.
- Runs SQL data services and web services in the Developer tool.
- Runs mappings in a deployed application.
- Caches data objects for mappings and SQL data services deployed in an application.
- Runs SQL queries that end users run against an SQL data service through a third-party JDBC or ODBC client tool.
- Runs web service requests against a web service.

Create and configure a Data Integration Service in the Administrator tool. You can create one or more Data Integration Services on a node. When a Data Integration Service fails, it automatically restarts on the same node.

When you create a Data Integration Service you must associate it with a Model Repository Service. When you create mappings, profiles, SQL data services, and web services, you store them in a Model repository. When you run or preview the mappings, profiles, SQL data services, and web services in the Analyst tool or the Developer tool, the Data Integration Service associated with the Model repository generates the preview data or target data.

When you deploy an application, you must associate it with a Data Integration Service. The Data Integration Service runs the mappings, SQL data services, and web services in the application. The Data Integration Service also writes metadata to the associated Model repository.

During deployment, the Data Integration Service works with the Model Repository Service to create a copy of the metadata required to run the objects in the application. Each application requires its own run time metadata. Data Integration Services do not share run-time metadata even when applications contain the same data objects.

Data Integration Service Components

The Data Integration Service has the following components:

- Data Transformation Manager
- Profiling Service Module
- Mapping Service Module
- SQL Service Module
- Web Service Module
- Data Object Cache Manager
- Result Set Cache Manager
- Deployment Manager
- Monitoring Manager

Data Transformation Manager

The Data Transformation Manager (DTM) is the component in the Data Integration Service that extracts, transforms, and loads data to complete a data transformation process. When a service module in the Data Integration Service receives a request for data transformation, the service module calls the DTM to perform the processes required to complete the request. The service module runs multiple instances of the DTM to complete multiple requests for data transformation. For example, the Mapping Service Module runs a separate instance of the DTM each time it receives a request from the Developer tool to preview a mapping.

The DTM consists of the following components:

- Logical DTM (LDTM). Compiles and optimizes requests for data transformation. The LDTM filters data at the start of the process to reduce the number of rows to be processed and optimize the transformation process.
- Execution DTM (EDTM). Runs the transformation processes.

The LDTM and EDTM work together to extract, transform, and load data to optimally complete the data transformation.

Profiling Service Module

The Profiling Service Module is the component in the Data Integration Service that manages requests to run profiles and generate scorecards.

When you run a profile in the Analyst tool or the Developer tool, the application sends the request to the Data Integration Service. The Profiling Service Module starts a DTM instance to get the profiling rules and run the profile.

When you run a scorecard in the Analyst tool or the Developer tool, the application sends the request to the Data Integration Service. The Profiling Service Module starts a DTM instance to generate a scorecard for the profile.

Mapping Service Module

The Mapping Service Module is the component service in the Data Integration Service that manages requests to preview target data and run mappings.

The following table lists the requests that the Mapping Service Module manages from the different client tools:

Request	Client Tools
Preview target data based on mapping logic.	Developer tool
Run a mapping.	Command line Developer tool Third-party client tools
Run a mapping in a deployed application.	Command line
Run an SQL data service.	Developer tool
Run a web service.	Developer tool

Sample third-party client tools include SQL SQuirreL Client, DBClient, and MySQL ODBC Client.

When you preview or run a mapping, the client tool sends the request and the mapping to the Data Integration Service. The Mapping Service Module starts a DTM instance, which generates the preview data or runs the mapping. If the preview includes a relational or flat file target, the Mapping Service Module writes the preview data to the target.

When you preview data contained in an SQL data service in the Developer tool, the Developer tool sends the request and SQL statement to the Data Integration Service. The Mapping Service Module starts a DTM instance, which runs the SQL statement and generates the preview data.

When you preview a web service operation mapping in the Developer tool, the Developer tool sends the request to the Data Integration Service. The Mapping Service Module starts a DTM instance, which runs the operation mapping and generates the preview data.

Note: To preview relational table data using the Analyst tool or Developer tool, the database client must be installed on the machine on which the Mapping Service Module runs. You must configure the connection to the database in the Analyst tool or Developer tool.

SQL Service Module

The SQL Service Module is the component service in the Data Integration Service that manages SQL queries sent to an SQL data service from a third party client tool.

When the Data Integration Service receives an SQL request from a third party client tool, the SQL Service Module starts a DTM instance to run the SQL query against the virtual tables in the SQL data service.

If you do not cache the data when you deploy an SQL data service, the SQL Service Module starts a DTM instance to run the SQL data service. Every time the third party client tool sends an SQL query to the virtual database, the DTM instance reads data from the source tables instead of cache tables.

Web Service Module

The Web Service Module is a component in the Data Integration Service that manages web service operation requests sent to a web service from a web service client.

When the Data Integration Service receives requests from a web service client, the Web Service Module starts a DTM instance to run the operation mapping. The Web Service Module also sends the operation mapping response to the web service client.

Data Object Cache Manager

When you deploy an application, you can choose to cache the logical data objects and virtual tables in a database. If the application contains an SQL data service, you can cache logical data objects and virtual tables. If the application contains a web service, you can cache logical data objects. The Data Object Cache Manager is the component in the Data Integration Service that caches data for an application.

If you cache data for an application, the Data Object Cache Manager initially caches the data when you enable the SQL data service or the web service. You must specify the database in which to store the data object cache. Optimal performance for the cache depends on the speed and performance of the database.

You can set up a schedule to refresh the cached data. You can also periodically refresh the cache from a command line program or from the Administrator tool.

Result Set Cache Manager

You can temporarily cache the results of a DTM process that runs SQL queries against an SQL data service. The Result Set Cache Manager is the component of the Data Integration Service that manages result set caches.

When you enable result set caching, the Result Set Cache Manager creates in-memory caches to temporarily store the results of a DTM process. If the Result Set Cache Manager requires more space than allocated, it stores the data in cache files. The Result Set Cache Manager caches the results by user for a specified expiration period. When the same user makes the same request before the cache expires, the Result Set Cache Manager returns the cached results. If a cache does not exist or has expired, the Data Integration Service starts a DTM instance to process the request.

The Result Set Cache Manager removes expired result set caches when no space is available in memory or on disk. In addition, the Result Set Cache Manager removes associated result set caches when you restart an application and removes all result set caches when you restart the Data Integration Service.

You configure the result set cache memory size, file directory, and file size in the Data Integration Service process properties. You enable result set caching for a specific SQL data service by setting the cache expiration period in the SQL data service properties.

Deployment Manager

The Deployment Manager is the component in Data Integration Service that manages the applications. When you deploy an application to a Data Integration Service, the Deployment Manager manages the interaction between the Data Integration Service and the Model Repository Service.

The Deployment Manager starts and stops an application. When it starts an application, the Deployment Manager validates the mappings, web service, and SQL data services in the application and their dependent objects.

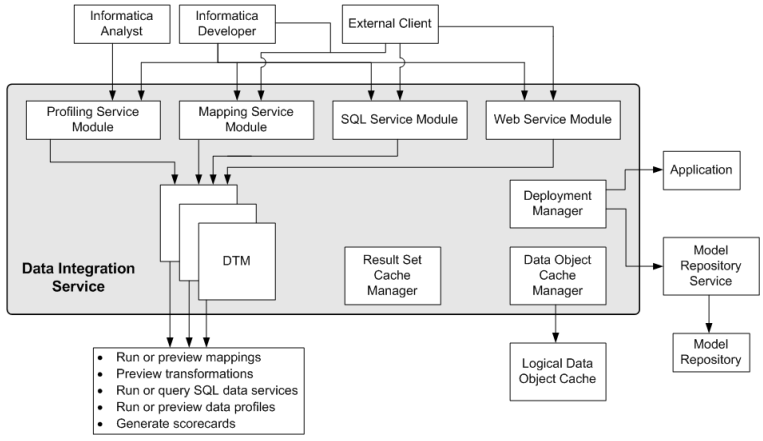
After validation, the Deployment Manager works with the Model Repository Service associated with the Data Integration Service to store the run-time metadata required to run the mappings, web services, and SQL data services in the application. The Deployment Manager creates a separate set of run-time metadata in the Model repository for each application.

When the Data Integration Service runs mappings, web services, and SQL data services in an application, the Deployment Manager retrieves the run-time metadata and makes it available to the DTM.

Data Integration Service Architecture

The Data Integration Service performs the data transformation processes for mappings, profiles, SQL data services, and web services in a Model repository. Each component in the Data Integration Service performs its role to complete the data transformation process. The Mapping Service Module manages the data transformation for mappings. The Profiling Service Module manages the data transformation for profiles. The SQL Service Module manages the data transformation for SQL data services. The Web Service Module manages the data transformations for web services. The Deployment Manager and Data Object Cache Manager manage application deployment and data caching and ensure that the data objects required to complete data transformation are available. The Result Set Cache Manager manages temporary result set caches when SQL queries are run against an SQL data service.

The following diagram shows the architecture of the Data Integration Service:



Requests to the Data Integration Service can come from the Analyst tool, the Developer tool, or an external client. The Analyst tool and the Developer tool send requests to preview or run mappings, profiles, SQL data services, and web services. An external client can send a request to run deployed mappings. An external client can send SQL queries to access data in virtual tables of SQL data services, execute virtual stored procedures, and access metadata. An external client can also send a request to run a web service operation to read, transform, or write data.

When the Deployment Manager deploys an application, the Deployment Manager works with the Model Repository Service to store run-time metadata in the Model repository for the mappings, SQL data services, and web services in the application. If you choose to cache the data for an application, the Deployment Manager caches the data in a relational database.

Data and File Caching

The Data Object Cache Manager and the DTM are the components in the Data Integration Service that perform data and file caching.

The Data Object Cache Manager caches data for applications in the data object cache database. When you refresh the cache, the Data Object Cache Manager updates the data in the data object cache database.

When the DTM runs mappings, it creates data caches to temporarily store data used by the mapping objects. When it processes a large amount of data, the DTM writes the data into cache files. After the Data Integration Service completes the mapping, the DTM releases the data caches and cache files.

Data Integration Service Logs

The Data Integration Service generates operational and error log events that are collected by the Log Manager in the domain. You can view the logs in the log viewer of the Administrator tool.

When the DTM runs, it generates log events for the process that it is running. The DTM bypasses the Log Manager and sends the log events to log files. The DTM stores the log files in the directory specified in the properties for the Data Integration Service process.

Data Integration Service Properties

To view the Data Integration Service properties, select the service in the Domain Navigator and click the Properties view. You can change the properties while the service is running, but you must restart the service for most properties to take effect.

General Properties

The following table describes general properties of a Data Integration Service:

General Property	Description
Name	Name of the Data Integration Service. Read only.
Description	Short description of the Data Integration Service.
License	License key that you enter when you create the service. Read only.
Node	Node where the service runs. Click the Node name to view the Node configuration.

Model Repository Properties

The following table describes the Model repository properties for the Data Integration Service:

Property	Description
Model Repository Service	Service that stores run-time metadata required to run mappings and SQL data services.
User Name	User name to access the Model repository. The user must have the Create Project privilege for the Model Repository Service.

Property	Description
Password	User password to access the Model repository.
Security Domain	LDAP security domain name if you are using LDAP. If you are not using LDAP the domain is native.

Logging Properties

The following table describes the log level properties:

Property	Description
Log Level	Level of error messages that the Data Integration Service writes to the Service log. Choose one of the following message levels: - Fatal. Writes FATAL messages to the log. FATAL messages include nonrecoverable system failures that cause the Data Integration Service to shut down or become unavailable. - Error. Writes FATAL and ERROR code messages to the log. ERROR messages include connection failures, failures to save or retrieve metadata, service errors. - Warning. Writes FATAL, WARNING, and ERROR messages to the log. WARNING errors include recoverable system failures or warnings. - Info. Writes FATAL, INFO, WARNING, and ERROR messages to the log. INFO messages include system and service change messages. - Trace. Write FATAL, TRACE, INFO, WARNING, and ERROR code messages to the log. TRACE messages log user request failures such as SQL request failures, mapping run request failures, and deployment failures. - Debug. Write FATAL, DEBUG, TRACE, INFO, WARNING, and ERROR messages to the log. DEBUG messages are user request logs.

Logical Data Object/Virtual Table Cache Properties

The following table describes the data object and virtual table cache properties:

Property	Description
Cache Removal Time	The amount of milliseconds the Data Integration Service waits before cleaning up cache storage after a refresh. Default is 3,600,000.
Cache Connection	The database connection name for the database that stores the data object cache. Select a valid connection object name.
Maximum Concurrent Refresh Requests	Maximum number of cache refreshes that can occur at the same time. Limit the concurrent cache refreshes to maintain system resources.

Profiling Warehouse Database Properties

The following table describes the profiling warehouse database properties:

Property	Description
Profiling Warehouse Database	The connection to the profiling warehouse. Select the connection object name.
Maximum Ranks	Number of minimum and maximum values to display for a profile. Default is 5.
Maximum Patterns	Maximum number of patterns to display for a profile. Default is 10.
Max Profile Execution Pool Size	Maximum number of threads to run profiling. Default is 10.
Maximum DB Connections	Maximum number of database connections for each profiling job. Default is 5.
Profile Results Export Path	Location where the Data Integration Service exports profile results file. If the Data Integration Service and Analyst Service run on different nodes, both services must be able to access this location. Otherwise, the export fails.

Mapping Service Properties

The following table describes Mapping Service Module properties of a Data Integration Service:

Property	Description
Maximum Notification Thread Pool Size	The maximum number of concurrent job completion notifications that the Mapping Service Module sends to external clients after the Data Integration Service completes jobs. The Mapping Service Module is a component in the Data Integration Service that manages requests sent to run mappings. Default is 5.

Deployment Options

The following table describes the deployment options for the Data Integration Service:

Property	Description
Default Deployment Mode	Determines whether to enable and start each application after you deploy it to a Data Integration Service. Default Deployment mode affects applications that you deploy from the Developer tool, command line, and Administrator tool. Choose one of the following options: - Enable and Start. Enable the application and start the application. - Enable Only. Enable the application but do not start the application. - Disable. Do not enable the application.

Advanced Profiling Properties

The following table describes the advanced profiling properties:

Property	Description
Pattern Threshold	Maximum number of values required to derive a pattern. Default is 5.
Maximum # Value Frequency Pairs	Maximum number of value-frequency pairs to store in the profiling warehouse. Default is 16,000.
Maximum String Length	Maximum length of a string that the Profiling Service can process. Default is 255.
Maximum Numeric Precision	Maximum number of digits for a numeric value. Default is 38.
Maximum Concurrent Profile Jobs	The maximum number of concurrent profile threads used for profiling flat files. If left blank, the Profiling Service plug-in determines the best number based on the set of running jobs and other environment factors.
Profile Job Queue Size	Maximum number of profiling jobs that can wait to run in the Profile Service. Default is 40.
Maximum Concurrent Columns	Maximum number of columns that you can combine for profiling flat files in a single execution pool thread. Default is 5.
Maximum Concurrent Profile Threads	The maximum number of concurrent execution pool threads that can profile flat files. Default is 1.
Maximum Column Heap Size	Amount of memory to allow each column for column profiling. Default is 64 megabytes.
Reserved Profile Threads	Number of threads of the Maximum Execution Pool Size that are for priority requests. Default is 1.

Modules

You can disable some of the Data Integration Service modules.

You might want to disable a module if you are testing and you have limited resources on the computer. You can save memory by limiting the Data Integration functionality.

You can disable the following service modules:

- Core Service. Runs deployments. Do not shut down this module if you need to deploy applications.
- Mapping Service. Runs mappings and previews.
- Profiling Service. Runs profiles and generate scorecards.
- SQL Service. Runs SQL queries from a database client to an SQL data service.
- Web Service. Runs web service operation mappings.

To disable a module, complete the following steps:

1. Disable the Data Integration Service.
2. Select the Data Integration Service in the Navigator.
3. On the Properties tab, click Edit for the Module property.
4. Select False for the module to disable.
5. Click OK.
6. Enable the Data Integration Service.

Pass-through Security Properties

The following table describes the pass-through security properties:

Property	Description
Connection Names	List of connections that allow pass-through security. Configure pass-through security in each Data Integration Service instance that uses the connection.
Allow Caching	Allows data object caching for all pass-through connections in the Data Integration Service. Populates data object cache using the credentials from the connection object. **Note:** When you enable data object caching with pass-through security, you might allow users access to data in the cache database that they might not have in an uncached environment.

HTTP Proxy Server Properties

The following table describes the HTTP proxy server properties:

Property	Description
HTTP Proxy Server Host	Name of the HTTP proxy server.
HTTP Proxy Server Port	Port number of the HTTP proxy server. Default is 8080.
HTTP Proxy Server User	Authenticated user name for the HTTP proxy server. This is required if the proxy server requires authentication.
HTTP Proxy Server Password	Password for the authenticated user. This is required if the proxy server requires authentication.
HTTP Proxy Server Domain	Domain for authentication.

HTTP Configuration Properties

The HTTP configuration properties specify clients that can send web service requests to the Data Integration Service. By default, any client can send requests.

When you configure these properties, the Data Integration Service compares the IP address or host name of clients that submit web service requests against these properties. You can use constants or Java regular expressions as values for these properties. The Data Integration Service either allows the request to continue or refuses to process the request.

For example, to configure the Data Integration Service to accept requests from clients in a local network, enter the following expression in the Allowed IP Addresses:

```
"192.168.1.[0-9]*"
```

The Data Integration Service refuses to process requests from clients with IP addresses that do not match this pattern.

The following table describes the HTTP configuration properties:

Property	Description
Allowed IP Addresses	List of Java regular expression patterns that the requesting client's IP address is compared to. Separate multiple expressions with a white space. If you configure this property, the Data Integration Service accepts requests from IP addresses that match. If you do not configure this property, the Data Integration Service accepts all requests unless the IP address matches a denied pattern.
Allowed Host Names	List of Java regular expression patterns that the requesting client's host name is compared to. Separate multiple expressions with a white space. If you configure this property, the Data Integration Service accepts requests from host names that match. If you do not configure this property, the Data Integration Service accepts all requests unless the host name matches a denied pattern.
Denied IP Addresses	List of Java regular expression patterns that the requesting client's IP address is compared to. Separate multiple expressions with a white space. If you configure this property, the Data Integration Service accepts requests from IP addresses that do not match. If you do not configure this property, the Data Integration Service uses the Allowed IP Addresses property to determine which clients can send requests.
Denied Host Names	List of Java regular expression patterns that the requesting client's host name is compared to. Separate multiple expressions with a white space. If you configure this property, the Data Integration Service accepts requests from host names that do not match. If you do not configure this property, the Data Integration Service uses the Allowed Host Names property to determine which clients can send requests.

Custom Properties

You can edit custom properties for a Data Integration Service.

The following table describes the custom properties:

Property	Description
Custom Property Name	Configure a custom property that is unique to your environment or that you need to apply in special cases. Enter the property name and an initial value. Use custom properties only at the request of Informatica Global Customer Support.

Data Integration Service Management

Create a Data Integration Service in the Administrator tool. After you create the Data Integration Service, you can change the Data Integration Service properties on the Properties view. You can change the Model Repository Service, the level of error messages in the service log, profiling properties, and virtual table cache properties.

Deploy applications to the Data Integration Service on the Applications view. You can start and stop the applications, and enable or disable them to run on startup.

Enabling, Disabling, and Recycling the Data Integration Service

You can enable, disable, or recycle the Data Integration Service from the Administrator tool. You might disable a Data Integration Service if you need to perform maintenance or you need to temporarily restrict users from using

the service. You might recycle a service if you modified a property. When you recycle the service, the Data Integration Service restarts the service.

When you disable a Data Integration Service, you must choose the mode to disable it in. You can choose one of the following options:

- Complete. Allows the jobs to run to completion before disabling the service.
- Abort. Tries to stop all jobs before aborting them and disabling the service.

To enable the service, select the service in the Domain Navigator and click Enable the Service. The Model Repository Service must be running before you enable the Data Integration Service.

To disable the service, select the service in the Domain Navigator and click Disable the Service.

To recycle the service, select the service in the Domain Navigator and click Recycle.

Note: When you enable or disable a service with Microsoft Internet Explorer, the progress bar does not animate unless you enable an advanced option in the browser. Enable Play Animations in Web Pages in the Internet Options Advanced tab.

Pass-through Security

Pass-through security is the capability to connect to an SQL data service or an external source with the client user credentials instead of the credentials from a connection object.

Users might have access to different sets of data based on the job in the organization. Client systems restrict access to databases by the user name and the password. When you create an SQL data service, you might combine data from different systems to create one view of the data. However, when you define the connection to the SQL data service, the connection has one user name and password.

If you configure pass-through security, you can restrict users from some of the data in an SQL data service based on their user name. When a user connects to the SQL data service, the Data Integration Service ignores the user name and the password in the connection object. The user connects with the client user name or the LDAP user name.

A web service operation mapping might need to use a connection object to access data. If you configure pass-through security and the web service uses WS-Security, the web service operation mapping connects to a source using the user name and password provided in the web service SOAP request.

Configure pass-through security for connections in a Data Integration Service. Define the connections that allow pass-through security. You can configure the list in the Administrator tool or with infacmd dis UpdateServiceOptions.

You can set pass-through security for connections to deployed applications. You cannot set pass-through security in the Developer tool.

Do not use a connection that is enabled for pass-through security to access Data Quality Reference tables. A mapping fails when you enable pass-through security for a connection in a Data Quality transformation. The Data Quality mapping does not add the owner name prefix when it accesses the reference tables. The mapping fails with a table not found error.

For more information about configuring security for SQL data services, see the Informatica How-To Library article "How to Configure Security for SQL Data Services": http://communities.informatica.com/docs/DOC-4507.

Example

An organization combines employee data from multiple databases to present a single view of employee data in an SQL data service. The SQL data service contains data from the Employee and Compensation databases. The Employee database contains name, address, and department information. The Compensation database contains salary and stock option information.

A user might have access to the Employee database but not the Compensation database. When the user runs a query against the SQL data service, the Data Integration Service replaces the credentials in each database connection with the user name and the user password. The query fails if the user includes salary information from the Compensation database.

Related Topics:

- " Connection Permissions" on page 117

Pass-through Security with Data Object Caching

To use data object caching with pass-through security, you must enable caching in the pass-through security properties for the Data Integration Service.

When you deploy an SQL data service or a web service, you can choose to cache the logical data objects in a database. You must specify the database in which to store the data object cache. The Data Integration Service validates the user credentials for access to the cache database. If a user can connect to the cache database, the user has access to all tables in the cache. The Data Integration Service does not validate user credentials against the source databases when caching is enabled.

For example, you configure caching for the EmployeeSQLDS SQL data service and enable pass-through security for connections. The Data Integration Service caches tables from the Compensation and the Employee databases. A user might not have access to the Compensation database. However, if the user has access to the cache database, the user can select compensation data in an SQL query.

When you configure pass-through security, the default is to disallow data object caching for data objects that depend on pass-through connections. When you enable data object caching with pass-through security, verify that you do not allow unauthorized users access to some of the data in the cache. When you enable caching for pass-through security connections, you enable data object caching for all pass-through security connections.

Adding Pass-through Security

Select the connections that use pass-through security.

1. In the **Administrator tool**, select the Data Integration Service.
2. Click the **Properties** view.
3. Edit the pass-through security options.

   The **Edit Pass-through Security Options** dialog box appears.
4. Optionally, click **New** to create a connection.
5. To choose pass-through connections, click **Select**. You can select multiple connections at a time.
6. Select **Allow Caching** to allow data object caching for the SQL data services that use the connections.
7. Click OK.

You must recycle the Data Integration Service to enable caching for the connections.

Data Integration Service Processes

View the Data Integration Service process nodes on the Processes tab.

You can edit service process properties such as the HTTP port, logs directory, custom properties, and environment variables. You can also set properties for the Address Manager.

Data Integration Service Security Properties

When you enable the Transport Layer Security (TLS) protocol for the Data Integration Service, web service requests to the Data Integration Service can use the HTTP or HTTPS security protocol.

You can enable the TLS protocol for the Data Integration Service and for each web service. The properties work together in the following ways:

- Enable for the Data Integration Service and disable for the web service. The web service uses HTTP or HTTPS.
- Enable for the Data Integration Service and enable for the web service. The web service must use HTTPS.
- Disable for the Data Integration Service and enable for the web service. The web service will not start.

The following table describes the Data Integration Service Security properties:

Property	Description
HTTP Port	Unique HTTP port number for the Data Integration Service.
HTTPS Port	HTTPS port number for the Data Integration Service when you enable the TLS protocol. Use a different port number than the HTTP port number.

HTTP Configuration Properties for a Process

The HTTP configuration properties for a Data Integration Service process specify the maximum number of HTTP or HTTPS connections that can be made to the process. The properties also specify the keystore and truststore file to use when you enable the Data Integration Service for TLS.

The following table describes the HTTP configuration properties for a Data Integration Service process:

Property	Description
Maximum Concurrent Requests	Maximum number of HTTP or HTTPS connections that can be made to this Data Integration Service process. Default is 200.
Maximum Backlog Requests	Maximum number of HTTP or HTTPS connections that can wait in a queue for this Data Integration Service process. Default is 100.
Keystore File	Path and file name of the keystore file that contains the keys and certificates required if you enable TLS and use the HTTPS protocol for the Data Integration Service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
Keystore Password	Password for the keystore file.
Truststore File	Path and file name of the truststore file that contains authentication certificates trusted by the Data Integration Service.
Truststore Password	Password for the truststore file.
SSL Protocol	Secure Sockets Layer protocol to use.

Result Set Cache Properties

The following table describes the result set cache properties:

Property	Description
Maximum Total Disk Size	Maximum size in megabytes allowed for the total result set cache file storage. Default is 0.
Storage Directory	Absolute path to the directory that stores result set cache files.
File Name Prefix	The string prefix for all result set cache files stored on disk. Default is RSCACHE.
Maximum Per Cache Memory Size	Maximum number of kilobytes allocated for a single result set cache instance in memory. Default is 0.
Maximum Total Memory Size	Maximum number of kilobytes allocated for the total result set cache storage in memory. Default is 0.
Maximum Number of Caches	Maximum number of result set cache instances allowed for this Data Integration Service process. Default is 0.
Enable Encryption	Indicates whether result set cache files are encrypted using 128-bit AES encryption. Valid values are true or false. Default is true.

Advanced Properties

The following table describes the Advanced properties:

Property	Description
Maximum Heap Size	Amount of RAM allocated to the Java Virtual Machine (JVM) that runs the Data Integration Service. Use this property to increase the performance. Append one of the following letters to the value to specify the units: - b for bytes. - k for kilobytes. - m for megabytes. - g for gigabytes. Default is 512 megabytes.
JVM Command Line Options	Java Virtual Machine (JVM) command line options to run Java-based programs. When you configure the JVM options, you must set the Java SDK classpath, Java SDK minimum memory, and Java SDK maximum memory properties.

Logging Options

The following table describes the logging options for the Data Integration Service process:

Property	Description
Logging Directory	Directory for Data Integration Service node process logs. Default is <InformaticaInstallationDir>\tomcat\bin\disLogs.

SQL Properties

The following table describes the SQL properties:

Property	Description
Maximum # of Concurrent Connections	Limits the number of database connections that the Data Integration Service can make for SQL data services. Default is 100.

Execution Options

The following table describes the execution options for the Data Integration Service process:

Property	Description
Maximum Execution Pool Size	The maximum number of requests that the Data Integration Service can run concurrently. Requests include data previews, mappings, profiling jobs, SQL queries, and web service requests. Default is 10.
Temporary Directories	Location of temporary directories for Data Integration Service process on the node. Default is `<Informatica Services Installation Directory>/tomcat/bin/disTemp`. Add a second path to this value to provide a dedicated directory for temporary files created in profile operations. Use a semicolon to separate the paths. Do not use a space after the semicolon.
Maximum Memory Size	The maximum amount of memory, in bytes, that the Data Integration Service can allocate for running requests. If you do not want to limit the amount of memory the Data Integration Service can allocate, set this threshold to 0. When you set this threshold to a value greater than 0, the Data Integration Service uses it to calculate the maximum total memory allowed for running all requests concurrently. The Data Integration Service calculates the maximum total memory as follows: Maximum Memory Size + Maximum Heap Size + memory required for loading program components Default is 512,000,000. **Note:** If you run profiles or data quality mappings, set this threshold to 0.
Maximum Session Size	The maximum amount of memory, in bytes, that the Data Integration Service can allocate for any request. For optimal memory utilization, set this threshold to a value that exceeds the Maximum Memory Size divided by the Maximum Execution Pool Size. The Data Integration Service uses this threshold even if you set Maximum Memory Size to 0 bytes. Default is 50,000,000.

Custom Properties

You can edit custom properties for a Data Integration Service.

The following table describes the custom properties:

Property	Description
Custom Property Name	Configure a custom property that is unique to your environment or that you need to apply in special cases. Enter the property name and an initial value. Use custom properties only at the request of Informatica Global Customer Support.

Environment Variables

You can configure environment variables for the Data Integration Service process.

The following table describes the environment variables:

Property	Description
Environment Variable	Enter a name and a value for the environment variable.

Creating a Data Integration Service

You can create one or more Data Integration Services for a Model Repository Service.

1. On the Domain tab, select the **Services and Nodes** view.
2. Click **Actions** > **New** > **Data Integration Service**.

   The **New Data Integration Service** dialog box appears.
3. Enter the following information:

Property	Description
Name	Name of the Data Integration Service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the Data Integration Service. The description cannot exceed 765 characters.
Location	Domain where the Data Integration Service will run.
License	License key assigned to the Data Integration Service.
Node	Select the Node where the Data Integration Service will run.
HTTP Port	Unique port number for the Data Integration Service. Default is 8095.
Model Repository Service	Model Repository Service that stores run-time metadata required to run the mappings and SQL data services.
Username	User name to access the Model Repository Service.
Repository User Password	User password to access the Model Repository Service.
Repository User Namespace	LDAP security domain namespace for the Model repository User. The namespace field appears when the Informatica domain contains an LDAP security domain.

4. Click **Next**.

   The **New Data Integration Service Step 2** dialog box appears.
5. Optionally, click **Select** to choose a connection for a Profiling Warehouse database.

   The Select Database Connections dialog box appears.

6. Select a connection for the profiling warehouse database.
7. Choose to use an existing profiling warehouse database or to create a new one.
8. Optionally, select a connection for the data object caching database.
9. Click **Next**.

   The **New Data Integration Service Step 3** dialog box appears.
10. Optionally, select **Enable Transport Layer Security (TLS)** and enter the TLS protocol properties.

    When you enable the TLS protocol for the Data Integration Service, web service requests to the Data Integration Service can use the HTTP or HTTPS security protocol.
11. Optionally, select **Enable Service** to enable the service after you create it.

    The Model Repository Service must be running to enable the Data Integration Service.
12. Click **Finish**.

If you did not choose to enable the service, you must recycle the service to start it.

Application Management

A developer can create an SQL data service, web service, or mapping and add it to an application in the Developer tool. To run the application, the developer must deploy it. A developer can deploy an application to an application archive file or deploy the application directly to the Data Integration Service.

As an administrator, you can deploy an application archive file to a Data Integration Service. You can enable the application to run and start the application.

When you deploy an application archive file to a Data Integration Service, the Deployment Manager validates the mappings, web services, and SQL data services in the application. The deployment fails if errors occur. The connections that are defined in the application must be valid in the domain that you deploy the application to.

The Data Integration Service stores the application in the Model repository associated with the Data Integration Service.

You can configure the default deployment mode for a Data Integration Service. The default deployment mode determines the state of each application after deployment. An application is disabled, stopped, or running after deployment.

Application Properties View

The Applications view displays the applications that have been deployed to a Data Integration Service. You can view the objects in the application and the properties. You can start and stop an application, a web service, and an SQL data service in the application. You can also back up and restore an application.

The Applications view shows the applications in alphabetic order. The Application view does not show empty folders. Expand the application name in the top panel to view the SQL data services, web services, mappings, and data objects in the application.

Refresh the Applications view to see the latest applications and their states.

Application State

The Applications view shows the state for each application deployed to the Data Integration Service.

An application can have one of the following states:

- Running. The application is running.
- Stopped. The application is enabled to run but it is not running.
- Disabled. The application is disabled from running. If you recycle the Data Integration Service, the application will not start.
- Failed. The administrator started the application but it failed to start.

General Properties

The Administrator tool shows read-only properties for objects contained in an application. Each general property that is described in this section does not apply to every type of object. For example, the JDBC URL property only applies to an SQL data service object.

The following table describes the general properties:

Property	Description
Name	Name of the selected object. Read only.
Description	Short description of the selected object.
Location	The location of the object. This includes the domain and Data Integration Service name. Read-only.
JDBC URL	JDBC connection string used to access the SQL data service. The SQL data service contains virtual tables that you can query. It also contains virtual stored procedures that you can run. Read only.
WSDL URL	The WSDL URL used to connect to the web service. Read-only.
Last Modification Date	Date the application was last modified. Read only.
Deployment Date	Date the application was deployed. Read only.
Created By	User who created the application. Read only.
Unique Identifier	ID that identifies the application in the Model repository. Read only.
Creation Project Path	Path in the project that contains the application. Read only.
Creation Date	Date the application was created. Read only.
Last Modified By	User who modified the application last. Read only.
Creation Domain	Domain in which the application was created. Read only.
Deployed By	User who deployed the application. Read only.

Application Properties

Configure the whether the application starts when the Data Integration Service starts.

Configure Startup Type to determine whether an application starts when the Data Integration Service starts. When you enable the application, the application starts by default when you start or recycle the Data Integration Service.

Choose Disabled to prevent the application from starting. You cannot manually start an application if it is disabled.

SQL Data Service Properties

Configure the settings the Data Integration Service uses when it runs the SQL data service.

The following table describes the SQL data service properties:

Property	Description
Startup Type	Determines whether the SQL data service is enabled to run when the application starts or when you start the SQL data service. Enter ENABLED to allow the SQL data service to run. Enter DISABLED to prevent the SQL data service from running.
Trace Level	Level of error messages written to the session log. Choose one of the following message levels: - Off - Severe - Warning - Info - Fine - Finest - All Default is INFO.
Connection Timeout	Maximum number of milliseconds to wait for a connection to the SQL data service. Default is 3,600,000.
Request Timeout	Maximum number of milliseconds for an SQL request to wait for an SQL data service response. Default is 3,600,000.
Sort Order	Sort order that the Data Integration Service uses for sorting and comparing data when running in Unicode mode. You can choose the sort order based on your code page. When the Data Integration runs in ASCII mode, it ignores the sort order value and uses a binary sort order. Default is binary.
Maximum Active Connections	Maximum number of active connections to the SQL data service.
Result Set Cache Expiration Period	Amount of time in seconds that the result set cache is available for use. If set to -1, the cache never expires. If set to 0, result set caching is disabled. Default is 0.

Logical Data Object Properties

Configure whether to cache logical data objects and configure how often to refresh the cache.

The following table describes the logical data object properties:

Property	Description
Enable Caching	Cache the logical data object.
Cache Refresh Period (minutes)	Number of milliseconds between cache refreshes.

Virtual Table Properties

Configure whether to cache virtual tables for an SQL data service and configure how often to refresh the cache. You must disable the SQL data service before configuring virtual table properties.

The following table describes the virtual table properties:

Property	Description
Enable Caching	Cache the SQL data service virtual database.
Cache Refresh Period	Number of milliseconds between cache refreshes.

Virtual Column Properties

Configure the properties for the virtual columns included in an SQL data service.

The following table describes the virtual column properties:

Property	Description
Deny With	When you use column level security, this property determines whether to substitute the restricted column value or to fail the query. If you substitute the column value, you can choose to substitute the value with NULL or with a constant value. Select one of the following options: - ERROR. Fails the query and returns an error when an SQL query selects a restricted column. - NULL. Returns a null value for a restricted column in each row. - VALUE. Returns a constant value for a restricted column in each row.
Insufficient Permission Value	The constant that the Data Integration Service returns for a restricted column.

Mapping Properties

Configure the settings the Data Integration Services uses when it runs the mappings in the application.

The following table describes the mapping properties:

Property	Description
Date format	Date/time format the Data Integration Services uses when the mapping converts strings to dates. Default is MM/DD/YYYY HH24:MI:SS.
Enable high precision	Runs the mapping with high precision. High precision data values have greater accuracy. Enable high precision if the mapping produces large numeric values, for example, values with precision of more than 15 digits, and you require accurate values. Enabling high precision prevents precision loss in large numeric values. Default is enabled.
Tracing level	Overrides the tracing level for each transformation in the mapping. The tracing level determines the amount of information the Data Integration Service sends to the mapping log files.

Property	Description
	Choose one of the following tracing levels: - None. The Data Integration Service uses the tracing levels set in the mapping. - Terse. The Data Integration Service logs initialization information, error messages, and notification of rejected data. - Normal. The Data Integration Service logs initialization and status information, errors encountered, and skipped rows due to transformation row errors. It summarizes mapping results, but not at the level of individual rows. - Verbose Initialization. In addition to normal tracing, the Data Integration Service logs additional initialization details, names of index and data files used, and detailed transformation statistics. - Verbose Data. In addition to verbose initialization tracing, the Data Integration Service logs each row that passes into the mapping. The Data Integration Service also notes where it truncates string data to fit the precision of a column and provides detailed transformation statistics. The Data Integration Service writes row data for all rows in a block when it processes a transformation. Default is None.
Optimization level	Controls the optimization methods that the Data Integration Service applies to a mapping as follows: - None. The Data Integration Service does not optimize the mapping. - Minimal. The Data Integration Service applies the early projection optimization method to the mapping. - Normal. The Data Integration Service applies the early projection, early selection, and predicate optimization methods to the mapping. - Full. The Data Integration Service applies the early projection, early selection, predicate optimization, and semi-join optimization methods to the mapping. Default is Normal.
Sort order	Order in which the Data Integration Service sorts character data in the mapping. Default is Binary.

Web Service Properties

Configure the settings that the Data Integration Service uses when it runs a web service.

The following table describes the web service properties:

Property	Description
Startup Type	Determines whether the web service is enabled to run when the application starts or when you start the web service.
Trace Level	Level of error messages written to the run-time web service log. Choose one of the following message levels: - OFF - SEVERE - WARNING - INFO - FINE - FINEST - ALL Default is INFO.
Request Timeout	Maximum number of milliseconds that the Data Integration Service runs an operation mapping before the web service request times out. Default is 3,600,000.

Property	Description
Maximum Concurrent Requests	Maximum number of requests that a web service can process at one time. Default is 10.
Sort Order	Sort order that the Data Integration Service to sort and compare data when running in Unicode mode.
Enable Transport Layer Security	Indicates that the web service must use HTTPS. If the Data Integration Service is not configured to use HTTPS, the web service will not start.
Enable WS-Security	Enables the Data Integration Service to validate the user credentials and verify that the user has permission to run each web service operation.

Web Service Operation Properties

Configure the settings that the Data Integration Service uses when it runs a web service operation.

The following tables describes the web service operation property:

Property	Description
Result Set Cache Expiration Period	Amount of time in milliseconds that the result set cache is available for use. If set to -1, the cache never expires. If set to 0, result set caching is disabled. Default is 0. This property is reserved for future use.

Deploying an Application

Deploy an object to an application archive file if you want to check the application into version control or if your organization requires that administrators deploy objects to Data Integration Services.

1. Click the **Domain** tab.
2. Select a Data Integration Service, and then click the **Applications** view.
3. In Domain Actions, click **Deploy Application from Files**.

   The **Deploy Application** dialog box appears.
4. Click **Upload Files**.

   The **Add Files** dialog box appears.
5. Click **Browse** to search for an application file.
6. Click **Add More Files** if you want to deploy multiple application files.

   You can add up to 10 files.
7. Click **OK** to finish the selection.

   The application file names appear in the **Uploaded Applications Archive Files** panel. The destination Data Integration Service appears as selected in the **Data Integration Services** panel.
8. To select additional Data Integration Services, select them in the **Data Integration Services** panel. To choose all Data Integration Services, select the the box at the top of the list.
9. Click **OK** to start the deployment.

   If no errors are reported, the deployment succeeds and the application starts.

10. If a name conflict occurs, choose one of the following options to resolve the conflict:
    - **Keep the existing application and discard the new application**.
    - **Replace the existing application with the new application**.
    - **Update the existing application with the new application**.
    - **Rename the new application**. Enter the new application name if you select this option.

    If you replace or update the existing application and the existing application is running, select the **Force Stop the Existing Application if it is Running** option to stop the existing application. You cannot update or replace an existing application that is running.

    After you select an option, click **OK**.
11. Click **Close**.

You can also deploy an application file using the infacmd dis deployApplication program.

Enabling an Application

An application must be enabled to run before you can start it. When you enable a Data Integration Service, the enabled applications start automatically.

You can configure a default deployment mode for a Data Integration Service. When you deploy an application to a Data Integration Service, the property determines the application state after deployment. An application might be enabled or disabled. If an application is disabled, you can enable it manually. If the application is enabled after deployment, the SQL data services and web services are also enabled.

1. Select the Data Integration Service in the Navigator.
2. Click the Applications view.
3. Select the application in the Content panel.
4. Click the Properties View in the Detail Panel.
5. Scroll to the Applications property and click Edit.
6. Choose enabled.

   The application is enabled to run. You must enable each SQL data service that you want to run.

Renaming an Application

Rename an application to change the name. You can rename an application when the application is not running.

1. Select the Data Integration Service in the Navigator.
2. In the **Application** view, select the application that you want to rename.
3. Click **Actions** > **Rename Application**.
4. Enter the name and click **OK**.

Enabling an SQL Data Service

Before you can start an SQL data service, the Data Integration Service must be running and the SQL data service must be enabled.

When an deployed application is enabled by default, the SQL data services in the application are also enabled.

When a deployed application is disabled by default, the SQL data services are also disabled. When you enable the application manually, you must also enable each SQL data service in the application.

1. In the Applications view, select the SQL data service that you want to enable.
2. In the content panel, click Startup type.
3. Enter ENABLED.

Renaming an SQL Data Service

Rename an SQL data service to change the name of the SQL data service. You can rename an SQL data service when the SQL data service is not running.

1. Select the Data Integration Service in the Navigator.
2. In the **Application** view, select the SQL data service that you want to rename.
3. Click **Actions** > **Rename SQL Data Service**.
4. Enter the name and click **OK**.

Enabling a Web Service

Enable a web service so that you can start the web service. Before you can start a web service, the Data Integration Service must be running and the web service must be enabled.

1. Select the Data Integration Service in the Navigator.
2. In the **Application** view, select the web service that you want to enable.
3. In **Web Service Properties** section of the **Properties** view, click **Edit**.

   The **Edit Properties** dialog box appears.
4. In the **Startup Type** field, select **Enabled** and click **OK**.

Renaming a Web Service

Rename a web service to change the service name of a web service. You can rename a web service when the web service is stopped.

1. Select the Data Integration Service in the Navigator.
2. In the **Application** view, select the web service that you want to rename.
3. Click **Actions** > **Rename Web Service**.

   The **Rename Web Service** dialog box appears.
4. Enter the web service name and click **OK**.

Downloading the WSDL of a Web Service

You can download the WSDL of a web service to save the WSDL to a file.

1. Select the Data Integration Service in the Navigator.
2. In the **Application** view, select the web service.
3. Click **Actions** > **Get WSDL**.
4. Save the WSDL to an XML file.

You can change the filename extension from .xml to .WSDL.

Starting an Application

You can start an application from the Administrator tool.

An application must be running before you can access an SQL data service in the application. You can start the application from the Applications Actions menu if the application is enabled to run.

1. Select the Data Integration Service in the Navigator.
2. Click the Applications view.
3. Select the application in the Content Panel.
4. Click Actions > Start Application.

Backing Up an Application

You can back up an application to an XML file. The backup file contains all the properties settings for the application. You can restore the application to another Data Integration Service.

You must stop the application before you back it up.

1. In the Applications view, select the application to back up.
2. Click Application Actions > Backup.

   The Administrator tool prompts you to open the XML file or save the XML file.
3. Click Open to view the XML file in a browser.
4. Click Save to save the XML file.
5. If you click Save, enter an XML file name and choose the location to back up the application.

   The Administrator Tool backs up the application to an XML file in the location you choose.

Restoring an Application

You can restore an application from an XML backup file. The application must be an XML backup file that you create with the Backup option.

1. In the Domain Navigator, select a Data Integration Service that you want to restore the application to.
2. Click the Applications view.
3. Click Applications Actions > Restore from file.

   The Administrator tool prompts you for the file to restore.
4. Browse for and select the XML file.
5. Click OK to start the restore.

   The Administrator tool checks for a duplicate application.
6. If a conflict occurs, choose one of the following options:
   - Keep the existing application and discard the new application. The Administrator tool does not restore the file.
   - Replace the existing application with the new application. The Administrator tool restores the backup application to the Data Integration Service.
   - Rename the new application. Choose a different name for the application you are restoring.
7. Click OK to restore the application.

   The application starts if the default deployment option is set to Enable and Start for the Data Integration Service.

Refreshing the Applications View

Refresh the Applications view to view newly deployed and restored applications, remove applications that were recently undeployed, and update the state of each application.

1. Select the Data Integration Service in the Navigator.
2. Click the **Applications** view.
3. Select the application in the **Content** panel.
4. Click **Refresh Application View** in the application Actions menu.

   The **Application** view refreshes.

CHAPTER 14

Metadata Manager Service

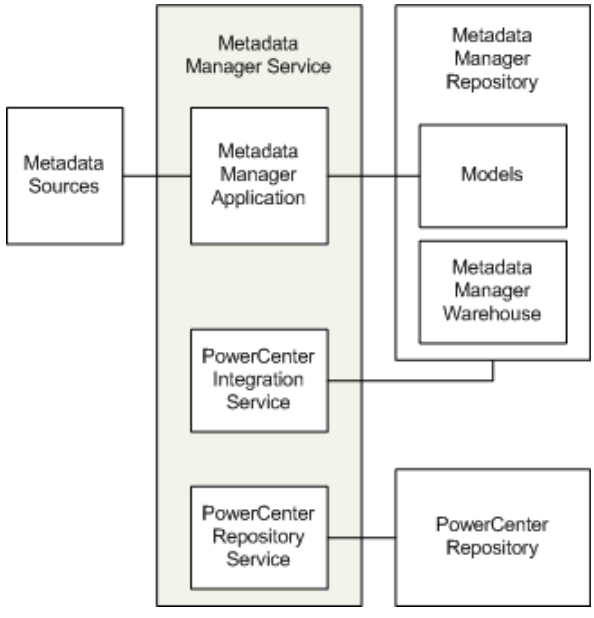
This chapter includes the following topics:

- Metadata Manager Service Overview, 186
- Configuring a Metadata Manager Service, 187
- Creating a Metadata Manager Service, 188
- Creating and Deleting Repository Content, 190
- Enabling and Disabling the Metadata Manager Service, 192
- Configuring the Metadata Manager Service Properties, 192
- Configuring the Associated PowerCenter Integration Service, 198

Metadata Manager Service Overview

The Metadata Manager Service is an application service that runs the Metadata Manager application in an Informatica domain. The Metadata Manager application manages access to metadata in the Metadata Manager repository. Create a Metadata Manager Service in the domain to access the Metadata Manager application.

The following figure shows the Metadata Manager components managed by the Metadata Manager Service on a node in an Informatica domain:



The Metadata Manager Service manages the following components:

- Metadata Manager application. The Metadata Manager application is a web-based application. Use Metadata Manager to browse and analyze metadata from disparate source repositories. You can load, browse, and analyze metadata from application, business intelligence, data integration, data modeling, and relational metadata sources.
- PowerCenter repository for Metadata Manager. Contains the metadata objects used by the PowerCenter Integration Service to load metadata into the Metadata Manager warehouse. The metadata objects include sources, targets, sessions, and workflows.
- PowerCenter Repository Service. Manages connections to the PowerCenter repository for Metadata Manager.
- PowerCenter Integration Service. Runs the workflows in the PowerCenter repository to read from metadata sources and load metadata into the Metadata Manager warehouse.
- Metadata Manager repository. Contains the Metadata Manager warehouse and models. The Metadata Manager warehouse is a centralized metadata warehouse that stores the metadata from metadata sources. Models define the metadata that Metadata Manager extracts from metadata sources.
- Metadata sources. The application, business intelligence, data integration, data modeling, and database management sources that Metadata Manager extracts metadata from.

Configuring a Metadata Manager Service

You can create and configure a Metadata Manager Service and the related components in the Administrator tool.

1. Set up the Metadata Manager repository database. Set up a database for the Metadata Manager repository. You supply the database information when you create the Metadata Manager Service.
2. Create a PowerCenter Repository Service and PowerCenter Integration Service (Optional). You can use an existing PowerCenter Repository Service and PowerCenter Integration Service, or you can create them. If want to create the application services to use with Metadata Manager, create the services in the following order:
   - PowerCenter Repository Service. Create a PowerCenter Repository Service but do not create contents. Start the PowerCenter Repository Service in exclusive mode.
   - PowerCenter Integration Service. Create the PowerCenter Integration Service. The service will not start because the PowerCenter Repository Service does not have content. You enable the PowerCenter Integration Service after you create and configure the Metadata Manager Service.
3. Create the Metadata Manager Service. Use the Administrator tool to create the Metadata Manager Service.
4. Configure the Metadata Manager Service. Configure the properties for the Metadata Manager Service.
5. Create repository contents. Create contents for the Metadata Manager repository and restore the PowerCenter repository. Use the Metadata Manager Service Actions menu to create the contents for both repositories.
6. Enable the PowerCenter Integration Service. Enable the associated PowerCenter Integration Service for the Metadata Manager Service.
7. Create a Reporting Service (Optional). To run reports on the Metadata Manager repository, create a Reporting Service. After you create the Reporting Service, you can log in to Data Analyzer and run reports against the Metadata Manager repository.
8. Enable the Metadata Manager Service. Enable the Metadata Manager Service in the Informatica domain.
9. Create or assign users. Create users and assign them privileges for the Metadata Manager Service, or assign existing users privileges for the Metadata Manager Service.

Note: You can use a Metadata Manager Service and the associated Metadata Manager repository in one Informatica domain. After you create the Metadata Manager Service and Metadata Manager repository in one domain, you cannot create a second Metadata Manager Service to use the same Metadata Manager repository. You also cannot back up and restore the repository to use with a different Metadata Manager Service in a different domain.

Creating a Metadata Manager Service

Use the Administrator tool to create the Metadata Manager Service. After you create the Metadata Manager Service, create the Metadata Manager repository contents and PowerCenter repository contents to enable the service.

1. In the Administrator tool, click the **Domain** tab.
2. Click **Actions** > **New Metadata Manager Service**.

   The **New Metadata Manager Service** dialog box appears.
3. Enter values for the Metadata Manager Service general properties, and click **Next**.
4. Enter values for the Metadata Manager Service database properties, and click **Next**.
5. Enter values for the Metadata Manager Service security properties, and click **Finish**.

Metadata Manager Service Properties

The following table describes the properties that you configure for the Metadata Manager Service:

Property	Description
Name	Name of the Metadata Manager Service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the Metadata Manager Service after you create it.
License	License object that allows use of the service. To apply changes, restart the Metadata Manager Service.
Node	Node in the Informatica domain that the Metadata Manager Service runs on.
Associated Integration Service	PowerCenter Integration Service used by Metadata Manage to load metadata into the Metadata Manager warehouse.
Repository User Name	User account for the PowerCenter repository. Use the repository user account you configured for the PowerCenter Repository Service. For a list of the required privileges for this user, see “Privileges for the Associated PowerCenter Integration Service User.”on page 198
Repository Password	Password for the PowerCenter repository user.

Property	Description
Security Domain	Security domain that contains the user account you configured for the PowerCenter Repository Service.
Database Type	Type of database for the Metadata Manager repository. To apply changes, restart the Metadata Manager Service.
Code Page	Metadata Manager repository code page. The Metadata Manager Service and Metadata Manager application use the character set encoded in the repository code page when writing data to the Metadata Manager repository. **Note:** The Metadata Manager repository code page, the code page on the machine where the associated PowerCenter Integration Service runs, and the code page for any database management and PowerCenter resources that you load into the Metadata Manager warehouse must be the same.
Connect String	Native connect string to the Metadata Manager repository database. The Metadata Manager Service uses the connect string to create a connection object to the Metadata Manager repository in the PowerCenter repository. To apply changes, restart the Metadata Manager Service.
Database User	User account for the Metadata Manager repository database. Set up this account using the appropriate database client tools. To apply changes, restart the Metadata Manager Service.
Database Password	Password for the Metadata Manager repository database user. Must be in 7-bit ASCII. To apply changes, restart the Metadata Manager Service.
Tablespace Name	Tablespace name for Metadata Manager repositories on IBM DB2. When you specify the tablespace name, the Metadata Manager Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node. To apply changes, restart the Metadata Manager Service.
Database Hostname	Host name for the Metadata Manager repository database.
Database Port	Port number for the Metadata Manager repository database.
SID/Service Name	Indicates whether the Database Name property contains an Oracle full service name or SID.
Database Name	Full service name or SID for Oracle databases. Service name for IBM DB2 databases. Database name for Microsoft SQL Server databases.

Additional JDBC Parameters	Additional JDBC options.
	To authenticate the user credentials using Windows authentication and establish a trusted connection to a Microsoft SQL Server repository, enter the following text:
	`AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll].`
	`jdbc:informatica:sqlserver://[host]:[port];DatabaseName=[DB name];AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]`
	When you use a trusted connection to connect to a Microsoft SQL Server database, the Metadata Manager Service connects to the repository with the credentials of the user logged in to the machine on which the service is running.
	To start the Metadata Manager Service as a Windows service using a trusted connection, configure the Windows service properties to log on using a trusted user account.

Port Number	Port number the Metadata Manager application runs on. Default is 10250. If you configure HTTPS, verify that the port number one less than the HTTPS port is also available. For example, if you configure 10255 for the HTTPS port number, you must verify that 10254 is also available. Metadata Manager uses port 10254 for HTTP.

Property	Description
Enable Secured Socket Layer	Indicates that you want to configure SSL security protocol for the Metadata Manager application.
Keystore File	Keystore file that contains the keys and certificates required if you use the SSL security protocol with the Metadata Manager application. Required if you select Enable Secured Socket Layer.
Keystore Password	Password for the keystore file. Required if you select Enable Secured Socket Layer.

Database Connect Strings

When you create a database connection, specify a connect string for that connection. The Metadata Manager Service uses the connect string to create a connection object to the Metadata Manager repository database in the PowerCenter repository.

The following table lists the native connect string syntax for each supported database:

Database	Connect String Syntax	Example
IBM DB2	*dbname*	mydatabase
Microsoft SQL Server	*servername*@*dbname*	sqlserver@mydatabase
Oracle	*dbname*.world (same as TNSNAMES entry)	oracle.world

Overriding the Repository Database Code Page

You can override the default database code page for the Metadata Manager repository database when you create or configure the Metadata Manager Service. Override the code page if the Metadata Manager repository contains characters that the database code page does not support.

To override the code page, add the CODEPAGEOVERRIDE parameter to the Additional JDBC Options property. Specify a code page that is compatible with the default repository database code page.

For example, use the following parameter to override the default Shift-JIS code page with MS932:

```
CODEPAGEOVERRIDE=MS932;
```

Creating and Deleting Repository Content

You can create and delete contents for the following repositories used by Metadata Manager:

- Metadata Manager repository. Create the Metadata Manager warehouse tables and import models for metadata sources into the Metadata Manager repository.

- PowerCenter repository. Restore a repository backup file packaged with PowerCenter to the PowerCenter repository database. The repository backup file includes the metadata objects used by Metadata Manager to load metadata into the Metadata Manager warehouse. When you restore the repository, the Service Manager creates a folder named Metadata Load in the PowerCenter repository. The Metadata Load folder contains the metadata objects, including sources, targets, sessions, and workflows.

The tasks you complete depend on whether the Metadata Manager repository contains contents or if the PowerCenter repository contains the PowerCenter objects for Metadata Manager.

The following table describes the tasks you must complete for each repository:

Repository	Condition	Action
Metadata Manager repository	Does not have content.	Create the Metadata Manager repository.
	Has content.	No action.
PowerCenter repository	Does not have content.	Restore the PowerCenter repository if the PowerCenter Repository Service runs in exclusive mode.
	Has content.	No action if the PowerCenter repository has the objects required for Metadata Manager in the Metadata Load folder. The Service Manager imports the required objects from an XML file when you enable the service.

Creating the Metadata Manager Repository

When you create the Metadata Manager repository, you create the Metadata Manager warehouse tables and import models for metadata sources.

1. In the Navigator, select the Metadata Manager Service for which the Metadata Manager repository has no content.
2. Click **Actions** > **Repository Contents** > **Create**.
3. Optionally, choose to restore the PowerCenter repository. You can restore the repository if the PowerCenter Repository Service runs in exclusive mode and the repository does not contain contents.
4. Click **OK**.

   The activity log displays the results of the create contents operation.

Restoring the PowerCenter Repository

Restore the repository backup file for the PowerCenter repository to create the objects used by Metadata Manager in the PowerCenter repository database.

1. In the Navigator, select the Metadata Manager Service for which the PowerCenter repository has no contents.
2. Click **Actions** > **Restore PowerCenter Repository**.
3. Optionally, choose to restart the PowerCenter Repository Service in normal mode.
4. Click **OK**.

   The activity log displays the results of the restore repository operation.

Deleting the Metadata Manager Repository

Delete Metadata Manager repository content when you want to delete all metadata and repository database tables from the repository. Delete the repository content if the metadata is obsolete. If the repository contains information that you want to save, back up the repository before you delete it. Use the database client or the Metadata Manager repository backup utility to back up the database before you delete contents.

1. In the Navigator, select the Metadata Manager Service for which you want to delete Metadata Manager repository content.
2. Click **Actions** > **Repository Contents** > **Delete**.
3. Enter the user name and password for the database account.
4. Click **OK**.

   The activity log displays the results of the delete contents operation.

Enabling and Disabling the Metadata Manager Service

Use the Administrator tool to enable, disable, or recycle the Metadata Manager Service. Disable a Metadata Manager Service to perform maintenance or to temporarily restrict users from accessing Metadata Manager. When you disable the Metadata Manager Service, you also stop Metadata Manager. You might recycle a service if you modified a property. When you recycle the service, the Metadata Manager Service is disabled and enabled.

When you enable the Metadata Manager Service, the Service Manager starts the Metadata Manager application on the node where the Metadata Manager Service runs. If the PowerCenter repository does not contain the Metadata Load folder, the Administrator tool imports the metadata objects required by Metadata Manager into the PowerCenter repository.

You can enable, disable, and recycle the Metadata Manager Service from the **Actions** menu.

Note: The PowerCenter Repository Service for Metadata Manager must be enabled and running before you can enable the Metadata Manager Service.

Configuring the Metadata Manager Service Properties

After you create a Metadata Manager Service, you can configure it. After you configure Metadata Manager Service properties, you must disable and enable the Metadata Manager Service for the changes to take effect.

Use the Administrator tool to configure the following types of Metadata Manager Service properties:

- General properties. Include the name and description of the service, the license object for the service, and the node where the service runs.
- Metadata Manager Service properties. Include port numbers for the Metadata Manager application and the Metadata Manager Agent, and the Metadata Manager file location.
- Database properties. Include database properties for the Metadata Manager repository.
- Configuration properties. Include the HTTP security protocol and keystore file, and maximum concurrent and queued requests to the Metadata Manager application.
- Connection pool properties. Metadata Manager maintains a connection pool for connections to the Metadata Manager repository. Connection pool properties include the number of active available connections to the

Metadata Manager repository database and the amount of time that Metadata Manager holds database connection requests in the connection pool.

- Advanced properties. Include properties for the Java Virtual Manager (JVM) memory settings, ODBC connection mode, and Metadata Manager Browse and Load tab options.
- Custom properties. Configure repository properties that are unique to your environment or that apply in special cases. A Metadata Manager Service does not have custom properties when you initially create it. Use custom properties if Informatica Global Customer Support instructs you to do so.

To view or update properties:

- Select the Metadata Manager Service in the Navigator.

General Properties

To edit the general properties, select the Metadata Manager Service in the Navigator, select the **Properties** view, and then click **Edit** in the General Properties section.

The following table describes the general properties for a Metadata Manager Service:

Property	Description
Name	Name of the Metadata Manager Service. You cannot edit this property.
Description	Description of the Metadata Manager Service.
License	License object you assigned the Metadata Manager Service to when you created the service. You cannot edit this property.
Node	Node in the Informatica domain that the Metadata Manager Service runs on. To assign the Metadata Manager Service to a different node, you must first disable the service.

Assigning the Metadata Manager Service to a Different Node

1. Disable the Metadata Manager Service.
2. Click Edit in the General Properties section.
3. Select another node for the Node property, and then click OK.
4. Click Edit in the Metadata Manager Service Properties section.
5. Change the Metadata Manager File Location property to a location that is accessible from the new node, and then click OK.
6. Copy the contents of the Metadata Manager file location directory on the original node to the location on the new node.
7. If the Metadata Manager Service is running in HTTPS security mode, click Edit in the Configuration Properties section. Change the Keystore File location to a location that is accessible from the new node, and then click OK.
8. Enable the Metadata Manager Service.

Metadata Manager Service Properties

To edit the Metadata Manager Service properties, select the Metadata Manager Service in the Navigator, select the **Properties** view, and then click **Edit** in the Metadata Manager Service Properties section.

The following table describes the Metadata Manager Service properties:

Property	Description
Port Number	Port number that the Metadata Manager application runs on. Default is 10250. If you configure HTTPS, make sure that the port number one less than the HTTPS port is also available. For example, if you configure 10255 for the HTTPS port number, you must make sure 10254 is also available. Metadata Manager uses port 10254 for HTTP.
Agent Port	Port number for the Metadata Manager Agent. The agent uses this port to communicate with metadata source repositories. Default is 10251.
Metadata Manager File Location	Location of the files used by the Metadata Manager application. Files include the following file types: - Index files. Index files created by Metadata Manager required to search the Metadata Manager warehouse. - Parameter files. Files generated by Metadata Manager and used by PowerCenter workflows. - Log files. Log files generated by Metadata Manager when you load resources. By default, Metadata Manager stores the files in the following directory: <Informatica installation directory>\server\tomcat\mm_files\<service name>

Configuring the Metadata Manager File Location

Use the following rules and guidelines when you configure the Metadata Manager file location:

- If you change this location, copy the contents of the directory to the new location.
- If you configure a shared file location, the location must be accessible to all nodes running a Metadata Manager Service and to all users of the Metadata Manager application.

Database Properties

To edit the Metadata Manager repository database properties, select the Metadata Manager Service in the Navigator, select the **Properties** view, and then click **Edit** in the Database Properties section.

The following table describes the database properties for a Metadata Manager repository database:

Property	Description
Database Type	Type of database for the Metadata Manager repository. To apply changes, restart the Metadata Manager Service.
Code Page	Metadata Manager repository code page. The Metadata Manager Service and Metadata Manager use the character set encoded in the repository code page when writing data to the Metadata Manager repository. To apply changes, restart the Metadata Manager Service. **Note:** The Metadata Manager repository code page, the code page on the machine where the associated PowerCenter Integration Service runs, and the code page for any database management and PowerCenter resources you load into the Metadata Manager warehouse must be the same.
Connect String	Native connect string to the Metadata Manager repository database. The Metadata Manager Service uses the connection string to create a target connection to the Metadata Manager repository in the PowerCenter repository. To apply changes, restart the Metadata Manager Service. **Note:** If you set the ODBC Connection Mode property to True, use the ODBC connection name for the connect string.

Property	Description
Database User	User account for the Metadata Manager repository database. Set up this account using the appropriate database client tools. To apply changes, restart the Metadata Manager Service.
Database Password	Password for the Metadata Manager repository database user. Must be in 7-bit ASCII. To apply changes, restart the Metadata Manager Service.
Tablespace Name	Tablespace name for the Metadata Manager repository on IBM DB2. When you specify the tablespace name, the Metadata Manager Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name. To apply changes, restart the Metadata Manager Service. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node.
Database Hostname	Host name for the Metadata Manager repository database. To apply changes, restart the Metadata Manager Service.
Database Port	Port number for the Metadata Manager repository database. To apply changes, restart the Metadata Manager Service.
SID/Service Name	Indicates whether the Database Name property contains an Oracle full service name or an SID.
Database Name	Full service name or SID for Oracle databases. Service name for IBM DB2 databases. Database name for Microsoft SQL Server databases. To apply changes, restart the Metadata Manager Service.
Additional JDBC Parameters	Additional JDBC options. For example, you can use this option to specify the location of a backup server if you are using a database server that is highly available such as Oracle RAC.

Configuration Properties

To edit the configuration properties, select the Metadata Manager Service in the Navigator, select the **Properties** view, and then click **Edit** in the Configuration Properties section.

The following table describes the configuration properties for a Metadata Manager Service:

Property	Description
URLScheme	Indicates the security protocol that you configure for the Metadata Manager application: HTTP or HTTPS.
Keystore File	Keystore file that contains the keys and certificates required if you use the SSL security protocol with the Metadata Manager application. You must use the same security protocol for the Metadata Manager Agent if you install it on another machine.
Keystore Password	Password for the keystore file.
MaxConcurrentRequests	Maximum number of request processing threads available, which determines the maximum number of client requests that Metadata Manager can handle simultaneously. Default is 100.
MaxQueueLength	Maximum queue length for incoming connection requests when all possible request processing threads are in use by the Metadata Manager application. Metadata Manager refuses client requests when the queue is full. Default is 500.

You can use the MaxConcurrentRequests property to set the number of clients that can connect to Metadata Manager. You can use the MaxQueueLength property to set the number of client requests Metadata Manager can process at one time.

You can change the parameter values based on the number of clients that you expect to connect to Metadata Manager. For example, you can use smaller values in a test environment. In a production environment, you can increase the values. If you increase the values, more clients can connect to Metadata Manager, but the connections might use more system resources.

Connection Pool Properties

To edit the connection pool properties, select the Metadata Manager Service in the Navigator, select the **Properties** view, and then click **Edit** in the Connection Pool Properties section.

The following table describes the connection pool properties for a Metadata Manager Service:

Property	Description
Maximum Active Connections	Number of active connections to the Metadata Manager repository database available. The Metadata Manager application maintains a connection pool for connections to the repository database. Default is 20.
Maximum Wait Time	Amount of time in seconds that Metadata Manager holds database connection requests in the connection pool. If Metadata Manager cannot process the connection request to the repository within the wait time, the connection fails. Default is 180.

Advanced Properties

To edit the advanced properties, select the Metadata Manager Service in the Navigator, select the **Properties** view, and then click **Edit** in the Advanced Properties section.

The following table describes the advanced properties for a Metadata Manager Service:

Property	Description
Max Heap Size	Amount of RAM in megabytes allocated to the Java Virtual Manager (JVM) that runs Metadata Manager. Use this property to increase the performance of Metadata Manager. For example, you can use this value to increase the performance of Metadata Manager during indexing. Default is 1024.
Maximum Catalog Child Objects	Number of child objects that appear in the Metadata Manager metadata catalog for any parent object. The child objects can include folders, logical groups, and metadata objects. Use this option to limit the number of child objects that appear in the metadata catalog for any parent object. Default is 100.
Error Severity Level	Level of error messages written to the Metadata Manager Service log. Specify one of the following message levels: - Fatal - Error - Warning - Info - Trace - Debug

Property	Description
	When you specify a severity level, the log includes all errors at that level and above. For example, if the severity level is Warning, the log includes fatal, error, and warning messages. Use Trace or Debug if Informatica Global Customer Support instructs you to use that logging level for troubleshooting purposes. Default is Error.
Max Concurrent Resource Load	Maximum number of resources that Metadata Manager can load simultaneously. Maximum is 5. Metadata Manager adds resource loads to the load queue in the order that you request the loads. If you simultaneously load more than the maximum, Metadata Manager adds the resource loads to the load queue in a random order. For example, you set the property to 5 and schedule eight resource loads to run at the same time. Metadata Manager adds the eight loads to the load queue in a random order. Metadata Manager simultaneously processes the first five resource loads in the queue. The last three resource loads wait in the load queue. If a resource load succeeds, fails and cannot be resumed, or fails during the path building task and can be resumed, Metadata Manager removes the resource load from the queue. Metadata Manager starts processing the next load waiting in the queue. If a resource load fails when the PowerCenter Integration Service runs the workflows and the workflows can be resumed, the resource load is resumable. Metadata Manager keeps the resumable load in the load queue until the timeout interval is exceeded or until you resume the failed load. Metadata Manager includes a resumable load due to a failure during workflow processing in the concurrent load count. Default is 3.
Timeout Interval	Amount of time in minutes that Metadata Manager holds a resumable resource load in the load queue. You can resume a resource load within the timeout period if the load fails when PowerCenter runs the workflows and the workflows can be resumed. If you do not resume a failed load within the timeout period, Metadata Manager removes the resource from the load queue. Default is 30. **Note:** If a resource load fails during the path building task, you can resume the failed load at any time.
ODBC Connection Mode	Connection mode that the PowerCenter Integration Service uses to connect to metadata sources and the Metadata Manager repository when loading resources. You can select one of the following options: - True. The PowerCenter Integration Service uses ODBC. - False. The PowerCenter Integration Service uses native connectivity. You must set this property to True if the PowerCenter Integration Service runs on a UNIX machine and you want to extract metadata from or load metadata to a Microsoft SQL Server database or if you use a Microsoft SQL Server database for the Metadata Manager repository.

Custom Properties

The following table describes the custom properties:

Property	Description
Custom Property Name	Configure a custom property that is unique to your environment or that you need to apply in special cases. Enter the property name and an initial value. Use custom properties only if Informatica Global Customer Support instructs you to do so.

Configuring the Associated PowerCenter Integration Service

You can configure or remove the PowerCenter Integration Service that Metadata Manager uses to load metadata into the Metadata Manager warehouse. If you remove the PowerCenter Integration Service, configure another PowerCenter Integration Service to enable the Metadata Manager Service.

To edit the associated PowerCenter Integration Service properties, select the Metadata Manager Service in the Navigator, select the **Associated Services** view, and click **Edit**. To apply changes, restart the Metadata Manager Service.

The following table describes the associated PowerCenter Integration Service properties:

Property	Description
Associated Integration Service	Name of the PowerCenter Integration Service that you want to use with Metadata Manager.
Repository User Name	Name of the PowerCenter repository user that has the required privileges.
Repository Password	Password for the PowerCenter repository user.
Security Domain	Security domain for the PowerCenter repository user. The Security Domain field appears when the Informatica domain contains an LDAP security domain.

Privileges for the Associated PowerCenter Integration Service User

The PowerCenter repository user for the associated PowerCenter Integration Service must be able to perform the following tasks:

- Restore the PowerCenter repository.
- Import and export PowerCenter repository objects.
- Create, edit, and delete connection objects in the PowerCenter repository.
- Create folders in the PowerCenter repository.
- Load metadata into the Metadata Manager warehouse.

To perform these tasks, the user must have the required privileges and permissions for the domain, PowerCenter Repository Service, and Metadata Manager Service.

The following table lists the required privileges and permissions that the PowerCenter repository user for the associated PowerCenter Integration Service must have:

Service	Privileges	Permissions
Domain	- Access Informatica Administrator - Manage Services	Permission on PowerCenter Repository Service
PowerCenter Repository Service	- Access Repository Manager - Create Folders - Create, Edit, and Delete Design Objects - Create, Edit, and Delete Sources and Targets - Create, Edit, and Delete Run-time Objects - Manage Run-time Object Execution - Create Connections	- Read, Write, and Execute on all connection objects created by the Metadata Manager Service - Read, Write, and Execute on the Metadata Load folder and all folders created to extract profiling data from the Metadata Manager source
Metadata Manager Service	Load Resource	n/a

In the PowerCenter repository, the user who creates a folder or connection object is the owner of the object. The object owner or a user assigned the Administrator role for the PowerCenter Repository Service can delete repository folders and connection objects. If you change the associated PowerCenter Integration Service user, you must assign this user as the owner of the following repository objects in the PowerCenter Client:

- All connection objects created by the Metadata Manager Service
- The Metadata Load folder and all profiling folders created by the Metadata Manager Service

CHAPTER 15

PowerCenter Integration Service

This chapter includes the following topics:

- PowerCenter Integration Service Overview, 200
- Creating a PowerCenter Integration Service, 201
- Enabling and Disabling PowerCenter Integration Services and Processes, 202
- Operating Mode, 204
- PowerCenter Integration Service Properties, 207
- Operating System Profiles, 215
- Associated Repository for the PowerCenter Integration Service, 217
- PowerCenter Integration Service Processes, 218

PowerCenter Integration Service Overview

The PowerCenter Integration Service is an application service that runs sessions and workflows. Use the Administrator tool to manage the PowerCenter Integration Service.

You can use the Administrator tool to complete the following configuration tasks for the PowerCenter Integration Service:

- Create a PowerCenter Integration Service. Create a PowerCenter Integration Service to replace an existing PowerCenter Integration Service or to use multiple PowerCenter Integration Services.
- Enable or disable the PowerCenter Integration Service. Enable the PowerCenter Integration Service to run sessions and workflows. You might disable the PowerCenter Integration Service to prevent users from running sessions and workflows while performing maintenance on the machine or modifying the repository.
- Configure normal or safe mode.Configure the PowerCenter Integration Service to run in normal or safe mode.
- Configure the PowerCenter Integration Service properties. Configure the PowerCenter Integration Service properties to change behavior of the PowerCenter Integration Service.
- Configure the associated repository. You must associate a repository with a PowerCenter Integration Service. The PowerCenter Integration Service uses the mappings in the repository to run sessions and workflows.
- Configure the PowerCenter Integration Service processes. Configure service process properties for each node, such as the code page and service process variables.
- Configure permissions on the PowerCenter Integration Service.
- Remove a PowerCenter Integration Service. You may need to remove a PowerCenter Integration Service if it becomes obsolete.

Creating a PowerCenter Integration Service

You can create a PowerCenter Integration Service when you configure Informatica application services. You may need to create an additional PowerCenter Integration Service to replace an existing one or create multiple PowerCenter Integration Services.

You must assign a PowerCenter repository to the PowerCenter Integration Service. You can assign the repository when you create the PowerCenter Integration Service or after you create the PowerCenter Integration Service. You must assign a repository before you can run the PowerCenter Integration Service. The repository that you assign to the PowerCenter Integration Service is called the *associated repository*. The PowerCenter Integration Service retrieves metadata, such as workflows and mappings, from the associated repository.

After you create a PowerCenter Integration Service, you must assign a code page for each PowerCenter Integration Service process. The code page for each PowerCenter Integration Service process must be a subset of the code page of the associated repository. You must select the associated repository before you can select the code page for a PowerCenter Integration Service process. The PowerCenter Repository Service must be enabled to set up a code page for a PowerCenter Integration Service process.

Note: If you configure a PowerCenter Integration Service to run on a node that is unavailable, you must start the node and configure $PMRootDir for the service process before you run workflows with the PowerCenter Integration Service.

1. In the Administrator tool, click the Domain tab.
2. On the Navigator Actions menu, click New > PowerCenter Integration Service.

   The New Integration Service dialog box appears.
3. Enter values for the following PowerCenter Integration Service options.

   The following table describes the PowerCenter Integration Service options:

Property	Description
Name	Name of the PowerCenter Integration Service. The characters must be compatible with the code page of the associated repository. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the PowerCenter Integration Service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Browse to choose a different folder. You can also move the PowerCenter Integration Service to a different folder after you create it.
License	License to assign to the PowerCenter Integration Service. If you do not select a license now, you can assign a license to the service later. Required if you want to enable the PowerCenter Integration Service. The options allowed in your license determine the properties you must set for the PowerCenter Integration Service.
Node	Node on which the PowerCenter Integration Service runs. Required if you do not select a license or your license does not include the high availability option.
Assign	Indicates whether the PowerCenter Integration Service runs on a grid or nodes.
Grid	Name of the grid on which the PowerCenter Integration Service run.

Property	Description
	Available if your license includes the high availability option. Required if you assign the PowerCenter Integration Service to run on a grid.
Primary Node	Primary node on which the PowerCenter Integration Service runs. Required if you assign the PowerCenter Integration Service to run on nodes.
Backup Nodes	Nodes used as backup to the primary node. Displays if you configure the PowerCenter Integration Service to run on mutiple nodes and you have the high availability option. Click Select to choose the nodes to use for backup.
Associated Repository Service	PowerCenter Repository Service associated with the PowerCenter Integration Service. If you do not select the associated PowerCenter Repository Service now, you can select it later. You must select the PowerCenter Repository Service before you run the PowerCenter Integration Service. To apply changes, restart the PowerCenter Integration Service.
Repository User Name	User name to access the repository. To apply changes, restart the PowerCenter Integration Service.
Repository Password	Password for the user. Required when you select an associated PowerCenter Repository Service. To apply changes, restart the PowerCenter Integration Service.
Security Domain	Security domain for the user. Required when you select an associated PowerCenter Repository Service. To apply changes, restart the PowerCenter Integration Service. The Security Domain field appears when the Informatica domain contains an LDAP security domain.
Data Movement Mode	Mode that determines how the PowerCenter Integration Service handles character data. Choose ASCII or Unicode. ASCII mode passes 7-bit ASCII or EBCDIC character data. Unicode mode passes 8-bit ASCII and multibyte character data from sources to targets. Default is ASCII. To apply changes, restart the PowerCenter Integration Service.

4. Click Finish.

   You must specify a PowerCenter Repository Service before you can enable the PowerCenter Integration Service.

   You can specify the code page for each PowerCenter Integration Service process node and select the Enable Service option to enable the service. If you do not specify the code page information now, you can specify it later. You cannot enable the PowerCenter Integration Service until you assign the code page for each PowerCenter Integration Service process node.

5. Click Finish.

Enabling and Disabling PowerCenter Integration Services and Processes

You can enable and disable a PowerCenter Integration Service process or the entire PowerCenter Integration Service. If you run the PowerCenter Integration Service on a grid or with the high availability option, you have one PowerCenter Integration Service process configured for each node. For a grid, the PowerCenter Integration

Service runs all enabled PowerCenter Integration Service processes. With high availability, the PowerCenter Integration Service runs the PowerCenter Integration Service process on the primary node.

Enabling or Disabling a PowerCenter Integration Service Process

Use the Administrator tool to enable and disable a PowerCenter Integration Service process. Each service process runs on one node. You must enable the PowerCenter Integration Service process if you want the node to perform PowerCenter Integration Service tasks. You may want to disable the service process on a node to perform maintenance on that node or to enable safe mode for the PowerCenter Integration Service.

When you disable a PowerCenter Integration Service process, you must choose the mode to disable it in. You can choose one of the following options:

- Complete. Allows the sessions and workflows to run to completion before disabling the service process.
- Stop. Stops all sessions and workflows and then disables the service process.
- Abort. Tries to stop all sessions and workflows before aborting them and disabling the service process.

To enable or disable a PowerCenter Integration Service process:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Integration Service.
3. In the contents panel, click the Processes view.
4. Select a process
5. On the Domain tab Actions menu, select Disable Process to disable the service process or select Enable Process to enable the service process.
6. To enable a service process, go to the Domain tab Actions menu and select Enable Process.
7. To disable a service process, go to the Domain tab Actions menu and select Disable Process.

   Choose the disable mode and click OK.

Enabling or Disabling the PowerCenter Integration Service

Use the Administrator tool to enable and disable a PowerCenter Integration Service. You may want to disable a PowerCenter Integration Service if you need to perform maintenance or if you want temporarily restrict users from using the service. You can enable a disabled PowerCenter Integration Service to make it available again.

When you disable the PowerCenter Integration Service, you shut down the PowerCenter Integration Service and disable all service processes for the PowerCenter Integration Service. If you are running a PowerCenter Integration Service on a grid, you disable all service processes on the grid.

When you disable the PowerCenter Integration Service, you must choose what to do if a process or workflow is running. You must choose one of the following options:

- Complete. Allows the sessions and workflows to run to completion before shutting down the service.
- Stop. Stops all sessions and workflows and then shuts down the service.
- Abort. Tries to stop all sessions and workflows before aborting them and shutting down the service.

When you enable the PowerCenter Integration Service, the service starts. The associated PowerCenter Repository Service must be started before you can enable the PowerCenter Integration Service. If you enable a PowerCenter Integration Service when the associated PowerCenter Repository Service is not running, the following error appears:

```
The Service Manager could not start the service due to the following error: [DOM_10076] Unable to
enable service [<Integration Service] because of dependent services [<PowerCenter Repository Service>]
are not initialized.
```

If the PowerCenter Integration Service is unable to start, the Service Manager keeps trying to start the service until it reaches the maximum restart attempts defined in the domain properties. For example, if you try to start the PowerCenter Integration Service without specifying the code page for each PowerCenter Integration Service process, the domain tries to start the service. The service does not start without specifying a valid code page for each PowerCenter Integration Service process. The domain keeps trying to start the service until it reaches the maximum number of attempts.

If the service fails to start, review the logs for this PowerCenter Integration Service to determine the reason for failure and fix the problem. After you fix the problem, you must disable and re-enable the PowerCenter Integration Service to start it.

To enable or disable a PowerCenter Integration Service:

1. In the Administrator tool, click the Domain tab
2. In the Navigator, select the PowerCenter Integration Service.
3. On the Domain tab Actions menu, select Disable Service to disable the service or select Enable Service to enable the service.
4. To disable and immediately enable the PowerCenter Integration Service, select Recycle.

Operating Mode

You can run the PowerCenter Integration Service in normal or safe operating mode. Normal mode provides full access to users with permissions and privileges to use a PowerCenter Integration Service. Safe mode limits user access to the PowerCenter Integration Service and workflow activity during environment migration or PowerCenter Integration Service maintenance activities.

Run the PowerCenter Integration Service in normal mode during daily operations. In normal mode, users with workflow privileges can run workflows and get session and workflow information for workflows assigned to the PowerCenter Integration Service.

You can configure the PowerCenter Integration Service to run in safe mode or to fail over in safe mode. When you enable the PowerCenter Integration Service to run in safe mode or when the PowerCenter Integration Service fails over in safe mode, it limits access and workflow activity to allow administrators to perform migration or maintenance activities.

Run the PowerCenter Integration Service in safe mode to control which workflows a PowerCenter Integration Service runs and which users can run workflows during migration and maintenance activities. Run in safe mode to verify a production environment, manage workflow schedules, or maintain a PowerCenter Integration Service. In safe mode, users that have the Administrator role for the associated PowerCenter Repository Service can run workflows and get information about sessions and workflows assigned to the PowerCenter Integration Service.

Normal Mode

When you enable a PowerCenter Integration Service to run in normal mode, the PowerCenter Integration Service begins running scheduled workflows. It also completes workflow failover for any workflows that failed while in safe mode, recovers client requests, and recovers any workflows configured for automatic recovery that failed in safe mode.

Users with workflow privileges can run workflows and get session and workflow information for workflows assigned to the PowerCenter Integration Service.

When you change the operating mode from safe to normal, the PowerCenter Integration Service begins running scheduled workflows and completes workflow failover and workflow recovery for any workflows configured for

automatic recovery. You can use the Administrator tool to view the log events about the scheduled workflows that started, the workflows that failed over, and the workflows recovered by the PowerCenter Integration Service.

Safe Mode

In safe mode, access to the PowerCenter Integration Service is limited. You can configure the PowerCenter Integration Service to run in safe mode or to fail over in safe mode:

- Enable in safe mode. Enable the PowerCenter Integration Service in safe mode to perform migration or maintenance activities. When you enable the PowerCenter Integration Service in safe mode, you limit access to the PowerCenter Integration Service.

  When you enable a PowerCenter Integration Service in safe mode, you can choose to have the PowerCenter Integration Service complete, abort, or stop running workflows. In addition, the operating mode on failover also changes to safe.
- Fail over in safe mode. Configure the PowerCenter Integration Service process to fail over in safe mode during migration or maintenance activities. When the PowerCenter Integration Service process fails over to a backup node, it restarts in safe mode and limits workflow activity and access to the PowerCenter Integration Service. The PowerCenter Integration Service restores the state of operations for any workflows that were running when the service process failed over, but does not fail over or automatically recover the workflows. You can manually recover the workflow.

  After the PowerCenter Integration Service fails over in safe mode during normal operations, you can correct the error that caused the PowerCenter Integration Service process to fail over and restart the service in normal mode.

The behavior of the PowerCenter Integration Service when it fails over in safe mode is the same as when you enable the PowerCenter Integration Service in safe mode. All scheduled workflows, including workflows scheduled to run continuously or start on service initialization, do not run. The PowerCenter Integration Service does not fail over schedules or workflows, does not automatically recover workflows, and does not recover client requests.

Running the PowerCenter Integration Service in Safe Mode

This section describes the specific migration and maintenance activities that you can complete in the PowerCenter Workflow Manager and PowerCenter Workflow Monitor, the behavior of the PowerCenter Integration Service in safe mode, and the privileges required to run and monitor workflows in safe mode.

Performing Migration or Maintenance

You might want to run a PowerCenter Integration Service in safe mode for the following reasons:

- Test a development environment. Run the PowerCenter Integration Service in safe mode to test a development environment before migrating to production. You can run workflows that contain session and command tasks to test the environment. Run the PowerCenter Integration Service in safe mode to limit access to the PowerCenter Integration Service when you run the test sessions and command tasks.
- Manage workflow schedules. During migration, you can unschedule workflows that only run in a development environment. You can enable the PowerCenter Integration Service in safe mode, unschedule the workflow, and then enable the PowerCenter Integration Service in normal mode. After you enable the service in normal mode, the workflows that you unscheduled do not run.
- Troubleshoot the PowerCenter Integration Service. Configure the PowerCenter Integration Service to fail over in safe mode and troubleshoot errors when you migrate or test a production environment configured for high availability. After the PowerCenter Integration Service fails over in safe mode, you can correct the error that caused the PowerCenter Integration Service to fail over.

- Perform maintenance on the PowerCenter Integration Service. When you perform maintenance on a PowerCenter Integration Service, you can limit the users who can run workflows. You can enable the PowerCenter Integration Service in safe mode, change PowerCenter Integration Service properties, and verify the PowerCenter Integration Service functionality before allowing other users to run workflows. For example, you can use safe mode to test changes to the paths for PowerCenter Integration Service files for PowerCenter Integration Service processes.

Workflow Tasks

The following table describes the tasks that users with the Administrator role can perform when the PowerCenter Integration Service runs in safe mode:

Task	Task Description
Run workflows.	Start, stop, abort, and recover workflows. The workflows may contain session or command tasks required to test a development or production environment.
Unschedule workflows.	Unschedule workflows in the PowerCenter Workflow Manager.
Monitor PowerCenter Integration Service properties.	Connect to the PowerCenter Integration Service in the PowerCenter Workflow Monitor. Get PowerCenter Integration Service details and monitor information.
Monitor workflow and task details.	Connect to the PowerCenter Integration Service in the PowerCenter Workflow Monitor and get task, session, and workflow details.
Recover workflows.	Manually recover failed workflows.

PowerCenter Integration Service Behavior

Safe mode affects PowerCenter Integration Service behavior for the following workflow and high availability functionality:

- Workflow schedules. Scheduled workflows remain scheduled, but they do not run if the PowerCenter Integration Service is running in safe mode. This includes workflows scheduled to run continuously and run on service initialization.

  Workflow schedules do not fail over when a PowerCenter Integration Service fails over in safe mode. For example, you configure a PowerCenter Integration Service to fail over in safe mode. The PowerCenter Integration Service process fails for a workflow scheduled to run five times, and it fails over after it runs the workflow three times. The PowerCenter Integration Service does not complete the remaining workflows when it fails over to the backup node. The PowerCenter Integration Service completes the workflows when you enable the PowerCenter Integration Service in safe mode.
- Workflow failover. When a PowerCenter Integration Service process fails over in safe mode, workflows do not fail over. The PowerCenter Integration Service restores the state of operations for the workflow. When you enable the PowerCenter Integration Service in normal mode, the PowerCenter Integration Service fails over the workflow and recovers it based on the recovery strategy for the workflow.
- Workflow recovery.The PowerCenter Integration Service does not recover workflows when it runs in safe mode or when the operating mode changes from normal to safe.

  The PowerCenter Integration Service recovers a workflow that failed over in safe mode when you change the operating mode from safe to normal, depending on the recovery strategy for the workflow. For example, you configure a workflow for automatic recovery and you configure the PowerCenter Integration Service to fail over in safe mode. If the PowerCenter Integration Service process fails over, the workflow is not recovered while the

PowerCenter Integration Service runs in safe mode. When you enable the PowerCenter Integration Service in normal mode, the workflow fails over and the PowerCenter Integration Service recovers it.

You can manually recover the workflow if the workflow fails over in safe mode. You can recover the workflow after the resilience timeout for the PowerCenter Integration Service expires.

- Client request recovery. The PowerCenter Integration Service does not recover client requests when it fails over in safe mode. For example, you stop a workflow and the PowerCenter Integration Service process fails over before the workflow stops. The PowerCenter Integration Service process does not recover your request to stop the workflow when the workflow fails over.

  When you enable the PowerCenter Integration Service in normal mode, it recovers the client requests.

Related Topics:

- "Managing High Availability for the PowerCenter Integration Service" on page 137

Configuring the PowerCenter Integration Service Operating Mode

You can use the Administrator tool to configure the PowerCenter Integration Service to run in safe mode, run in normal mode, or run in safe or normal mode on failover. To configure the operating mode on failover, you must have the high availability option.

Note: When you change the operating mode on fail over from safe to normal, the change takes effect immediately.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a PowerCenter Integration Service.
3. Click the Properties view.
4. Go to the Operating Mode Configuration section and click Edit.
5. To run the PowerCenter Integration Service in normal mode, set OperatingMode to Normal.

   To run the service in safe mode, set OperatingMode to Safe.
6. To run the service in normal mode on failover, set OperatingModeOnFailover to Normal.

   To run the service in safe mode on failover, set OperatingModeOnFailover to Safe.
7. Click OK.
8. Restart the PowerCenter Integration Service.

The PowerCenter Integration Service starts in the selected mode. The service status at the top of the content pane indicates when the service has restarted.

PowerCenter Integration Service Properties

Use the Administrator tool to configure the following PowerCenter Integration Service properties:

- General properties. Assign a license and configure the PowerCenter Integration Service to run on a grid or nodes.
- PowerCenter Integration Service properties. Set the values for the PowerCenter Integration Service variables.
- Advanced properties. Configure advanced properties that determine security and control the behavior of sessions and logs
- Operating mode configuration. Set the PowerCenter Integration Service to start in normal or safe mode and to fail over in normal or safe mode.

- Compatibility and database properties. Configure the source and target database properties, such the maximum number of connections, and configure properties to enable compatibility with previous versions of PowerCenter.
- Configuration properties. Configure the configuration properties, such as the data display format.
- HTTP proxy properties. Configure the connection to the HTTP proxy server.
- Custom properties. Custom properties include properties that are unique to your Informatica environment or that apply in special cases. A PowerCenter Integration Service has no custom properties when you create it. Use custom properties only if Informatica Global Customer Support instructs you to. You can override some of the custom properties at the session level.

To view the properties, select the PowerCenter Integration Service in the Navigator and click Properties view. To modify the properties, edit the section for the property you want to modify.

General Properties

The amount of system resources that the PowerCenter Integration Services uses depends on how you set up the PowerCenter Integration Service. You can configure a PowerCenter Integration Service to run on a grid or on nodes. You can view the system resource usage of the PowerCenter Integration Service using the PowerCenter Workflow Monitor.

When you use a grid, the PowerCenter Integration Service distributes workflow tasks and session threads across multiple nodes. You can increase performance when you run sessions and workflows on a grid. If you choose to run the PowerCenter Integration Service on a grid, select the grid. You must have the server grid option to run the PowerCenter Integration Service on a grid. You must create the grid before you can select the grid.

If you configure the PowerCenter Integration Service to run on nodes, choose one or more PowerCenter Integration Service process nodes. If you have only one node and it becomes unavailable, the domain cannot accept service requests. With the high availability option, you can run the PowerCenter Integration Service on multiple nodes. To run the service on multiple nodes, choose the primary and backup nodes.

To edit the general properties, select the PowerCenter Integration Service in the Navigator, and then click the Properties view. Edit the section General Properties section. To apply changes, restart the PowerCenter Integration Service.

The following table describes the general properties:

Property	Description
Name	Name of the PowerCenter Integration Service.
Description	Description of the PowerCenter Integration Service.
License	License assigned to the PowerCenter Integration Service.
Assign	Indicates whether the PowerCenter Integration Service runs on a grid or on nodes.
Grid	Name of the grid on which the PowerCenter Integration Service runs. Required if you run the PowerCenter Integration Service on a grid.
Primary Node	Primary node on which the PowerCenter Integration Service runs. Required if you run the PowerCenter Integration Service on nodes and you specify at least one backup node. You can select any node in the domain.
Backup Node	Backup node on which the PowerCenter Integration Service can run on. If the primary node becomes unavailable, the PowerCenter Integration Service runs on a backup node. You can select multiple nodes

Property	Description
	as backup nodes. Available if you have the high availability option and you run the PowerCenter Integration Service on nodes.

PowerCenter Integration Service Properties

You can set the values for the service variables at the service level. You can override some of the PowerCenter Integration Service variables at the session level or workflow level. To override the properties, configure the properties for the session or workflow.

To edit the service properties, select the PowerCenter Integration Service in the Navigator, and then click the Properties view. Edit the PowerCenter Integration Service Properties section.

The following table describes the service properties:

Property	Description
DataMovementMode	Mode that determines how the PowerCenter Integration Service handles character data. In ASCII mode, the PowerCenter Integration Service recognizes 7-bit ASCII and EBCDIC characters and stores each character in a single byte. Use ASCII mode when all sources and targets are 7-bit ASCII or EBCDIC character sets. In Unicode mode, the PowerCenter Integration Service recognizes multibyte character sets as defined by supported code pages. Use Unicode mode when sources or targets use 8-bit or multibyte character sets and contain character data. Default is ASCII. To apply changes, restart the PowerCenter Integration Service.
$PMSuccessEmailUser	Service variable that specifies the email address of the user to receive email messages when a session completes successfully. Use this variable for the Email User Name attribute for success email. If multiple email addresses are associated with a single user, messages are sent to all of the addresses. If the Integration Service runs on UNIX, you can enter multiple email addresses separated by a comma. If the Integration Service runs on Windows, you can enter multiple email addresses separated by a semicolon or use a distribution list. The PowerCenter Integration Service does not expand this variable when you use it for any other email type.
$PMFailureEmailUser	Service variable that specifies the email address of the user to receive email messages when a session fails to complete. Use this variable for the Email User Name attribute for failure email. If multiple email addresses are associated with a single user, messages are sent to all of the addresses. If the Integration Service runs on UNIX, you can enter multiple email addresses separated by a comma. If the Integration Service runs on Windows, you can enter multiple email addresses separated by a semicolon or use a distribution list. The PowerCenter Integration Service does not expand this variable when you use it for any other email type.
$PMSessionLogCount	Service variable that specifies the number of session logs the PowerCenter Integration Service archives for the session. Minimum value is 0. Default is 0.
$PMWorkflowLogCount	Service variable that specifies the number of workflow logs the PowerCenter Integration Service archives for the workflow. Minimum value is 0. Default is 0.
$PMSessionErrorThreshold	Service variable that specifies the number of non-fatal errors the PowerCenter Integration Service allows before failing the session. Non-fatal errors include reader, writer, and DTM errors. If you want to stop the session on errors, enter the number of non-fatal errors you

Property	Description
	want to allow before stopping the session. The PowerCenter Integration Service maintains an independent error count for each source, target, and transformation. Use to configure the Stop On option in the session properties. Defaults to 0. If you use the default setting 0, non-fatal errors do not cause the session to stop.

Advanced Properties

You can configure the properties that control the behavior of PowerCenter Integration Service security, sessions, and logs. To edit the advanced properties, select the PowerCenter Integration Service in the Navigator, and then click the Properties view. Edit the Advanced Properties section.

The following table describes the advanced properties:

Property	Description
Error Severity Level	Level of error logging for the domain. These messages are written to the Log Manager and log files. Specify one of the following message levels: - Error. Writes ERROR code messages to the log. - Warning. Writes WARNING and ERROR code messages to the log. - Information. Writes INFO, WARNING, and ERROR code messages to the log. - Tracing. Writes TRACE, INFO, WARNING, and ERROR code messages to the log. - Debug. Writes DEBUG, TRACE, INFO, WARNING, and ERROR code messages to the log. Default is INFO.
Resilience Timeout	Number of seconds that the service tries to establish or reestablish a connection to another service. If blank, the value is derived from the domain-level settings. Valid values are between 0 and 2,592,000, inclusive. Default is 180 seconds.
Limit on Resilience Timeouts	Number of seconds that the service holds on to resources for resilience purposes. This property places a restriction on clients that connect to the service. Any resilience timeouts that exceed the limit are cut off at the limit. If blank, the value is derived from the domain-level settings. Valid values are between 0 and 2,592,000, inclusive. Default is 180 seconds.
Timestamp Workflow Log Messages	Appends a timestamp to messages that are written to the workflow log. Default is No.
Allow Debugging	Allows you to run debugger sessions from the Designer. Default is Yes.
LogsInUTF8	Writes to all logs using the UTF-8 character set. Disable this option to write to the logs using the PowerCenter Integration Service code page. This option is available when you configure the PowerCenter Integration Service to run in Unicode mode. When running in Unicode data movement mode, default is Yes. When running in ASCII data movement mode, default is No.
Use Operating System Profiles	Enables the use of operating system profiles. You can select this option if the PowerCenter Integration Service runs on UNIX. To apply changes, restart the PowerCenter Integration Service.

TrustStore	Enter the value for TrustStore using the following syntax:
	`<path>/<filename >`
	For example:
	`./Certs/trust.keystore`

Property	Description
ClientStore	Enter the value for ClientStore using the following syntax: <path>/<filename > For example: ./Certs/client.keystore
JCEProvider	Enter the JCEProvider class name to support NTLM authentication. For example: com.unix.crypto.provider.UnixJCE.
IgnoreResourceRequirements	Ignores task resource requirements when distributing tasks across the nodes of a grid. Used when the PowerCenter Integration Service runs on a grid. Ignored when the PowerCenter Integration Service runs on a node. Enable this option to cause the Load Balancer to ignore task resource requirements. It distributes tasks to available nodes whether or not the nodes have the resources required to run the tasks. Disable this option to cause the Load Balancer to match task resource requirements with node resource availability when distributing tasks. It distributes tasks to nodes that have the required resources. Default is Yes.
Run sessions impacted by dependency updates	Runs sessions that are impacted by dependency updates. By default, the PowerCenter Integration Service does not run impacted sessions. When you modify a dependent object, the parent object can become invalid. The PowerCenter client marks a session with a warning if the session is impacted. At run time, the PowerCenter Integration Service fails the session if it detects errors.
Persist Run-time Statistics to Repository	Level of run-time information stored in the repository. Specify one of the following levels: - None. PowerCenter Integration Service does not store any session or workflow run-time information in the repository. - Normal. PowerCenter Integration Service stores workflow details, task details, session statistics, and source and target statistics in the repository. Default is Normal. - Verbose. PowerCenter Integration Service stores workflow details, task details, session statistics, source and target statistics, partition details, and performance details in the repository. To store session performance details in the repository, you must also configure the session to collect performance details and write them to the repository. The PowerCenter Workflow Monitor shows run-time statistics stored in the repository.
Flush Session Recovery Data	Flushes session recovery data for the recovery file from the operating system buffer to the disk. For real-time sessions, the PowerCenter Integration Service flushes the recovery data after each flush latency interval. For all other sessions, the PowerCenter Integration Service flushes the recovery data after each commit interval or user-defined commit. Use this property to prevent data loss if the PowerCenter Integration Service is not able to write recovery data for the recovery file to the disk. Specify one of the following levels: - Auto. PowerCenter Integration Service flushes recovery data for all real-time sessions with a JMS or WebSphere MQ source and a non-relational target. - Yes. PowerCenter Integration Service flushes recovery data for all sessions. - No. PowerCenter Integration Service does not flush recovery data. Select this option if you have highly available external systems or if you need to optimize performance. Required if you enable session recovery. Default is Auto. **Note:** If you select Yes or Auto, you might impact performance.

Operating Mode Configuration

The operating mode determines how much user access and workflow activity the PowerCenter Integration Service allows when runs. You can set the service to run in normal mode to allow users full access or in safe mode to limit access. You can also set how the services operates when it fails over to another node.

The following table describes the operating mode properties:

Property	Description
OperatingMode	Mode in which the PowerCenter Integration Service runs.
OperatingModeOnFailover	Operating mode of the PowerCenter Integration Service when the service process fails over to another node.

Compatibility and Database Properties

You can configure properties to reinstate previous Informatica behavior or to configure database behavior. To edit the compatibility and database properties, select the PowerCenter Integration Service in the Navigator, and then click the Properties view > Compatibility and Database Properties > Edit.

The following table describes the compatibility and database properties:

Property	Description
PMServer3XCompatibility	Handles Aggregator transformations as it did in version 3.5. The PowerCenter Integration Service treats null values as zeros in aggregate calculations and performs aggregate calculations before flagging records for insert, update, delete, or reject in Update Strategy expressions. Disable this option to treat null values as NULL and perform aggregate calculations based on the Update Strategy transformation. This overrides both *Aggregate treat nulls as zero* and *Aggregate treat rows as insert*. Default is No.
JoinerSourceOrder6xCompatibility	Processes master and detail pipelines sequentially as it did in versions prior to 7.0. The PowerCenter Integration Service processes all data from the master pipeline before it processes the detail pipeline. When the target load order group contains multiple Joiner transformations, the PowerCenter Integration Service processes the detail pipelines sequentially. The PowerCenter Integration Service fails sessions when the mapping meets any of the following conditions: - The mapping contains a multiple input group transformation, such as the Custom transformation. Multiple input group transformations require the PowerCenter Integration Service to read sources concurrently. - You configure any Joiner transformation with transaction level transformation scope. Disable this option to process the master and detail pipelines concurrently. Default is No.
AggregateTreatNullAsZero	Treats null values as zero in Aggregator transformations. Disable this option to treat null values as NULL in aggregate calculations. Default is No.
AggregateTreatRowAsInsert	When enabled, the PowerCenter Integration Service ignores the update strategy of rows when it performs aggregate calculations. This option ignores sorted input option of the Aggregator transformation. When disabled, the PowerCenter

Property	Description
	Integration Service uses the update strategy of rows when it performs aggregate calculations. Default is No.
DateHandling40Compatibility	Handles dates as in version 4.0. Disable this option to handle dates as defined in the current version of PowerCenter. Date handling significantly improved in version 4.5. Enable this option to revert to version 4.0 behavior. Default is No.
TreatCHARasCHARonRead	If you have PowerExchange for PeopleSoft, use this option for PeopleSoft sources on Oracle. You cannot, however, use it for PeopleSoft lookup tables on Oracle or PeopleSoft sources on Microsoft SQL Server.
Max Lookup SP DB Connections	Maximum number of connections to a lookup or stored procedure database when you start a session. If the number of connections needed exceeds this value, session threads must share connections. This can result in decreased performance. If blank, the PowerCenter Integration Service allows an unlimited number of connections to the lookup or stored procedure database. If the PowerCenter Integration Service allows an unlimited number of connections, but the database user does not have permission for the number of connections required by the session, the session fails. Minimum value is 0. Default is 0.
Max Sybase Connections	Maximum number of connections to a Sybase ASE database when you start a session. If the number of connections required by the session is greater than this value, the session fails. Minimum value is 100. Maximum value is 2147483647. Default is 100.
Max MSSQL Connections	Maximum number of connections to a Microsoft SQL Server database when you start a session. If the number of connections required by the session is greater than this value, the session fails. Minimum value is 100. Maximum value is 2147483647. Default is 100.
NumOfDeadlockRetries	Number of times the PowerCenter Integration Service retries a target write on a database deadlock. Minimum value is 10. Maximum value is 1,000,000,000. Default is 10.
DeadlockSleep	Number of seconds before the PowerCenter Integration Service retries a target write on database deadlock. If set to 0 seconds, the PowerCenter Integration Service retries the target write immediately. Minimum value is 0. Maximum value is 2147483647. Default is 0.

Configuration Properties

You can configure session and miscellaneous properties, such as whether to enforce code page compatibility.

To edit the configuration properties, select the PowerCenter Integration Service in the Navigator, and then click the Properties view > Configuration Properties > Edit.

The following table describes the configuration properties:

Property	Description
XMLWarnDupRows	Writes duplicate row warnings and duplicate rows for XML targets to the session log. Default is Yes.
CreateIndicatorFiles	Creates indicator files when you run a workflow with a flat file target. Default is No.
OutputMetaDataForFF	Writes column headers to flat file targets. The PowerCenter Integration Service writes the target definition port names to the flat file target in the first line, starting with the # symbol. Default is No.
TreatDBPartitionAsPassThrough	Uses pass-through partitioning for non-DB2 targets when the partition type is Database Partitioning. Enable this option if you specify Database Partitioning for a non-DB2 target. Otherwise, the PowerCenter Integration Service fails the session. Default is No.
ExportSessionLogLibName	Name of an external shared library to handle session event messages. Typically, shared libraries in Windows have a file name extension of .dll. In UNIX, shared libraries have a file name extension of .sl. If you specify a shared library and the PowerCenter Integration Service encounters an error when loading the library or getting addresses to the functions in the shared library, then the session will fail. The library name you specify can be qualified with an absolute path. If you do not provide the path for the shared library, the PowerCenter Integration Service will locate the shared library based on the library path environment variable specific to each platform.
TreatNullInComparisonOperatorsAs	Determines how the PowerCenter Integration Service evaluates null values in comparison operations. Specify one of the following options: - Null. The PowerCenter Integration Service evaluates null values as NULL in comparison expressions. If either operand is NULL, the result is NULL. - High. The PowerCenter Integration Service evaluates null values as greater than non-null values in comparison expressions. If both operands are NULL, the PowerCenter Integration Service evaluates them as equal. When you choose High, comparison expressions never result in NULL. - Low. The PowerCenter Integration Service evaluates null values as less than non-null values in comparison expressions. If both operands are NULL, the PowerCenter Integration Service treats them as equal. When you choose Low, comparison expressions never result in NULL. Default is NULL.
WriterWaitTimeOut	In target-based commit mode, the amount of time in seconds the writer remains idle before it issues a commit when the following conditions are true: - The PowerCenter Integration Service has written data to the target. - The PowerCenter Integration Service has not issued a commit. The PowerCenter Integration Service may commit to the target before or after the configured commit interval. Minimum value is 60. Maximum value is 2147483647. Default is 60. If you configure the timeout to be 0 or a negative number, the PowerCenter Integration Service defaults to 60 seconds.
MSExchangeProfile	Microsoft Exchange profile used by the Service Start Account to send post-session email. The Service Start Account must be set up as a Domain account to use this feature.

Property	Description
DateDisplayFormat	Date format the PowerCenter Integration Service uses in log entries. The PowerCenter Integration Service validates the date format you enter. If the date display format is invalid, the PowerCenter Integration Service uses the default date display format. Default is DY MON DD HH24:MI:SS YYYY.
ValidateDataCodePages	Enforces data code page compatibility. Disable this option to lift restrictions for source and target data code page selection, stored procedure and lookup database code page selection, and session sort order selection. The PowerCenter Integration Service performs data code page validation in Unicode data movement mode only. Option available if you run the PowerCenter Integration Service in Unicode data movement mode. Option disabled if you run the PowerCenter Integration Service in ASCII data movement mode. Default is Yes.

HTTP Proxy Properties

You can configure properties for the HTTP proxy server for Web Services and the HTTP transformation.

To edit the HTTP proxy properties, select the PowerCenter Integration Service in the Navigator, and click the Properties view > HTTP Proxy Properties > Edit.

The following table describes the HTTP proxy properties:

Property	Description
HttpProxyServer	Name of the HTTP proxy server.
HttpProxyPort	Port number of the HTTP proxy server. This must be a number.
HttpProxyUser	Authenticated user name for the HTTP proxy server. This is required if the proxy server requires authentication.
HttpProxyPassword	Password for the authenticated user. This is required if the proxy server requires authentication.
HttpProxyDomain	Domain for authentication.

Custom Properties

Custom properties include properties that are unique to your environment or that apply in special cases.

A PowerCenter Integration Service does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Operating System Profiles

By default, the PowerCenter Integration Service process runs all workflows using the permissions of the operating system user that starts Informatica Services. The PowerCenter Integration Service writes output files to a single shared location specified in the $PMRootDir service process variable.

When you configure the PowerCenter Integration Service to use operating system profiles, the PowerCenter Integration Service process runs workflows with the permission of the operating system user you define in the operating system profile. The operating system profile contains the operating system user name, service process variables, and environment variables. The operating system user must have access to the directories you configure in the profile and the directories the PowerCenter Integration Service accesses at run time. You can use operating system profiles for a PowerCenter Integration Service that runs on UNIX.

To use an operating system profile, assign the profile to a repository folder or assign the profile to a workflow when you start a workflow. You must have permission on the operating system profile to assign it to a folder or workflow. For example, you assign operating system profile Sales to workflow A. The user that runs workflow A must also have permissions to use operating system profile Sales. The PowerCenter Integration Service stores the output files for workflow A in a location specified in the $PMRootDir service process variable that the profile can access.

To manage permissions for operating system profiles, go to the Security page of the Administrator tool.

Operating System Profile Components

Configure the following components in an operating system profile:

- Operating system user name. Configure the operating system user that the PowerCenter Integration Service uses to run workflows.
- Service process variables. Configure service process variables in the operating system profile to specify different output file locations based on the profile assigned to the workflow.
- Environment variables. Configure environment variables that the PowerCenter Integration Services uses at run time.
- Permissions. Configure permissions for users to use operating system profiles.

Configuring Operating System Profiles

To use operating system profiles to run workflows, complete the following steps:

1. Enable operating system profiles in the advanced properties section of the PowerCenter Integration Service properties.
2. Set umask to 000 on every node where the PowerCenter Integration Service runs. To apply changes, restart Informatica services.
3. Configure *pmimpprocess* on every node where the PowerCenter Integration Service runs. *pmimpprocess* is a tool that the DTM process, command tasks, and parameter files use to switch between operating system users.
4. Create the operating system profiles on the Security page of the Administrator tool.

   On the Security tab Actions menu, select Confgure operating system profiles
5. Assign permissions on operating system profiles to users or groups.
6. You can assign operating system profiles to repository folders or to a workflow.

To configure pmimpprocess:

1. At the command prompt, switch to the following directory:

   ```
   <Informatica installation directory>/server/bin
   ```
2. Enter the following information at the command line to log in as the administrator user:

   ```
   su <administrator user name>
   ```

   For example, if the administrator user name is root enter the following command:

   ```
   su root
   ```

3. Enter the following commands to set the owner and group to the administrator user:

```
chown <administrator user name> pmimpprocess
chgrp <administrator user name> pmimpprocess
```

4. Enter the following commands to set the setuid bit:

```
chmod +g  pmimpprocess
chmod +s  pmimpprocess
```

Troubleshooting Operating System Profiles

After I selected Use Operating System Profiles, the PowerCenter Integration Service failed to start.

The PowerCenter Integration Service will not start if operating system profiles is enabled on Windows or a grid that includes a Windows node. You can enable operating system profiles on PowerCenter Integration Services that run on UNIX.

Or, *pmimpprocess* was not configured. To use operating system profiles, you must set the owner and group of *pmimpprocess* to administrator and enable the setuid bit for *pmimpprocess*.

Associated Repository for the PowerCenter Integration Service

When you create the PowerCenter Integration Service, you specify the repository associated with the PowerCenter Integration Service. You may need to change the repository connection information. For example, you need to update the connection information if the repository is moved to another database. You may need to choose a different repository when you move from a development repository to a production repository.

When you update or choose a new repository, you must specify the PowerCenter Repository Service and the user account used to access the repository. The Administrator tool lists the PowerCenter Repository Services defined in the same domain as the PowerCenter Integration Service.

To edit the associated repository properties, select the PowerCenter Integration Service in the Domain tab of the Administrator tool, and then click the Properties view > Associated Repository Properties > Edit.

The following table describes the associated repository properties:

Property	Description
Associated Repository Service	PowerCenter Repository Service name to which the PowerCenter Integration Service connects. To apply changes, restart the PowerCenter Integration Service.
Repository User Name	User name to access the repository. To apply changes, restart the PowerCenter Integration Service.
Repository Password	Password for the user. To apply changes, restart the PowerCenter Integration Service.
Security Domain	Security domain for the user. To apply changes, restart the PowerCenter Integration Service. The Security Domain field appears when the Informatica domain contains an LDAP security domain.

PowerCenter Integration Service Processes

The PowerCenter Integration Service can run each PowerCenter Integration Service process on a different node. When you select the PowerCenter Integration Service in the Administrator tool, you can view the PowerCenter Integration Service process nodes on the Processes tab.

You can change the following properties to configure the way that a PowerCenter Integration Service process runs on a node:

- General properties
- Custom properties
- Environment variables

General properties include the code page and directories for PowerCenter Integration Service files and Java components.

To configure the properties, select the PowerCenter Integration Service in the Administrator tool and click the Processes view. When you select a PowerCenter Integration Service process, the detail panel displays the properties for the service process.

Code Pages

You must specify the code page of each PowerCenter Integration Service process node. The node where the process runs uses the code page when it extracts, transforms, or loads data.

Before you can select a code page for a PowerCenter Integration Service process, you must select an associated repository for the PowerCenter Integration Service. The code page for each PowerCenter Integration Service process node must be a subset of the repository code page. When you edit this property, the field displays code pages that are a subset of the associated PowerCenter Repository Service code page.

When you configure the PowerCenter Integration Service to run on a grid or a backup node, you can use a different code page for each PowerCenter Integration Service process node. However, all codes pages for the PowerCenter Integration Service process nodes must be compatible.

Related Topics:

- “Understanding Globalization” on page 418

Directories for PowerCenter Integration Service Files

PowerCenter Integration Service files include run-time files, state of operation files, and session log files.

The PowerCenter Integration Service creates files to store the state of operations for the service. The state of operations includes information such as the active service requests, scheduled tasks, and completed and running processes. If the service fails, the PowerCenter Integration Service can restore the state and recover operations from the point of interruption.

The PowerCenter Integration Service process uses run-time files to run workflows and sessions. Run-time files include parameter files, cache files, input files, and output files. If the PowerCenter Integration Service uses operating system profiles, the operating system user specified in the profile must have access to the run-time files.

By default, the installation program creates a set of PowerCenter Integration Service directories in the server \infa_shared directory. You can set the shared location for these directories by configuring the service process variable $PMRootDir to point to the same location for each PowerCenter Integration Service process. Each PowerCenter Integration Service can use a separate shared location.

Configuring $PMRootDir

When you configure the PowerCenter Integration Service process variables, you specify the paths for the root directory and its subdirectories. You can specify an absolute directory for the service process variables. Make sure all directories specified for service process variables exist before running a workflow.

Set the root directory in the $PMRootDir service process variable. The syntax for $PMRootDir is different for Windows and UNIX:

- On Windows, enter a path beginning with a drive letter, colon, and backslash. For example:

  ```
  C:\Informatica\<infa_vesion>\server\infa_shared
  ```

- On UNIX**:** Enter an absolute path beginning with a slash. For example:

  ```
  /Informatica/<infa_vesion>/server/infa_shared
  ```

You can use $PMRootDir to define subdirectories for other service process variable values. For example, set the $PMSessionLogDir service process variable to $PMRootDir/SessLogs.

Configuring Service Process Variables for Multiple Nodes

When you configure the PowerCenter Integration Service to run on a grid or a backup node, all PowerCenter Integration Service processes associated with a PowerCenter Integration Service must use the same shared directories for PowerCenter Integration Service files.

Configure service process variables with identical absolute paths to the shared directories on each node that is configured to run the PowerCenter Integration Service. If you use a mounted drive or a mapped drive, the absolute path to the shared location must also be identical.

For example, if you have a primary and a backup node for the PowerCenter Integration Service, recovery fails when nodes use the following drives for the storage directory:

- Mapped drive on node1: F:\shared\Informatica\<infa_version>\infa_shared\Storage
- Mapped drive on node2: G:\shared\Informatica\<infa_version>\infa_shared\Storage

Recovery also fails when nodes use the following drives for the storage directory:

- Mounted drive on node1: /mnt/shared/Informatica/<infa_version>/infa_shared/Storage
- Mounted drive on node2: /mnt/shared_filesystem/Informatica/<infa_version>/infa_shared/Storage

To use the mapped or mounted drives successfully, both nodes must use the same drive.

Configuring Service Process Variables for Operating System Profiles

When you use operating system profiles, define absolute directory paths for $PMWorkflowLogDir and $PMStorageDir in the PowerCenter Integration Service properties. You configure $PMStorageDir in the PowerCenter Integration Service properties and the operating system profile. The PowerCenter Integration Service saves workflow recovery files to the $PMStorageDir configured in the PowerCenter Integration Service properties and saves the session recovery files to the $PMStorageDir configured in the operating system profile. Define the other service process variables within each operating system profile.

Directories for Java Components

You must specify the directory containing the Java components. The PowerCenter Integration Service uses the Java components for the following PowerCenter components:

- Custom transformation that uses Java code
- Java transformation
- PowerExchange for JMS

- PowerExchange for Web Services
- PowerExchange for webMethods

General Properties

The following table describes the general properties:

Property	Description
Codepage	Code page of the PowerCenter Integration Service process node.
$PMRootDir	Root directory accessible by the node. This is the root directory for other service process variables. It cannot include the following special characters: * ? < > " | , Default is <Installation_Directory>\server\infa_shared. The installation directory is based on the service version of the service that you created. When you upgrade the PowerCenter Integration Service, the $PMRootDir is not updated to the upgraded service version installation directory.
$PMSessionLogDir	Default directory for session logs. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SessLogs.
$PMBadFileDir	Default directory for reject files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/BadFiles.
$PMCacheDir	Default directory for index and data cache files. You can increase performance when the cache directory is a drive local to the PowerCenter Integration Service process. Do not use a mapped or mounted drive for cache files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Cache.
$PMTargetFileDir	Default directory for target files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/TgtFiles.
$PMSourceFileDir	Default directory for source files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SrcFiles.
$PMExtProcDir	Default directory for external procedures. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/ExtProc.
$PMTempDir	Default directory for temporary files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Temp.
$PMWorkflowLogDir	Default directory for workflow logs. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/WorkflowLogs.
$PMLookupFileDir	Default directory for lookup files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/LkpFiles.

Property	Description
$PMStorageDir	Default directory for state of operation files. The PowerCenter Integration Service uses these files for recovery if you have the high availability option or if you enable a workflow for recovery. These files store the state of each workflow and session operation. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Storage.
Java SDK ClassPath	Java SDK classpath. You can set the classpath to any JAR files you need to run a session that require java components. The PowerCenter Integration Service appends the values you set to the system CLASSPATH. For more information, see "Directories for Java Components" on page 219.
Java SDK Minimum Memory	Minimum amount of memory the Java SDK uses during a session. If the session fails due to a lack of memory, you may want to increase this value. Default is 32 MB.
Java SDK Maximum Memory	Maximum amount of memory the Java SDK uses during a session. If the session fails due to a lack of memory, you may want to increase this value. Default is 64 MB.

Custom Properties

You can configure custom properties for each node assigned to the PowerCenter Integration Service.

Custom properties include properties that are unique to your Informatica environment or that apply in special cases. A PowerCenter Integration Service process has no custom properties when you create it. Use custom properties only at the request of Informatica Global Customer Support.

Environment Variables

The database client path on a node is controlled by an environment variable.

Set the database client path environment variable for the PowerCenter Integration Service process if the PowerCenter Integration Service process requires a different database client than another PowerCenter Integration Service process that is running on the same node. For example, the service version of each PowerCenter Integration Service running on the node requires a different database client version. You can configure each PowerCenter Integration Service process to use a different value for the database client environment variable.

The database client code page on a node is usually controlled by an environment variable. For example, Oracle uses NLS_LANG, and IBM DB2 uses DB2CODEPAGE. All PowerCenter Integration Services and PowerCenter Repository Services that run on this node use the same environment variable. You can configure a PowerCenter Integration Service process to use a different value for the database client code page environment variable than the value set for the node.

You might want to configure the code page environment variable for a PowerCenter Integration Service process for the following reasons:

- A PowerCenter Integration Service and PowerCenter Repository Service running on the node require different database client code pages. For example, you have a Shift-JIS repository that requires that the code page environment variable be set to Shift-JIS. However, the PowerCenter Integration Service reads from and writes to databases using the UTF-8 code page. The PowerCenter Integration Service requires that the code page environment variable be set to UTF-8.

  Set the environment variable on the node to Shift-JIS. Then add the environment variable to the PowerCenter Integration Service process properties and set the value to UTF-8.

- Multiple PowerCenter Integration Services running on the node use different data movement modes. For example, you have one PowerCenter Integration Service running in Unicode mode and another running in ASCII mode on the same node. The PowerCenter Integration Service running in Unicode mode requires that the code page environment variable be set to UTF-8. For optimal performance, the PowerCenter Integration Service running in ASCII mode requires that the code page environment variable be set to 7-bit ASCII.

  Set the environment variable on the node to UTF-8. Then add the environment variable to the properties of the PowerCenter Integration Service process running in ASCII mode and set the value to 7-bit ASCII.

If the PowerCenter Integration Service uses operating system profiles, environment variables configured in the operating system profile override the environment variables set in the general properties for the PowerCenter Integration Service process.

CHAPTER 16

PowerCenter Integration Service Architecture

This chapter includes the following topics:

- PowerCenter Integration Service Architecture Overview, 223
- PowerCenter Integration Service Connectivity, 224
- PowerCenter Integration Service Process, 224
- Load Balancer, 226
- Data Transformation Manager (DTM) Process, 229
- Processing Threads, 230
- DTM Processing, 233
- Grids, 234
- System Resources, 236
- Code Pages and Data Movement Modes, 238
- Output Files and Caches, 238

PowerCenter Integration Service Architecture Overview

The PowerCenter Integration Service moves data from sources to targets based on PowerCenter workflow and mapping metadata stored in a PowerCenter repository. When a workflow starts, the PowerCenter Integration Service retrieves mapping, workflow, and session metadata from the repository. It extracts data from the mapping sources and stores the data in memory while it applies the transformation rules configured in the mapping. The PowerCenter Integration Service loads the transformed data into one or more targets.

To move data from sources to targets, the PowerCenter Integration Service uses the following components:

- PowerCenter Integration Service process. The PowerCenter Integration Service starts one or more PowerCenter Integration Service processes to run and monitor workflows. When you run a workflow, the PowerCenter Integration Service process starts and locks the workflow, runs the workflow tasks, and starts the process to run sessions.
- Load Balancer. The PowerCenter Integration Service uses the Load Balancer to dispatch tasks. The Load Balancer dispatches tasks to achieve optimal performance. It may dispatch tasks to a single node or across the nodes in a grid.

- Data Transformation Manager (DTM) process. The PowerCenter Integration Service starts a DTM process to run each Session and Command task within a workflow. The DTM process performs session validations, creates threads to initialize the session, read, write, and transform data, and handles pre- and post- session operations.

The PowerCenter Integration Service can achieve high performance using symmetric multi-processing systems. It can start and run multiple tasks concurrently. It can also concurrently process partitions within a single session. When you create multiple partitions within a session, the PowerCenter Integration Service creates multiple database connections to a single source and extracts a separate range of data for each connection. It also transforms and loads the data in parallel.

PowerCenter Integration Service Connectivity

The PowerCenter Integration Service is a repository client. It connects to the PowerCenter Repository Service to retrieve workflow and mapping metadata from the repository database. When the PowerCenter Integration Service process requests a repository connection, the request is routed through the master gateway, which sends back PowerCenter Repository Service information to the PowerCenter Integration Service process. The PowerCenter Integration Service process connects to the PowerCenter Repository Service. The PowerCenter Repository Service connects to the repository and performs repository metadata transactions for the client application.

The PowerCenter Workflow Manager communicates with the PowerCenter Integration Service process over a TCP/IP connection. The PowerCenter Workflow Manager communicates with the PowerCenter Integration Service process each time you schedule or edit a workflow, display workflow details, and request workflow and session logs. Use the connection information defined for the domain to access the PowerCenter Integration Service from the PowerCenter Workflow Manager.

The PowerCenter Integration Service process connects to the source or target database using ODBC or native drivers. The PowerCenter Integration Service process maintains a database connection pool for stored procedures or lookup databases in a workflow. The PowerCenter Integration Service process allows an unlimited number of connections to lookup or stored procedure databases. If a database user does not have permission for the number of connections a session requires, the session fails. You can optionally set a parameter to limit the database connections. For a session, the PowerCenter Integration Service process holds the connection as long as it needs to read data from source tables or write data to target tables.

The following table summarizes the software you need to connect the PowerCenter Integration Service to the platform components, source databases, and target databases:

Note: Both the Windows and UNIX versions of the PowerCenter Integration Service can use ODBC drivers to connect to databases. Use native drivers to improve performance.

PowerCenter Integration Service Process

The PowerCenter Integration Service starts a PowerCenter Integration Service process to run and monitor workflows. The PowerCenter Integration Service process is also known as the pmserver process. The PowerCenter Integration Service process accepts requests from the PowerCenter Client and from *pmcmd*. It performs the following tasks:

- Manage workflow scheduling.
- Lock and read the workflow.

- Read the parameter file.
- Create the workflow log.
- Run workflow tasks and evaluates the conditional links connecting tasks.
- Start the DTM process or processes to run the session.
- Write historical run information to the repository.
- Send post-session email in the event of a DTM failure.

Manage PowerCenter Workflow Scheduling

The PowerCenter Integration Service process manages workflow scheduling in the following situations:

- When you start the PowerCenter Integration Service. When you start the PowerCenter Integration Service, it queries the repository for a list of workflows configured to run on it.
- When you save a workflow. When you save a workflow assigned to a PowerCenter Integration Service to the repository, the PowerCenter Integration Service process adds the workflow to or removes the workflow from the schedule queue.

Lock and Read the PowerCenter Workflow

When the PowerCenter Integration Service process starts a workflow, it requests an execute lock on the workflow from the repository. The execute lock allows the PowerCenter Integration Service process to run the workflow and prevents you from starting the workflow again until it completes. If the workflow is already locked, the PowerCenter Integration Service process cannot start the workflow. A workflow may be locked if it is already running.

The PowerCenter Integration Service process also reads the workflow from the repository at workflow run time. The PowerCenter Integration Service process reads all links and tasks in the workflow except sessions and worklet instances. The PowerCenter Integration Service process reads session instance information from the repository. The DTM retrieves the session and mapping from the repository at session run time. The PowerCenter Integration Service process reads worklets from the repository when the worklet starts.

Read the Parameter File

When the workflow starts, the PowerCenter Integration Service process checks the workflow properties for use of a parameter file. If the workflow uses a parameter file, the PowerCenter Integration Service process reads the parameter file and expands the variable values for the workflow and any worklets invoked by the workflow.

The parameter file can also contain mapping parameters and variables and session parameters for sessions in the workflow, as well as service and service process variables for the service process that runs the workflow. When starting the DTM, the PowerCenter Integration Service process passes the parameter file name to the DTM.

Create the PowerCenter Workflow Log

The PowerCenter Integration Service process creates a log for the PowerCenter workflow. The workflow log contains a history of the workflow run, including initialization, workflow task status, and error messages. You can use information in the workflow log in conjunction with the PowerCenter Integration Service log and session log to troubleshoot system, workflow, or session problems.

Run the PowerCenter Workflow Tasks

The PowerCenter Integration Service process runs workflow tasks according to the conditional links connecting the tasks. Links define the order of execution for workflow tasks. When a task in the workflow completes, the PowerCenter Integration Service process evaluates the completed task according to specified conditions, such as success or failure. Based on the result of the evaluation, the PowerCenter Integration Service process runs successive links and tasks.

Run the PowerCenter Workflows Across the Nodes in a Grid

When you run a PowerCenter Integration Service on a grid, the service processes run workflow tasks across the nodes of the grid. The domain designates one service process as the master service process. The master service

process monitors the worker service processes running on separate nodes. The worker service processes run workflows across the nodes in a grid.

Start the DTM Process

When the workflow reaches a session, the PowerCenter Integration Service process starts the DTM process. The PowerCenter Integration Service process provides the DTM process with session and parameter file information that allows the DTM to retrieve the session and mapping metadata from the repository. When you run a session on a grid, the worker service process starts multiple DTM processes that run groups of session threads.

When you use operating system profiles, the PowerCenter Integration Services starts the DTM process with the system user account you specify in the operating system profile.

Write Historical Information

The PowerCenter Integration Service process monitors the status of workflow tasks during the workflow run. When workflow tasks start or finish, the PowerCenter Integration Service process writes historical run information to the repository. Historical run information for tasks includes start and completion times and completion status. Historical run information for sessions also includes source read statistics, target load statistics, and number of errors. You can view this information using the PowerCenter Workflow Monitor.

Send Post-Session Email

The PowerCenter Integration Service process sends post-session email if the DTM terminates abnormally. The DTM sends post-session email in all other cases.

Load Balancer

The Load Balancer dispatches tasks to achieve optimal performance and scalability. When you run a workflow, the Load Balancer dispatches the Session, Command, and predefined Event-Wait tasks within the workflow. The Load Balancer matches task requirements with resource availability to identify the best node to run a task. It dispatches the task to a PowerCenter Integration Service process running on the node. It may dispatch tasks to a single node or across nodes.

The Load Balancer dispatches tasks in the order it receives them. When the Load Balancer needs to dispatch more Session and Command tasks than the PowerCenter Integration Service can run, it places the tasks it cannot run in a queue. When nodes become available, the Load Balancer dispatches tasks from the queue in the order determined by the workflow service level.

The following concepts describe Load Balancer functionality:

- Dispatch process. The Load Balancer performs several steps to dispatch tasks.
- Resources. The Load Balancer can use PowerCenter resources to determine if it can dispatch a task to a node.
- Resource provision thresholds. The Load Balancer uses resource provision thresholds to determine whether it can start additional tasks on a node.
- Dispatch mode. The dispatch mode determines how the Load Balancer selects nodes for dispatch.
- Service levels. When multiple tasks are waiting in the dispatch queue, the Load Balancer uses service levels to determine the order in which to dispatch tasks from the queue.

Dispatch Process

The Load Balancer uses different criteria to dispatch tasks depending on whether the PowerCenter Integration Service runs on a node or a grid.

Dispatch Tasks on a Node

When the PowerCenter Integration Service runs on a node, the Load Balancer performs the following steps to dispatch a task:

1. The Load Balancer checks resource provision thresholds on the node. If dispatching the task causes any threshold to be exceeded, the Load Balancer places the task in the dispatch queue, and it dispatches the task later.

   The Load Balancer checks different thresholds depending on the dispatch mode.
2. The Load Balancer dispatches all tasks to the node that runs the master PowerCenter Integration Service process.

Dispatch Tasks Across a Grid

When the PowerCenter Integration Service runs on a grid, the Load Balancer performs the following steps to determine on which node to run a task:

1. The Load Balancer verifies which nodes are currently running and enabled.
2. If you configure the PowerCenter Integration Service to check resource requirements, the Load Balancer identifies nodes that have the PowerCenter resources required by the tasks in the workflow.
3. The Load Balancer verifies that the resource provision thresholds on each candidate node are not exceeded. If dispatching the task causes a threshold to be exceeded, the Load Balancer places the task in the dispatch queue, and it dispatches the task later.

   The Load Balancer checks thresholds based on the dispatch mode.
4. The Load Balancer selects a node based on the dispatch mode.

Resources

You can configure the PowerCenter Integration Service to check the resources available on each node and match them with the resources required to run the task. If you configure the PowerCenter Integration Service to run on a grid and to check resources, the Load Balancer dispatches a task to a node where the required PowerCenter resources are available. For example, if a session uses an SAP source, the Load Balancer dispatches the session only to nodes where the SAP client is installed. If no available node has the required resources, the PowerCenter Integration Service fails the task.

You configure the PowerCenter Integration Service to check resources in the Administrator tool.

You define resources available to a node in the Administrator tool. You assign resources required by a task in the task properties.

The PowerCenter Integration Service writes resource requirements and availability information in the workflow log.

Resource Provision Thresholds

The Load Balancer uses resource provision thresholds to determine the maximum load acceptable for a node. The Load Balancer can dispatch a task to a node when dispatching the task does not cause the resource provision thresholds to be exceeded.

The Load Balancer checks the following thresholds:

- Maximum CPU Run Queue Length. The maximum number of runnable threads waiting for CPU resources on the node. The Load Balancer excludes the node if the maximum number of waiting threads is exceeded.

  The Load Balancer checks this threshold in metric-based and adaptive dispatch modes.

- Maximum Memory %. The maximum percentage of virtual memory allocated on the node relative to the total physical memory size. The Load Balancer excludes the node if dispatching the task causes this threshold to be exceeded.

  The Load Balancer checks this threshold in metric-based and adaptive dispatch modes.

- Maximum Processes. The maximum number of running processes allowed for each PowerCenter Integration Service process that runs on the node. The Load Balancer excludes the node if dispatching the task causes this threshold to be exceeded.

  The Load Balancer checks this threshold in all dispatch modes.

If all nodes in the grid have reached the resource provision thresholds before any PowerCenter task has been dispatched, the Load Balancer dispatches tasks one at a time to ensure that PowerCenter tasks are still executed.

You define resource provision thresholds in the node properties.

Related Topics:

- "Defining Resource Provision Thresholds" on page 357

Dispatch Mode

The dispatch mode determines how the Load Balancer selects nodes to distribute workflow tasks. The Load Balancer uses the following dispatch modes:

- Round-robin. The Load Balancer dispatches tasks to available nodes in a round-robin fashion. It checks the Maximum Processes threshold on each available node and excludes a node if dispatching a task causes the threshold to be exceeded. This mode is the least compute-intensive and is useful when the load on the grid is even and the tasks to dispatch have similar computing requirements.
- Metric-based. The Load Balancer evaluates nodes in a round-robin fashion. It checks all resource provision thresholds on each available node and excludes a node if dispatching a task causes the thresholds to be exceeded. The Load Balancer continues to evaluate nodes until it finds a node that can accept the task. This mode prevents overloading nodes when tasks have uneven computing requirements.
- Adaptive. The Load Balancer ranks nodes according to current CPU availability. It checks all resource provision thresholds on each available node and excludes a node if dispatching a task causes the thresholds to be exceeded. This mode prevents overloading nodes and ensures the best performance on a grid that is not heavily loaded.

When the Load Balancer runs in metric-based or adaptive mode, it uses task statistics to determine whether a task can run on a node. The Load Balancer averages statistics from the last three runs of the task to estimate the computing resources required to run the task. If no statistics exist in the repository, the Load Balancer uses default values.

In adaptive dispatch mode, the Load Balancer can use the CPU profile for the node to identify the node with the most computing resources.

You configure the dispatch mode in the domain properties.

Service Levels

Service levels establish priority among tasks that are waiting to be dispatched.

When the Load Balancer has more Session and Command tasks to dispatch than the PowerCenter Integration Service can run at the time, the Load Balancer places the tasks in the dispatch queue. When nodes become available, the Load Balancer dispatches tasks from the queue. The Load Balancer uses service levels to determine the order in which to dispatch tasks from the queue.

You create and edit service levels in the domain properties in the Administrator tool. You assign service levels to workflows in the workflow properties in the PowerCenter Workflow Manager.

Data Transformation Manager (DTM) Process

The PowerCenter Integration Service process starts the DTM process to run a session. The DTM process is also known as the pmdtm process. The DTM is the process associated with the session task.

Note: If you use operating system profiles, the PowerCenter Integration Service runs the DTM process as the operating system user you specify in the operating system profile.

Read the Session Information

The PowerCenter Integration Service process provides the DTM with session instance information when it starts the DTM. The DTM retrieves the mapping and session metadata from the repository and validates it.

Perform Pushdown Optimization

If the session is configured for pushdown optimization, the DTM runs an SQL statement to push transformation logic to the source or target database.

Create Dynamic Partitions

The DTM adds partitions to the session if you configure the session for dynamic partitioning. The DTM scales the number of session partitions based on factors such as source database partitions or the number of nodes in a grid.

Form Partition Groups

If you run a session on a grid, the DTM forms partition groups. A partition group is a group of reader, writer, and transformation threads that runs in a single DTM process. The DTM process forms partition groups and distributes them to worker DTM processes running on nodes in the grid.

Expand Variables and Parameters

If the workflow uses a parameter file, the PowerCenter Integration Service process sends the parameter file to the DTM when it starts the DTM. The DTM creates and expands session-level, service-level, and mapping-level variables and parameters.

Create the Session Log

The DTM creates logs for the session. The session log contains a complete history of the session run, including initialization, transformation, status, and error messages. You can use information in the session log in conjunction with the PowerCenter Integration Service log and the workflow log to troubleshoot system or session problems.

Validate Code Pages

The PowerCenter Integration Service processes data internally using the UCS-2 character set. When you disable data code page validation, the PowerCenter Integration Service verifies that the source query, target query, lookup database query, and stored procedure call text convert from the source, target, lookup, or stored procedure data code page to the UCS-2 character set without loss of data in conversion. If the PowerCenter Integration Service encounters an error when converting data, it writes an error message to the session log.

Verify Connection Object Permissions

After validating the session code pages, the DTM verifies permissions for connection objects used in the session. The DTM verifies that the user who started or scheduled the workflow has execute permissions for connection objects associated with the session.

Start Worker DTM Processes

The DTM sends a request to the PowerCenter Integration Service process to start worker DTM processes on other nodes when the session is configured to run on a grid.

Run Pre-Session Operations

After verifying connection object permissions, the DTM runs pre-session shell commands. The DTM then runs pre-session stored procedures and SQL commands.

Run the Processing Threads

After initializing the session, the DTM uses reader, transformation, and writer threads to extract, transform, and load data. The number of threads the DTM uses to run the session depends on the number of partitions configured for the session.

Run Post-Session Operations

After the DTM runs the processing threads, it runs post-session SQL commands and stored procedures. The DTM then runs post-session shell commands.

Send Post-Session Email

When the session finishes, the DTM composes and sends email that reports session completion or failure. If the DTM terminates abnormally, the PowerCenter Integration Service process sends post-session email.

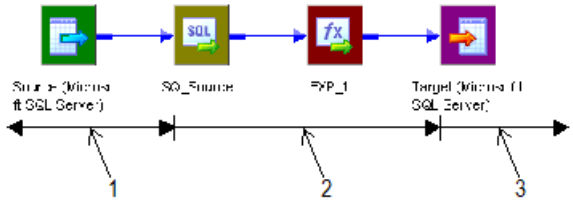
Processing Threads

The DTM allocates process memory for the session and divides it into buffers. This is also known as buffer memory. The DTM uses multiple threads to process data in a session. The main DTM thread is called the master thread.

The master thread creates and manages other threads. The master thread for a session can create mapping, pre-session, post-session, reader, transformation, and writer threads.

For each target load order group in a mapping, the master thread can create several threads. The types of threads depend on the session properties and the transformations in the mapping. The number of threads depends on the partitioning information for each target load order group in the mapping.

The following figure shows the threads the master thread creates for a simple mapping that contains one target load order group:



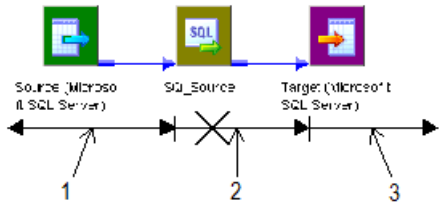
1. One reader thread.
2. One transformation thread.
3. One writer thread.

The mapping contains a single partition. In this case, the master thread creates one reader, one transformation, and one writer thread to process the data. The reader thread controls how the PowerCenter Integration Service

process extracts source data and passes it to the source qualifier, the transformation thread controls how the PowerCenter Integration Service process handles the data, and the writer thread controls how the PowerCenter Integration Service process loads data to the target.

When the pipeline contains *only* a source definition, source qualifier, and a target definition, the data bypasses the transformation threads, proceeding directly from the reader buffers to the writer. This type of pipeline is a pass-through pipeline.

The following figure shows the threads for a pass-through pipeline with one partition:



1. One reader thread.
2. Bypassed transformation thread.
3. One writer thread.

Thread Types

The master thread creates different types of threads for a session. The types of threads the master thread creates depend on the pre- and post-session properties, as well as the types of transformations in the mapping.

The master thread can create the following types of threads:

- Mapping threads
- Pre- and post-session threads
- Reader threads
- Transformation threads
- Writer threads

Mapping Threads

The master thread creates one mapping thread for each session. The mapping thread fetches session and mapping information, compiles the mapping, and cleans up after session execution.

Pre- and Post-Session Threads

The master thread creates one pre-session and one post-session thread to perform pre- and post-session operations.

Reader Threads

The master thread creates reader threads to extract source data. The number of reader threads depends on the partitioning information for each pipeline. The number of reader threads equals the number of partitions. Relational sources use relational reader threads, and file sources use file reader threads.

The PowerCenter Integration Service creates an SQL statement for each reader thread to extract data from a relational source. For file sources, the PowerCenter Integration Service can create multiple threads to read a single source.

Transformation Threads

The master thread creates one or more transformation threads for each partition. Transformation threads process data according to the transformation logic in the mapping.

The master thread creates transformation threads to transform data received in buffers by the reader thread, move the data from transformation to transformation, and create memory caches when necessary. The number of transformation threads depends on the partitioning information for each pipeline.

Transformation threads store transformed data in a buffer drawn from the memory pool for subsequent access by the writer thread.

If the pipeline contains a Rank, Joiner, Aggregator, Sorter, or a cached Lookup transformation, the transformation thread uses cache memory until it reaches the configured cache size limits. If the transformation thread requires more space, it pages to local cache files to hold additional data.

When the PowerCenter Integration Service runs in ASCII mode, the transformation threads pass character data in single bytes. When the PowerCenter Integration Service runs in Unicode mode, the transformation threads use double bytes to move character data.

Writer Threads

The master thread creates writer threads to load target data. The number of writer threads depends on the partitioning information for each pipeline. If the pipeline contains one partition, the master thread creates one writer thread. If it contains multiple partitions, the master thread creates multiple writer threads.

Each writer thread creates connections to the target databases to load data. If the target is a file, each writer thread creates a separate file. You can configure the session to merge these files.

If the target is relational, the writer thread takes data from buffers and commits it to session targets. When loading targets, the writer commits data based on the commit interval in the session properties. You can configure a session to commit data based on the number of source rows read, the number of rows written to the target, or the number of rows that pass through a transformation that generates transactions, such as a Transaction Control transformation.

Pipeline Partitioning

When running sessions, the PowerCenter Integration Service process can achieve high performance by partitioning the pipeline and performing the extract, transformation, and load for each partition in parallel. To accomplish this, use the following session and PowerCenter Integration Service configuration:

- Configure the session with multiple partitions.
- Install the PowerCenter Integration Service on a machine with multiple CPUs.

You can configure the partition type at most transformations in the pipeline. The PowerCenter Integration Service can partition data using round-robin, hash, key-range, database partitioning, or pass-through partitioning.

You can also configure a session for dynamic partitioning to enable the PowerCenter Integration Service to set partitioning at run time. When you enable dynamic partitioning, the PowerCenter Integration Service scales the number of session partitions based on factors such as the source database partitions or the number of nodes in a grid.

For relational sources, the PowerCenter Integration Service creates multiple database connections to a single source and extracts a separate range of data for each connection.

The PowerCenter Integration Service transforms the partitions concurrently, it passes data between the partitions as needed to perform operations such as aggregation. When the PowerCenter Integration Service loads relational data, it creates multiple database connections to the target and loads partitions of data concurrently. When the PowerCenter Integration Service loads data to file targets, it creates a separate file for each partition. You can choose to merge the target files.

DTM Processing

When you run a session, the DTM process reads source data and passes it to the transformations for processing. To help understand DTM processing, consider the following DTM process actions:

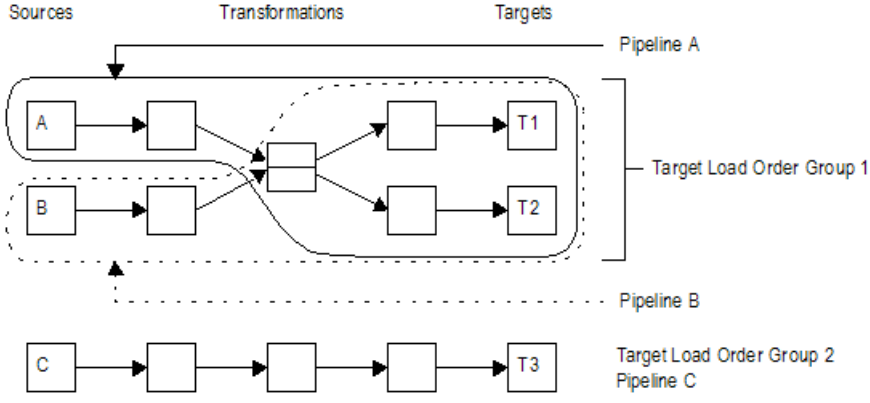
- Reading source data. The DTM reads the sources in a mapping at different times depending on how you configure the sources, transformations, and targets in the mapping.
- Blocking data. The DTM sometimes blocks the flow of data at a transformation in the mapping while it processes a row of data from a different source.
- Block processing. The DTM reads and processes a block of rows at a time.

Reading Source Data

Mappings contain one or more target load order groups. A target load order group is the collection of source qualifiers, transformations, and targets linked together in a mapping. Each target load order group contains one or more source pipelines. A source pipeline consists of a source qualifier and all of the transformations and target instances that receive data from that source qualifier.

By default, the DTM reads sources in a target load order group concurrently, and it processes target load order groups sequentially. You can configure the order that the DTM processes target load order groups.

The following figure shows a mapping that contains two target load order groups and three source pipelines:



In the mapping, the DTM processes the target load order groups sequentially. It first processes Target Load Order Group 1 by reading Source A and Source B at the same time. When it finishes processing Target Load Order Group 1, the DTM begins to process Target Load Order Group 2 by reading Source C.

Blocking Data

You can include multiple input group transformations in a mapping. The DTM passes data to the input groups concurrently. However, sometimes the transformation logic of a multiple input group transformation requires that the DTM block data on one input group while it waits for a row from a different input group.

Blocking is the suspension of the data flow into an input group of a multiple input group transformation. When the DTM blocks data, it reads data from the source connected to the input group until it fills the reader and transformation buffers. After the DTM fills the buffers, it does not read more source rows until the transformation logic allows the DTM to stop blocking the source. When the DTM stops blocking a source, it processes the data in the buffers and continues to read from the source.

The DTM blocks data at one input group when it needs a specific row from a different input group to perform the transformation logic. After the DTM reads and processes the row it needs, it stops blocking the source.

Block Processing

The DTM reads and processes a block of rows at a time. The number of rows in the block depend on the row size and the DTM buffer size. In the following circumstances, the DTM processes one row in a block:

- Log row errors. When you log row errors, the DTM processes one row in a block.
- Connect CURRVAL. When you connect the CURRVAL port in a Sequence Generator transformation, the session processes one row in a block. For optimal performance, connect only the NEXTVAL port in mappings.
- Configure array-based mode for Custom transformation procedure. When you configure the data access mode for a Custom transformation procedure to be row-based, the DTM processes one row in a block. By default, the data access mode is array-based, and the DTM processes multiple rows in a block.

Grids

When you run a PowerCenter Integration Service on a grid, a master service process runs on one node and worker service processes run on the remaining nodes in the grid. The master service process runs the workflow and workflow tasks, and it distributes the Session, Command, and predefined Event-Wait tasks to itself and other nodes. A DTM process runs on each node where a session runs. If you run a session on a grid, a worker service process can run multiple DTM processes on different nodes to distribute session threads.

Workflow on a Grid

When you run a workflow on a grid, the PowerCenter Integration Service designates one service process as the master service process, and the service processes on other nodes as worker service processes. The master service process can run on any node in the grid.

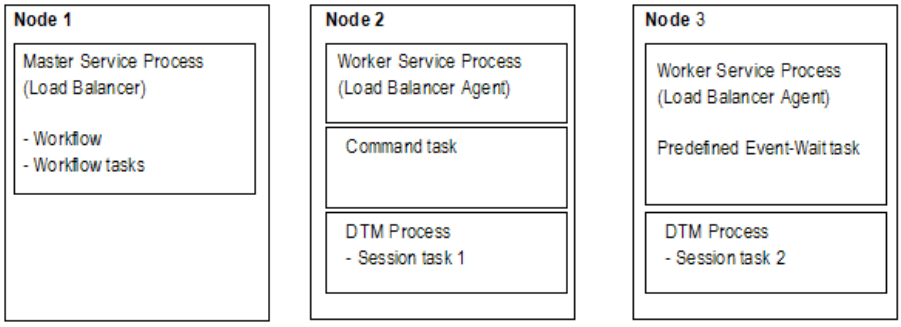
The master service process receives requests, runs the workflow and workflow tasks including the Scheduler, and communicates with worker service processes on other nodes. Because it runs on the master service process node, the Scheduler uses the date and time for the master service process node to start scheduled workflows. The master service process also runs the Load Balancer, which dispatches tasks to nodes in the grid.

Worker service processes running on other nodes act as Load Balancer agents. The worker service process runs predefined Event-Wait tasks within its process. It starts a process to run Command tasks and a DTM process to run Session tasks.

The master service process can also act as a worker service process. So the Load Balancer can distribute Session, Command, and predefined Event-Wait tasks to the node that runs the master service process or to other nodes.

For example, you have a workflow that contains two Session tasks, a Command task, and a predefined Event-Wait task.

The following figure shows an example of service process distribution when you run the workflow on a grid:



When you run the workflow on a grid, the PowerCenter Integration Service process distributes the tasks in the following way:

- On Node 1, the master service process starts the workflow and runs workflow tasks other than the Session, Command, and predefined Event-Wait tasks. The Load Balancer dispatches the Session, Command, and predefined Event-Wait tasks to other nodes.
- On Node 2, the worker service process starts a process to run a Command task and starts a DTM process to run Session task 1.
- On Node 3, the worker service process runs a predefined Event-Wait task and starts a DTM process to run Session task 2.

Session on a Grid

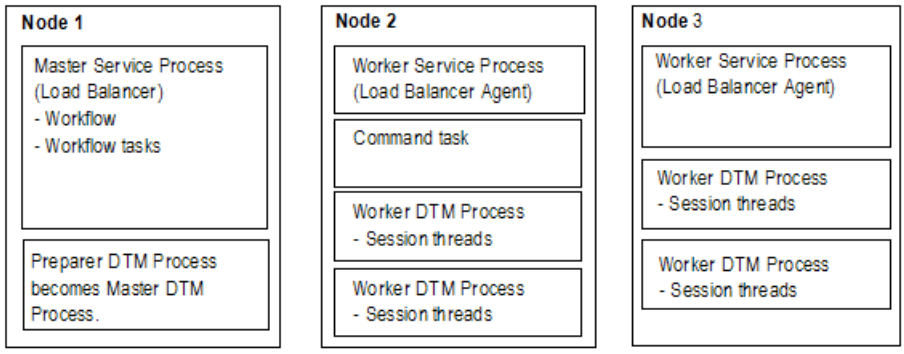
When you run a session on a grid, the master service process runs the workflow and workflow tasks, including the Scheduler. Because it runs on the master service process node, the Scheduler uses the date and time for the master service process node to start scheduled workflows. The Load Balancer distributes Command tasks as it does when you run a workflow on a grid. In addition, when the Load Balancer dispatches a Session task, it distributes the session threads to separate DTM processes.

The master service process starts a temporary preparer DTM process that fetches the session and prepares it to run. After the preparer DTM process prepares the session, it acts as the master DTM process, which monitors the DTM processes running on other nodes.

The worker service processes start the worker DTM processes on other nodes. The worker DTM runs the session. Multiple worker DTM processes running on a node might be running multiple sessions or multiple partition groups from a single session depending on the session configuration.

For example, you run a workflow on a grid that contains one Session task and one Command task. You also configure the session to run on the grid.

The following figure shows the service process and DTM distribution when you run a session on a grid:



When the PowerCenter Integration Service process runs the session on a grid, it performs the following tasks:

- On Node 1, the master service process runs workflow tasks. It also starts a temporary preparer DTM process, which becomes the master DTM process. The Load Balancer dispatches the Command task and session threads to nodes in the grid.
- On Node 2, the worker service process runs the Command task and starts the worker DTM processes that run the session threads.
- On Node 3, the worker service process starts the worker DTM processes that run the session threads.

System Resources

To allocate system resources for read, transformation, and write processing, you should understand how the PowerCenter Integration Service allocates and uses system resources. The PowerCenter Integration Service uses the following system resources:

- CPU usage
- DTM buffer memory
- Cache memory

CPU Usage

The PowerCenter Integration Service process performs read, transformation, and write processing for a pipeline in parallel. It can process multiple partitions of a pipeline within a session, and it can process multiple sessions in parallel.

If you have a symmetric multi-processing (SMP) platform, you can use multiple CPUs to concurrently process session data or partitions of data. This provides increased performance, as true parallelism is achieved. On a single processor platform, these tasks share the CPU, so there is no parallelism.

The PowerCenter Integration Service process can use multiple CPUs to process a session that contains multiple partitions. The number of CPUs used depends on factors such as the number of partitions, the number of threads, the number of available CPUs, and amount or resources required to process the mapping.

DTM Buffer Memory

The PowerCenter Integration Service process launches the DTM. The DTM allocates buffer memory to the session based on the DTM Buffer Size setting in the session properties. By default, the PowerCenter Integration Service determines the size of the buffer memory. However, you may want to configure the buffer memory and buffer block size manually.

The DTM divides the memory into buffer blocks as configured in the Buffer Block Size setting in the session properties. The reader, transformation, and writer threads use buffer blocks to move data from sources and to targets.

You can sometimes improve session performance by increasing buffer memory when you run a session handling a large volume of character data and the PowerCenter Integration Service runs in Unicode mode. In Unicode mode, the PowerCenter Integration Service uses double bytes to move characters, so increasing buffer memory might improve session performance.

If the DTM cannot allocate the configured amount of buffer memory for the session, the session cannot initialize. Informatica recommends you allocate no more than 1 GB for DTM buffer memory.

Cache Memory

The DTM process creates in-memory index and data caches to temporarily store data used by the following transformations:

- Aggregator transformation (without sorted input)
- Rank transformation
- Joiner transformation
- Lookup transformation (with caching enabled)

You can configure memory size for the index and data cache in the transformation properties. By default, the PowerCenter Integration Service determines the amount of memory to allocate for caches. However, you can manually configure a cache size for the data and index caches.

By default, the DTM creates cache files in the directory configured for the $PMCacheDir service process variable. If the DTM requires more space than it allocates, it pages to local index and data files.

The DTM process also creates an in-memory cache to store data for the Sorter transformations and XML targets. You configure the memory size for the cache in the transformation properties. By default, the PowerCenter Integration Service determines the cache size for the Sorter transformation and XML target at run time. The PowerCenter Integration Service allocates a minimum value of 16,777,216 bytes for the Sorter transformation cache and 10,485,760 bytes for the XML target. The DTM creates cache files in the directory configured for the $PMTempDir service process variable. If the DTM requires more cache space than it allocates, it pages to local cache files.

When processing large amounts of data, the DTM may create multiple index and data files. The session does not fail if it runs out of cache memory and pages to the cache files. It does fail, however, if the local directory for cache files runs out of disk space.

After the session completes, the DTM releases memory used by the index and data caches and deletes any index and data files. However, if the session is configured to perform incremental aggregation or if a Lookup transformation is configured for a persistent lookup cache, the DTM saves all index and data cache information to disk for the next session run.

Code Pages and Data Movement Modes

You can configure PowerCenter to move single byte and multibyte data. The PowerCenter Integration Service can move data in either ASCII or Unicode data movement mode. These modes determine how the PowerCenter Integration Service handles character data. You choose the data movement mode in the PowerCenter Integration Service configuration settings. If you want to move multibyte data, choose Unicode data movement mode. To ensure that characters are not lost during conversion from one code page to another, you must also choose the appropriate code pages for your connections.

ASCII Data Movement Mode

Use ASCII data movement mode when all sources and targets are 7-bit ASCII or EBCDIC character sets. In ASCII mode, the PowerCenter Integration Service recognizes 7-bit ASCII and EBCDIC characters and stores each character in a single byte. When the PowerCenter Integration Service runs in ASCII mode, it does not validate session code pages. It reads all character data as ASCII characters and does not perform code page conversions. It also treats all numerics as U.S. Standard and all dates as binary data.

You can also use ASCII data movement mode when sources and targets are 8-bit ASCII.

Unicode Data Movement Mode

Use Unicode data movement mode when sources or targets use 8-bit or multibyte character sets and contain character data. In Unicode mode, the PowerCenter Integration Service recognizes multibyte character sets as defined by supported code pages.

If you configure the PowerCenter Integration Service to validate data code pages, the PowerCenter Integration Service validates source and target code page compatibility when you run a session. If you configure the PowerCenter Integration Service for relaxed data code page validation, the PowerCenter Integration Service lifts source and target compatibility restrictions.

The PowerCenter Integration Service converts data from the source character set to UCS-2 before processing, processes the data, and then converts the UCS-2 data to the target code page character set before loading the data. The PowerCenter Integration Service allots two bytes for each character when moving data through a mapping. It also treats all numerics as U.S. Standard and all dates as binary data.

The PowerCenter Integration Service code page must be a subset of the PowerCenter repository code page.

Output Files and Caches

The PowerCenter Integration Service process generates output files when you run workflows and sessions. By default, the PowerCenter Integration Service logs status and error messages to log event files. Log event files are binary files that the Log Manager uses to display log events. During each session, the PowerCenter Integration Service also creates a reject file. Depending on transformation cache settings and target types, the PowerCenter Integration Service may create additional files as well.

The PowerCenter Integration Service stores output files and caches based on the service process variable settings. Generate output files and caches in a specified directory by setting service process variables in the session or workflow properties, PowerCenter Integration Service properties, a parameter file, or an operating system profile.

If you define service process variables in more than one place, the PowerCenter Integration Service reviews the precedence of each setting to determine which service process variable setting to use:

1. PowerCenter Integration Service process properties. Service process variables set in the PowerCenter Integration Service process properties contain the default setting.
2. Operating system profile. Service process variables set in an operating system profile override service process variables set in the PowerCenter Integration Service properties. If you use operating system profiles, the PowerCenter Integration Service saves workflow recovery files to the $PMStorageDir configured in the PowerCenter Integration Service process properties. The PowerCenter Integration Service saves session recovery files to the $PMStorageDir configured in the operating system profile.
3. Parameter file. Service process variables set in parameter files override service process variables set in the PowerCenter Integration Service process properties or an operating system profile.
4. Session or workflow properties. Service process variables set in the session or workflow properties override service process variables set in the PowerCenter Integration Service properties, a parameter file, or an operating system profile.

For example, if you set the $PMSessionLogFile in the operating system profile and in the session properties, the PowerCenter Integration Service uses the location specified in the session properties.

The PowerCenter Integration Service creates the following output files:

- Workflow log
- Session log
- Session details file
- Performance details file
- Reject files
- Row error logs
- Recovery tables and files
- Control file
- Post-session email
- Output file
- Cache files

When the PowerCenter Integration Service process on UNIX creates any file other than a recovery file, it sets the file permissions according to the umask of the shell that starts the PowerCenter Integration Service process. For example, when the umask of the shell that starts the PowerCenter Integration Service process is 022, the PowerCenter Integration Service process creates files with rw-r--r-- permissions. To change the file permissions, you must change the umask of the shell that starts the PowerCenter Integration Service process and then restart it.

The PowerCenter Integration Service process on UNIX creates recovery files with rw------- permissions.

The PowerCenter Integration Service process on Windows creates files with read and write permissions.

Workflow Log

The PowerCenter Integration Service process creates a workflow log for each workflow it runs. It writes information in the workflow log such as initialization of processes, workflow task run information, errors encountered, and workflow run summary. Workflow log error messages are categorized into severity levels. You can configure the PowerCenter Integration Service to suppress writing messages to the workflow log file. You can view workflow logs from the PowerCenter Workflow Monitor. You can also configure the workflow to write events to a log file in a specified directory.

As with PowerCenter Integration Service logs and session logs, the PowerCenter Integration Service process enters a code number into the workflow log file message along with message text.

Session Log

The PowerCenter Integration Service process creates a session log for each session it runs. It writes information in the session log such as initialization of processes, session validation, creation of SQL commands for reader and writer threads, errors encountered, and load summary. The amount of detail in the session log depends on the tracing level that you set. You can view the session log from the PowerCenter Workflow Monitor. You can also configure the session to write the log information to a log file in a specified directory.

As with PowerCenter Integration Service logs and workflow logs, the PowerCenter Integration Service process enters a code number along with message text.

Session Details

When you run a session, the PowerCenter Workflow Manager creates session details that provide load statistics for each target in the mapping. You can monitor session details during the session or after the session completes. Session details include information such as table name, number of rows written or rejected, and read and write throughput. To view session details, double-click the session in the PowerCenter Workflow Monitor.

Performance Detail File

The PowerCenter Integration Service process generates performance details for session runs. The PowerCenter Integration Service process writes the performance details to a file. The file stores performance details for the last session run.

You can review a performance details file to determine where session performance can be improved. Performance details provide transformation-by-transformation information on the flow of data through the session.

You can also view performance details in the PowerCenter Workflow Monitor if you configure the session to collect performance details.

Reject Files

By default, the PowerCenter Integration Service process creates a reject file for each target in the session. The reject file contains rows of data that the writer does not write to targets.

The writer may reject a row in the following circumstances:

- It is flagged for reject by an Update Strategy or Custom transformation.
- It violates a database constraint such as primary key constraint.
- A field in the row was truncated or overflowed, and the target database is configured to reject truncated or overflowed data.

By default, the PowerCenter Integration Service process saves the reject file in the directory entered for the service process variable $PMBadFileDir in the PowerCenter Workflow Manager, and names the reject file *target_table_name*.bad.

Note: If you enable row error logging, the PowerCenter Integration Service process does not create a reject file.

Row Error Logs

When you configure a session, you can choose to log row errors in a central location. When a row error occurs, the PowerCenter Integration Service process logs error information that allows you to determine the cause and source of the error. The PowerCenter Integration Service process logs information such as source name, row ID, current row data, transformation, timestamp, error code, error message, repository name, folder name, session name, and mapping information.

When you enable flat file logging, by default, the PowerCenter Integration Service process saves the file in the directory entered for the service process variable $PMBadFileDir.

Recovery Tables Files

The PowerCenter Integration Service process creates recovery tables on the target database system when it runs a session enabled for recovery. When you run a session in recovery mode, the PowerCenter Integration Service process uses information in the recovery tables to complete the session.

When the PowerCenter Integration Service process performs recovery, it restores the state of operations to recover the workflow from the point of interruption. The workflow state of operations includes information such as active service requests, completed and running status, workflow variable values, running workflows and sessions, and workflow schedules.

Control File

When you run a session that uses an external loader, the PowerCenter Integration Service process creates a control file and a target flat file. The control file contains information about the target flat file such as data format and loading instructions for the external loader. The control file has an extension of .ctl. The PowerCenter Integration Service process creates the control file and the target flat file in the PowerCenter Integration Service variable directory, $PMTargetFileDir, by default.

Email

You can compose and send email messages by creating an Email task in the Workflow Designer or Task Developer. You can place the Email task in a workflow, or you can associate it with a session. The Email task allows you to automatically communicate information about a workflow or session run to designated recipients.

Email tasks in the workflow send email depending on the conditional links connected to the task. For post-session email, you can create two different messages, one to be sent if the session completes successfully, the other if the session fails. You can also use variables to generate information about the session name, status, and total rows loaded.

Indicator File

If you use a flat file as a target, you can configure the PowerCenter Integration Service to create an indicator file for target row type information. For each target row, the indicator file contains a number to indicate whether the row was marked for insert, update, delete, or reject. The PowerCenter Integration Service process names this file *target_name*.ind and stores it in the PowerCenter Integration Service variable directory, $PMTargetFileDir, by default.

Output File

If the session writes to a target file, the PowerCenter Integration Service process creates the target file based on a file target definition. By default, the PowerCenter Integration Service process names the target file based on the target definition name. If a mapping contains multiple instances of the same target, the PowerCenter Integration Service process names the target files based on the target instance name.

The PowerCenter Integration Service process creates this file in the PowerCenter Integration Service variable directory, $PMTargetFileDir, by default.

Cache Files

When the PowerCenter Integration Service process creates memory cache, it also creates cache files. The PowerCenter Integration Service process creates cache files for the following mapping objects:

- Aggregator transformation
- Joiner transformation
- Rank transformation
- Lookup transformation
- Sorter transformation
- XML target

By default, the DTM creates the index and data files for Aggregator, Rank, Joiner, and Lookup transformations and XML targets in the directory configured for the $PMCacheDir service process variable. The PowerCenter Integration Service process names the index file PM*.idx, and the data file PM*.dat. The PowerCenter Integration Service process creates the cache file for a Sorter transformation in the $PMTempDir service process variable directory.

Incremental Aggregation Files

If the session performs incremental aggregation, the PowerCenter Integration Service process saves index and data cache information to disk when the session finished. The next time the session runs, the PowerCenter Integration Service process uses this historical information to perform the incremental aggregation. By default, the DTM creates the index and data files in the directory configured for the $PMCacheDir service process variable. The PowerCenter Integration Service process names the index file PMAGG*.dat and the data file PMAGG*.idx.

Persistent Lookup Cache

If a session uses a Lookup transformation, you can configure the transformation to use a persistent lookup cache. With this option selected, the PowerCenter Integration Service process saves the lookup cache to disk the first time it runs the session, and then uses this lookup cache during subsequent session runs. By default, the DTM creates the index and data files in the directory configured for the $PMCacheDir service process variable. If you do not name the files in the transformation properties, these files are named PMLKUP*.idx and PMLKUP*.dat.

CHAPTER 17

Model Repository Service

This chapter includes the following topics:

- Model Repository Service Overview, 243
- Model Repository Architecture, 243
- Model Repository Connectivity, 244
- Model Repository Database Requirements, 245
- Model Repository Service Status, 247
- Properties for the Model Repository Service, 248
- Properties for the Model Repository Service Process, 250
- Model Repository Service Management, 252
- Creating a Model Repository Service, 257

Model Repository Service Overview

The Model Repository Service manages the Model repository. The Model repository stores metadata created by Informatica products in a relational database to enable collaboration among the products. Informatica Developer, Informatica Analyst, Data Integration Service, and the Administrator tool store metadata in the Model repository.

Use the Administrator tool or the *infacmd* command line program to administer the Model Repository Service. Create one Model Repository Service for each Model repository. When you create a Model Repository Service, you can create a Model repository or use an existing Model repository. Manage users, groups, privileges, and roles on the Security tab of the Administrator tool. Manage permissions for Model repository objects in the Informatica Developer and the Informatica Analyst.

Because the Model Repository Service is not a highly available service and does not run on a grid, you assign each Model Repository Service to run on one node. If the Model Repository Service fails, it restarts on the same node. You can run multiple Model Repository Services on the same node.

Model Repository Architecture

The Model Repository Service process fetches, inserts, and updates metadata in the Model repository database tables. A Model Repository Service process is an instance of the Model Repository Service on the node where the Model Repository Service runs.

The Model Repository Service receives requests from the following client applications:

- Informatica Developer. Informatica Developer connects to the Model Repository Service to create, update, and delete objects. Informatica Developer and Informatica Analyst share objects in the Model repository.
- Informatica Analyst. Informatica Analyst connects to the Model Repository Service to create, update, and delete objects. Informatica Developer and Informatica Analyst client applications share objects in the Model repository.
- Data Integration Service. When you start a Data Integration Service, it connects to the Model Repository Service. The Data Integration Service connects to the Model Repository Service to run or preview project components. The Data Integration Service also connects to the Model Repository Service to store run-time metadata in the Model repository. Application configuration and objects within an application are examples of run-time metadata.

Note: A Model Repository Service can be associated with one Analyst Service and multiple Data Integration Services.

Model Repository Schema

The Model repository contains a design-time schema and a run-time schema. The objects stored in the design-time schema are managed by Informatica Developer and Informatica Analyst.

When you deploy an application to the Data Integration Service, the Deployment Manager copies objects in the application to the run-time schema of the Model Repository Service associated with the Data Integration Service.

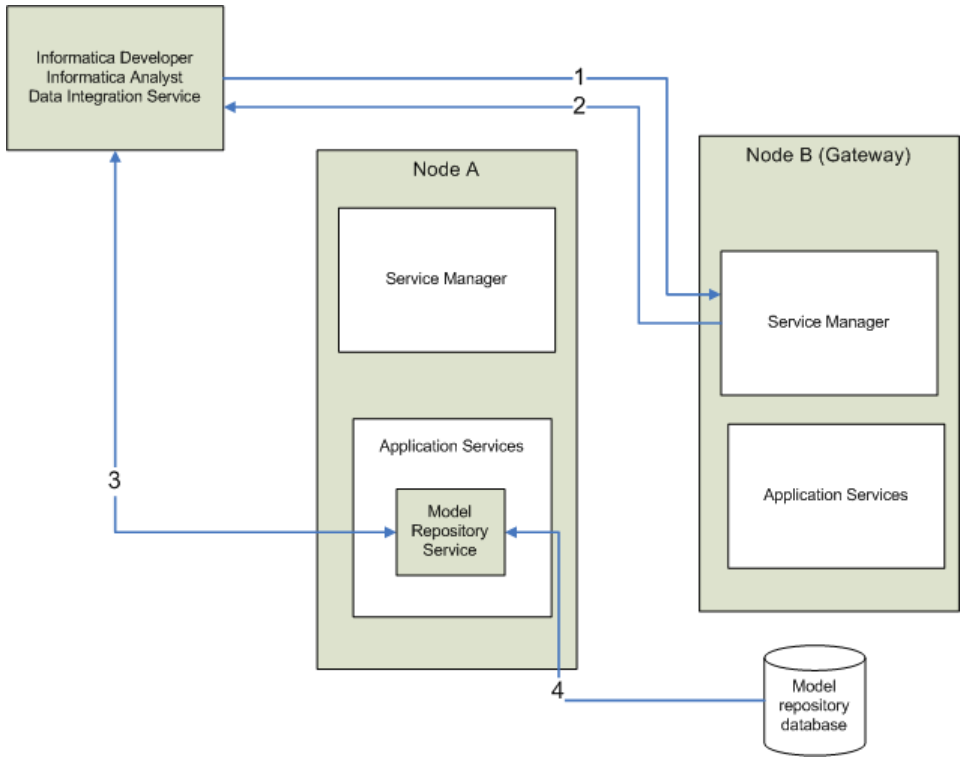
The Model repository stores the run-time metadata for each Data Integration Service separately. Data Integration Services cannot share run-time metadata. Run-time metadata includes applications and application configuration.

Each application in a Model repository is stored separately. If you replace or redeploy an application, the previous version is deleted from the repository. If you rename an application, the previous application remains in the Model repository.

Model Repository Connectivity

The Model Repository Service connects to the Model repository using JDBC drivers. Informatica Developer, Informatica Analyst, Informatica Administrator, and the Data Integration Service communicate with the Model Repository Service over TCP/IP. Informatica Developer, Informatica Analyst, and Data Integration Service are Model repository clients.

The following figure shows how a Model repository client connects to the Model repository database:



1. A Model repository client sends a repository connection request to the master gateway node, which is the entry point to the domain.
2. The Service Manager sends back the host name and port number of the node running the Model Repository Service. In the diagram, the Model Repository Service is running on node A.
3. The repository client establishes a TCP/IP connection with the Model Repository Service process on node A.
4. The Model Repository Service process communicates with the Model repository database and performs repository metadata transactions for the client. This communication occurs over JDBC.

Note: The Model repository tables have an open architecture. Although you can view the repository tables, never manually edit them through other utilities. Informatica is not responsible for corrupted data that is caused by customer alteration of the repository tables or data within those tables.

Model Repository Database Requirements

Before you create a repository, you need a database to store repository tables. Use the database client to create the database. After you create a database, you can use the Administrator tool to create a Model Repository Service.

Each Model repository must meet the following requirements:

- Each Model repository must have its own schema. Two Model repositories or the Model repository and the domain configuration database cannot share the same schema.
- Each Model repository must have a unique database name.

In addition, each Model repository must meet database-specific requirements.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2_SKIPINSERTED
  - DB2_EVALUNCOMMITTED
  - DB2_SKIPDELETED
  - AUTO_RUNSTATS
- On the database, set the following configuration parameters:

Parameter	Value
applheapsz	8192
appl_ctl_heap_sz	8192
logfilsiz	8000
DynamicSections	1000
maxlocks	98
locklist	50000
auto_stmt_stats	ON For IBM DB2 9.5 only.

- Set the tablespace pageSize parameter to 32768.

  In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

  In a multi-partition database, you must specify a tablespace that meets the pageSize requirements.

  Define the tablespace on a single node.
- Verify the database user has CREATETAB and CONNECT privileges.

Note: The default value for DynamicSections in DB2 is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 1000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica. The following error message can appear:

```
[informatica][DB2 JDBC Driver]No more available statements. Please recreate your package with a larger
dynamicSections value.
```

IBM DB2 Version 9.1

If the Model repository is in an IBM DB2 9.1 database, run the DB2 reorgchk command to optimize database operations. The reorgchk command generates the database statistics used by the DB2 optimizer in queries and updates.

Use the following command:

```
REORGCHK UPDATE STATISTICS on SCHEMA <SchemaName>
```

Run the command on the database after you create the repository content.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the read committed isolation level to READ_COMMITTED_SNAPSHOT to minimize locking contention.

  To set the isolation level for the database, run the following command:

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  To verify that the isolation level for the database is correct, run the following command:

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW permissions.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the open_cursors parameter to 1000 or higher.
- Verify the database user has CONNECT, RESOURCE, and CREATE VIEW privileges.

Model Repository Service Status

Use the Administrator tool to enable or disable a service. You can enable the Model Repository Service after you create it. You can also enable a disabled service to make the service or application available again. When you enable the service, a service process starts on a node designated to run the service and the service is available to perform repository transactions. You can disable the service to perform maintenance or to temporarily restrict users from accessing the Model Repository Service or Model repository.

You must enable the Model Repository Service to perform the following tasks in the Administrator tool:

- Create, back up, restore, and delete Model repository content.
- Create and delete Model repository index.
- Manage permissions on the Model repository.

Enabling, Disabling, and Recycling the Model Repository Service

You can enable, disable, and recycle the Model Repository Service in the Administrator tool.

When you enable the Model Repository Service, the Administrator tool requires at least 256 MB of free memory. It may require up to one GB of free memory. If enough free memory is not available, the service may fail to start.

When you disable the Model Repository Service, you must choose the mode to disable it in. You can choose one of the following options:

- Complete. Allows the jobs to run to completion before disabling the service.
- Abort. Tries to stop all jobs before aborting them and disabling the service.

When you recycle the Model Repository Service, the Service Manager restarts the Model Repository Service.

To enable or disable the Model Repository Service:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the Model Repository Service.

3. On the Domain Actions menu, click Enable Service to enable the Model Repository Service.
   The Enable option does not appear when the service is enabled.
4. Or, on the Domain Actions menu, click Disable Service to disable the Model Repository Service.
   The Disable option does not appear when the service is disabled.
5. Or, on the Domain Actions menu, click Recycle Service to restart the Model Repository Service.

Properties for the Model Repository Service

Use the Administrator tool to configure the following service properties:

- General properties
- Repository database properties
- Search properties
- Advanced properties
- Cache properties
- Custom properties

General Properties for the Model Repository Service

The following table describes the general properties for the Model Repository Service:

Property	Description
Name	Name of the Model Repository Service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the Model Repository Service. The description cannot exceed 765 characters.
License	Not applicable to the Model Repository Service.
Node	Displays the node on which the Model Repository Service runs.

Repository Database Properties for the Model Repository Service

The following table describes the database properties for the Model Repository Service:

Property	Description
Database Type	The type of database.
Username	The database user name for the Model repository.
Password	An encrypted version of the database password for the Model repository.

Property	Description
JDBC Connect String	The JDBC connection string used to connect to the Model repository database. For example, the connection string for an Oracle database contains the following syntax: `jdbc:informatica:oracle://Cadillac:1521;SID=Marble;MaxPooledStatements=20;CatalogOptions=0` The connection string for IBM DB2 and Microsoft SQL Server uses DatabaseName, not SID.
Dialect	The SQL dialect for a particular database. The dialect maps java objects to database objects. For example: `org.hibernate.dialect.Oracle9Dialect` For more information about dialects, see the Hibernate documentation: https://www.hibernate.org/
Driver	The Data Direct driver used to connect to the database. For example: `com.informatica.jdbc.oracle.OracleDriver`
Database Schema	The schema name for a Microsoft SQL Server database.
Database Tablespace	The tablespace name for an IBM DB2 database. For a multi-partition IBM DB2 database, the tablespace must span a single node and a single partition.

Search Properties for the Model Repository Service

The following table describes the search properties for the Model Repository Service:

Property	Description

Search Analyzer	The fully qualified java class name of the search analyzer.
	Default is:
	`com.informatica.repository.service.provider.search.analysis.MMStandardAnalyzer`
	For example, specify the following java class name of the search analyzer for Chinese, Japanese and Korean languages:
	`org.apache.lucene.analysis.cjk.CJKAnalyzer`

Search Analyzer Factory	The fully qualified java class name of the factory class.

Advanced Properties for the Model Repository Service

The following table describes the Advanced properties for the Model Repository Service:

Property	Description
Maximum Heap Size	Amount of RAM allocated to the Java Virtual Machine (JVM) that runs the Model Repository Service. Use this property to increase the performance. Append one of the following letters to the value to specify the units: - b for bytes. - k for kilobytes. - m for megabytes. - g for gigabytes. Default is 1024 megabytes.
JVM Command Line Options	Java Virtual Machine (JVM) command line options to run Java-based programs. When you configure the JVM options, you must set the Java SDK classpath, Java SDK minimum memory, and Java SDK maximum memory properties.

Property	Description
	You must set the following JVM command line options: - Xms. Minimum heap size. Default value is 256 m. - MaxPermSize. Maximum permanent generation size. Default is 128 m. - Dfile.encoding. File encoding. Default is UTF-8.

Cache Properties for the Model Repository Service

The following table describes the cache properties for the Model Repository Service:

Property	Description
Enable Cache	Enables the Model Repository Service to store Model repository objects in cache memory. To apply changes, restart the Model Repository Service.
Cache JVM Options	JVM options for the Model Repository Service cache. To configure the amount of memory allocated to cache, configure the maximum heap size. This field must include the maximum heap size, specified by the -Xmx option. The default value and minimum value for the maximum heap size is -Xmx128m. The options you configure apply when Model Repository Service cache is enabled. To apply changes, restart the Model Repository Service. The options you configure in this field do not apply to the JVM that runs the Model Repository Service.

Custom Properties for the Model Repository Service

Custom properties include properties that are unique to your environment or that apply in special cases.

A Model Repository Service process does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Properties for the Model Repository Service Process

The Model Repository Service runs the Model Repository Service process on one node. When you select the Model Repository Service in the Administrator tool, you can view information about the Model Repository Service process on the Processes tab. You can also configure repository search and logging for the Model Repository Service process.

Note: You must select the node to view the service process properties in the Service Process Properties section.

Node Properties for the Model Repository Service Process

Use the Administrator tool to configure the following types of Model Repository Service process properties:

- Search properties
- Repository database properties
- Audit properties
- Repository properties
- Custom Properties

- Environment variables

Search Properties for the Model Repository Service Process

Search properties for the Model Repository Service process.

The following table describes the search properties for the Model Repository Service process:

Property	Description
Search Index Root Directory	The directory that contains the search analyzer index files. Default is: `./target/repository/1249674846269/prs/index`

Repository Database Properties for the Model Repository Service Process

Repository database properties for the Model Repository Service process.

The following table describes the repository database properties for the Model Repository Service process:

Property	Description
Hibernate Connection Pool Size	The hibernate connection pool size. Default is 10.
Hibernate C3P0 Max Size	The maximum hibernate C3P0 size. Default is 10.
Hibernate C3P0 Min Size	The minimum hibernate C3P0 size. Default is 1.
Hibernate C3P0 Max Statements	The maximum number hibernate C3P0 statements. Default is 500.
Activate Dump Persistence Configuration to File	Writes persistence configuration to a log file. The Model Repository Service logs information about the database schema, object relational mapping, repository schema change audit log, and registered IMF packages. The Model Repository Service creates the log file when the Model repository is enabled, created, or upgraded. The Model Repository Service stores the logs in the specified repository logging directory. If a repository logging directory is not specified, the Model Repository Service does not generate these log files. You must disable and re-enable the Model Repository Service after you change this option. Default is False.
Activate Log Persistence SQL to File	Writes parameterized SQL statements to a log file, which is stored in the specified repository logging directory. If a repository logging directory is not specified, the Model Repository Service does not generate these log files. You must disable and re-enable the Model Repository Service after you change this option. Default is False.

For more information about hibernate and persistence, see the Hibernate documentation:

`https://www.hibernate.org/`

Audit Properties for the Model Repository Service Process

Audit properties for the Model Repository Service process.

The following table describes the audit properties for the Model Repository Service process:

Property	Description
Audit Enabled	Displays audit logs in the Log Viewer. Default is False.

Repository Properties for the Model Repository Service Process

Repository properties for the Model Repository Service process.

The following table describes the repository properties for the Model Repository Service process:

Property	Description
Repository Logging Directory	The directory that stores logs for Dump Persistence Configuration or Log Persistence SQL. Do not specify a directory path to disable the logs. These logs are not the repository logs that appear in the Log Viewer. Default is blank.
Repository Logging Severity Level	The severity level for repository logs. Valid values are: fatal, error, warning, info, trace, and debug. Default is info.

Custom Properties for the Model Repository Service Process

Custom properties include properties that are unique to your environment or that apply in special cases.

A Model Repository Service process does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Environment Variables for the Model Repository Service Process

You can edit environment variables for a Model Repository Service process.

The following table describes the environment variables for the Model Repository Service process:

Property	Description
Environment Variables	Environment variables defined for the Model Repository Service process.

Model Repository Service Management

Use the Administrator tool to manage the Model Repository Service and the Model repository content. For example, you can use the Administrator tool to manage repository content, search, and repository logs.

Content Management for the Model Repository Service

When you create the Model Repository Service, you can create the repository content. Alternatively, you can create the Model Repository Service using existing repository content. The repository name is the same as the name of the Model Repository Service.

You can also delete the repository content. You may choose to delete repository content to delete a corrupted repository or to increase disk or database space.

Creating and Deleting Repository Content

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select the Model Repository Service.
3. To create the repository content, on the Domain Actions menu, click **Repository Contents** > **Create**.
4. Or, to delete repository content, on the Domain Actions menu, click **Repository Contents** > **Delete**.

Model Repository Backup and Restoration

Regularly back up repositories to prevent data loss due to hardware or software problems. When you back up a repository, the Model Repository Service saves the repository to a file, including the repository objects and the search index. If you need to recover the repository, you can restore the content of the repository from this file.

When you back up a repository, the Model Repository Service writes the file to the service backup directory. The service backup directory is a subdirectory of the node backup directory with the name of the Model Repository Service. For example, a Model Repository Service named MRS writes repository backup files to the following location:

```
<node_backup_directory>\MRS
```

You specify the node backup directory when you set up the node. View the general properties of the node to determine the path of the backup directory. The Model Repository Service uses the extension .mrep for all Model repository backup files.

To ensure that the Model Repository Service creates a consistent backup file, the backup operation blocks all other repository operations until the backup completes. You might want to schedule repository backups when users are not logged in.

Backing Up the Repository Content

You can back up the content of a Model repository to restore the repository content to another repository or to retain a copy of the repository.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select the Model Repository Service.
3. On the Domain Actions menu, click **Repository Contents** > **Back Up**.

   The **Back Up Repository Contents** dialog box appears.

4. Enter the following information:

Option	Description
Output File Name	Name of the output file.
Description	Description of the contents of the output file.

5. Click **Overwrite** to overwrite a file with the same name.
6. Click **OK**.

   The Model Repository Service writes the backup file to the service backup directory.

Restoring the Repository Content

You can restore repository content to a Model repository from a repository backup file.

Verify that the repository is empty. If the repository contains content, the restore option is disabled.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select the Model Repository Service.
3. On the Domain Actions menu, click **Repository Contents** > **Restore**.

   The **Restore Repository Contents** dialog box appears.
4. Select a backup file to restore.
5. Click **OK**.

Viewing Repository Backup Files

You can view the repository backup files written to the Model Repository Service backup directory.

1. On the Domain tab, select the **Services and Nodes** view.
2. In the Navigator, select the Model Repository Service.
3. On the Domain Actions menu, click **Repository Contents** > **View Backup Files**.

   The **View Repository Backup Files** dialog box appears and shows the backup files for the Model Repository Service.

Security Management for the Model Repository Service

You manage users, groups, privileges, and roles on the Security tab of the Administrator tool.

You manage permissions for repository objects in Informatica Developer and Informatica Analyst. Permissions control access to projects in the repository. Even if a user has the privilege to perform certain actions, the user may also require permission to perform the action on a particular object.

To secure data in the repository, you can create a project and assign permissions to it. When you create a project, you are the owner of the project by default. The owner has all permissions, which you cannot change. The owner can assign permissions to users or groups in the repository.

Search Management for the Model Repository Service

The Model Repository Service uses a search engine to index the metadata in the Model repository. To correctly index the metadata, the search engine uses a search analyzer appropriate for the language of the metadata that

you are indexing. The Developer tool and Analyst tool use the search engine to perform searches on objects in the Model repository.

The Model Repository Service is packaged with the following search analyzers:

- com.informatica.repository.service.provider.search.analysis.MMStandardAnalyzer. This is the search analyzer for English. This is the default search analyzer.
- org.apache.lucene.analysis.cjk.CJKAnalyzer. This is the search analyzer for Chinese, Japanese and Korean.

When you configure the Model Repository Service, you can change the default search analyzer. You can use one of the packaged search analyzers or a custom search analyzer.

To use a custom search analyzer, specify the name of either the search analyzer or search analyzer factory in the Model Repository Service properties. You specify the factory when the search analyzer requires configuration to run. The Model Repository Service uses the factory to connect to the search analyzer. If you use a factory, the factory class implementation must have a public method with the following signature:

```
public org.apache.lucene.analysis.Analyzer createAnalyzer(Properties settings)
```

You can also create, delete, and re-index the search index if the Model repository contains content and the search index is enabled. Re-index the search index every time you change the search analyzer.

Changing the Search Analyzer

1. Specify the name of the search analyzer or the search analyzer factory in the Model Repository Service search properties in the Administrator tool.
2. To use a custom search analyzer, place the search analyzer and required .jar files in the following Model Repository Service directory:

   ```
   <Informatica_Installation_Directory>\tomcat\bin\logs\PRSService\
   ```
3. Restart the Model Repository Service to apply the changes.
4. Re-index the search index.

Managing a Search Index

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the Model Repository Service.
3. On the Domain Actions menu, click Search Index > Create to create a search index.
4. Or, on the Domain Actions menu, click Search Index > Delete to delete the search index.
5. Or, on the Domain Actions menu, click Search Index > Re-Index to re-index the search index.

Repository Log Management for the Model Repository Service

The Model Repository Service generates repository logs. The repository logs contain repository messages of different severity levels, such as fatal, error, warning, info, trace, and debug. You can configure the level of detail that appears in the repository log files. You can also configure where the Model Repository Service stores the log files.

Configuring Repository Logging

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the Model Repository Service.
3. In the contents panel, select the **Processes** view.

4. Select the node.

   The service process details appear in the Service Process Properties section.
5. Click **Edit** in the Repository section.

   The Edit Processes page appears.
6. Enter the directory path in the **Repository Logging Directory** field.
7. Specify the level of logging in the **Repository Logging Severity Level** field.
8. Click OK.

Audit Log Management for Model Repository Service

The Model Repository Service can generate audit logs in the Log Viewer. The audit log provides information about the following types of operations performed on the Model repository:

- Logging in and out of the Model repository
- Creating a project
- Creating a folder

By default, audit logging is disabled.

Enabling and Disabling Audit Logging

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the Model Repository Service.
3. In the contents panel, select the Processes view.
4. Select the node.

   The service process details appear in the Service Process Properties section.
5. Click **Edit** in the Audit section.

   The Edit Processes page appears.
6. Enter one of the following values in the Audit Enabled field.
   - True. Enables audit logging.
   - False. Disables audit logging. Default is false.
7. Click OK.

Cache Management for the Model Repository Service

To improve Model Repository Service performance, you can configure the Model Repository Service to use cache memory. When you configure the Model Repository Service to use cache memory, the Model Repository Service stores objects that it reads from the Model repository in memory. The Model Repository Service can read the repository objects from memory instead of the Model repository. Reading objects from memory reduces the load on the database server and improves response time.

Model Repository Cache Processing

When the cache process starts, the Model Repository Service stores each object it reads in memory. When the Model Repository Service gets a request for an object from a client application, the Model Repository Service compares the object in memory with the object in the repository. If the latest version of the object is not in memory, the Model repository updates the cache and then returns the object to the client application that requested the

object. When the amount of memory allocated to cache is full, the Model Repository Service deletes the cache for least recently used objects to allocate space for another object.

The Model Repository Service cache process runs as a separate process. The Java Virtual Manager (JVM) that runs the Model Repository Service is not affected by the JVM options you configure for the Model Repository Service cache.

Configuring Cache

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the Model Repository Service.
3. Click **Edit** in the **Cache Properties** section.
4. Select **Enable Cache**.
5. Specify the amount of memory allocated to cache in the **Cache JVM Options** field.
6. Restart the Model Repository Service.
7. Verify that the cache process is running.
   The Model Repository Service logs display the following message when the cache process is running:

```
MRSI_35204 "Caching process has started on host [host name] at port [port number] with JVM options [JVM options]."
```

Creating a Model Repository Service

1. Create a database for the Model repository.
2. In the Administrator tool, click the Domain tab.
3. On the Domain Actions menu, click New > Model Repository Service.
4. In the properties view, enter the general properties for the Model Repository Service.
5. Click Next.
6. Enter the database properties for the Model Repository Service.
7. Click Test Connection to test the connection to the database.
8. Select one of the following options:
   - Do Not Create New Content. Select this option if the specified database already contains content for the Model repository. This is the default.
   - Create New Content. Select this option to create content for the Model repository in the specified database.
9. Click Finish.

CHAPTER 18

PowerCenter Repository Service

This chapter includes the following topics:

- PowerCenter Repository Service Overview, 258
- Creating a Database for the PowerCenter Repository, 259
- Creating the PowerCenter Repository Service, 259
- PowerCenter Repository Service Configuration, 262
- PowerCenter Repository Service Process Configuration, 266

PowerCenter Repository Service Overview

A PowerCenter repository is a collection of database tables containing metadata. A PowerCenter Repository Service manages the repository. It performs all metadata transactions between the repository database and repository clients.

Create a PowerCenter Repository Service to manage the metadata in repository database tables. Each PowerCenter Repository Service manages a single repository. You need to create a unique PowerCenter Repository Service for each repository in a Informatica domain.

Creating and configuring a PowerCenter Repository Service involves the following tasks:

- Create a database for the repository tables. Before you can create the repository tables, you need to create a database to store the tables. If you create a PowerCenter Repository Service for an existing repository, you do not need to create a new database. You can use the existing database, as long as it meets the minimum requirements for a repository database.
- Create the PowerCenter Repository Service. Create the PowerCenter Repository Service to manage the repository. When you create a PowerCenter Repository Service, you can choose to create the repository tables. If you do not create the repository tables, you can create them later or you can associate the PowerCenter Repository Service with an existing repository.
- Configure the PowerCenter Repository Service. After you create a PowerCenter Repository Service, you can configure its properties. You can configure properties such as the error severity level or maximum user connections.

Creating a Database for the PowerCenter Repository

Before you can manage a repository with a PowerCenter Repository Service, you need a database to hold the repository database tables. You can create the repository on any supported database system.

Use the database management system client to create the database. The repository database name must be unique. If you create a repository in a database with an existing repository, the create operation fails. You must delete the existing repository in the target database before creating the new repository.

To protect the repository and improve performance, do not create the repository on an overloaded machine. The machine running the repository database system must have a network connection to the node that runs the PowerCenter Repository Service.

Tip: You can optimize repository performance on IBM DB2 EEE databases when you store a PowerCenter repository in a single-node tablespace. When setting up an IBM DB2 EEE database, the database administrator must define the database on a single node.

Creating the PowerCenter Repository Service

Use the Administrator tool to create a PowerCenter Repository Service.

Before You Begin

Before you create a PowerCenter Repository Service, complete the following tasks:

- Determine repository requirements. Determine whether the repository needs to be version-enabled and whether it is a local, global, or standalone repository.
- Verify license. Verify that you have a valid license to run application services. Although you can create a PowerCenter Repository Service without a license, you need a license to run the service. In addition, you need a license to configure some options related to version control and high availability.
- Determine code page. Determine the code page to use for the PowerCenter repository. The PowerCenter Repository Service uses the character set encoded in the repository code page when writing data to the repository. The repository code page must be compatible with the code pages for the PowerCenter Client and all application services in the Informatica domain.

  Tip: After you create the PowerCenter Repository Service, you cannot change the code page in the PowerCenter Repository Service properties. To change the repository code page after you create the PowerCenter Repository Service, back up the repository and restore it to a new PowerCenter Repository Service. When you create the new PowerCenter Repository Service, you can specify a compatible code page.

Creating a PowerCenter Repository Service

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the folder where you want to create the PowerCenter Repository Service.

   Note: If you do not select a folder, you can move the PowerCenter Repository Service into a folder after you create it.
3. In the Domain Actions menu, click New > PowerCenter Repository Service.

   The Create New Repository Service dialog box appears.

4. Enter values for the following PowerCenter Repository Service options.

   The following table describes the PowerCenter Repository Service options:

Property	Description
Name	Name of the PowerCenter Repository Service. The characters must be compatible with the code page of the repository. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [The PowerCenter Repository Service and the repository have the same name.
Description	Description of PowerCenter Repository Service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Select Folder to choose a different folder. You can also move the PowerCenter Repository Service to a different folder after you create it.
License	License that allows use of the service. If you do not select a license when you create the service, you can assign a license later. The options included in the license determine the selections you can make for the repository. For example, you must have the team-based development option to create a versioned repository. Also, you need the high availability option to run the PowerCenter Repository Service on more than one node. To apply changes, restart the PowerCenter Repository Service.
Node	Node on which the service process runs. Required if you do not select a license with the high availability option. If you select a license with the high availability option, this property does not appear.
Primary Node	Node on which the service process runs by default. Required if you select a license with the high availability option. This property appears if you select a license with the high availability option.
Backup Nodes	Nodes on which the service process can run if the primary node is unavailable. Optional if you select a license with the high availability option. This property appears if you select a license with the high availability option.
Database Type	Type of database storing the repository. To apply changes, restart the PowerCenter Repository Service.
Code Page	Repository code page. The PowerCenter Repository Service uses the character set encoded in the repository code page when writing data to the repository. You cannot change the code page in the PowerCenter Repository Service properties after you create the PowerCenter Repository Service.
Connect String	Native connection string the PowerCenter Repository Service uses to access the repository database. For example, use *servername@dbname* for Microsoft SQL Server and *dbname.world* for Oracle. To apply changes, restart the PowerCenter Repository Service.
Username	Account for the repository database. Set up this account using the appropriate database client tools. To apply changes, restart the PowerCenter Repository Service.
Password	Repository database password corresponding to the database user. Must be in 7-bit ASCII. To apply changes, restart the PowerCenter Repository Service.
TablespaceName	Tablespace name for IBM DB2 and Sybase repositories. When you specify the tablespace name, the PowerCenter Repository Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name.

Property	Description
	To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node. To apply changes, restart the PowerCenter Repository Service.
Creation Mode	Creates or omits new repository content. Select one of the following options: - Create repository content. Select if no content exists in the database. Optionally, choose to create a global repository, enable version control, or both. If you do not select these options during service creation, you can select them later. However, if you select the options during service creation, you cannot later convert the repository to a local repository or to a non-versioned repository. The option to enable version control appears if you select a license with the high availability option. - Do not create repository content. Select if content exists in the database or if you plan to create the repository content later.
Enable the Repository Service	Enables the service. When you select this option, the service starts running when it is created. Otherwise, you need to click the Enable button to run the service. You need a valid license to run a PowerCenter Repository Service.

5. If you create a PowerCenter Repository Service for a repository with existing content and the repository existed in a different Informatica domain, verify that users and groups with privileges for the PowerCenter Repository Service exist in the current domain.

   The Service Manager periodically synchronizes the list of users and groups in the repository with the users and groups in the domain configuration database. During synchronization, users and groups that do not exist in the current domain are deleted from the repository. You can use *infacmd* to export users and groups from the source domain and import them into the target domain.

6. Click OK.

Database Connect Strings

When you create a database connection, specify a connect string for that connection. The PowerCenter Repository Service uses native connectivity to communicate with the repository database.

The following table lists the native connect string syntax for each supported database:

Database	Connect String Syntax	Example
IBM DB2	<database name>	mydatabase
Microsoft SQL Server	<server name>@<database name>	sqlserver@mydatabase
Oracle	<database name>.world (same as TNSNAMES entry)	oracle.world
Sybase	<server name>@<database name>	sybaseserver@mydatabase

PowerCenter Repository Service Configuration

After you create a PowerCenter Repository Service, you can configure it. Use the Administrator tool to configure the following types of PowerCenter Repository Service properties:

- Repository properties. Configure repository properties, such as the Operating Mode.
- Node assignments. If you have the high availability option, configure the primary and backup nodes to run the service.
- Database properties. Configure repository database properties, such as the database user name, password, and connection string.
- Advanced properties. Configure advanced repository properties, such as the maximum connections and locks on the repository.
- Custom properties. Configure repository properties that are unique to your Informatica environment or that apply in special cases. Use custom properties only if Informatica Global Customer Support instructs you to do so.

To view and update properties, select the PowerCenter Repository Service in the Navigator. The Properties tab for the service appears.

Node Assignments

If you have the high availability option, you can designate primary and backup nodes to run the service. By default, the service runs on the primary node. If the node becomes unavailable, the service fails over to a backup node.

General Properties

To edit the general properties, select the PowerCenter Repository Service in the Navigator, select the **Properties** view, and then click **Edit** in the General Properties section.

The following table describes the general properties for a PowerCenter Repository Service:

Property	Description
Name	Name of the PowerCenter Repository Service. You cannot edit this property.
Description	Description of the PowerCenter Repository Service.
License	License object you assigned the PowerCenter Repository Service to when you created the service. You cannot edit this property.
Primary Node	Node in the Informatica domain that the PowerCenter Repository Service runs on. To assign the PowerCenter Repository Service to a different node, you must first disable the service.

Repository Properties

You can configure some of the repository properties when you create the service.

The following table describes the repository properties:

Property	Description
Operating Mode	Mode in which the PowerCenter Repository Service is running. Values are Normal and Exclusive. Run the PowerCenter Repository Service in exclusive mode to perform some administrative tasks, such as promoting a local repository to a global repository or enabling version control. To apply changes, restart the PowerCenter Repository Service.
Security Audit Trail	Tracks changes made to users, groups, privileges, and permissions. The Log Manager tracks the changes.
Global Repository	Creates a global repository. If the repository is a global repository, you cannot revert back to a local repository. To promote a local repository to a global repository, the PowerCenter Repository Service must be running in exclusive mode.
Version Control	Creates a versioned repository. After you enable a repository for version control, you cannot disable the version control. To enable a repository for version control, you must run the PowerCenter Repository Service in exclusive mode. This property appears if you have the team-based development option.

Database Properties

Database properties provide information about the database that stores the repository metadata. You specify the database properties when you create the PowerCenter Repository Service. After you create a repository, you may need to modify some of these properties. For example, you might need to change the database user name and password, or you might want to adjust the database connection timeout.

The following table describes the database properties:

Property	Description
Database Type	Type of database storing the repository. To apply changes, restart the PowerCenter Repository Service.
Code Page	Repository code page. The PowerCenter Repository Service uses the character set encoded in the repository code page when writing data to the repository. You cannot change the code page in the PowerCenter Repository Service properties after you create the PowerCenter Repository Service. This is a read-only field.
Connect String	Native connection string the PowerCenter Repository Service uses to access the database containing the repository. For example, use *servername@dbname* for Microsoft SQL Server and *dbname.world* for Oracle. To apply changes, restart the PowerCenter Repository Service.
Table Space Name	Tablespace name for IBM DB2 and Sybase repositories. When you specify the tablespace name, the PowerCenter Repository Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name. You cannot change the tablespace name in the repository database properties after you create the service. If you create a PowerCenter Repository Service with the wrong tablespace name, delete the PowerCenter Repository Service and create a new one with the correct tablespace name. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node. To apply changes, restart the PowerCenter Repository Service.

Property	Description
Optimize Database Schema	Enables optimization of repository database schema when you create repository contents or back up and restore an IBM DB2 or Microsoft SQL Server repository. When you enable this option, the Repository Service creates repository tables using Varchar(2000) columns instead of CLOB columns wherever possible. Using Varchar columns improves repository performance because it reduces disk input and output and because the database buffer cache can cache Varchar columns. To use this option, the repository database must meet the following page size requirements: - IBM DB2: Database page size 4 KB or greater. At least one temporary tablespace with page size 16 KB or greater. - Microsoft SQL Server: Database page size 8 KB or greater. Default is disabled.
Database Username	Account for the database containing the repository. Set up this account using the appropriate database client tools. To apply changes, restart the PowerCenter Repository Service.
Database Password	Repository database password corresponding to the database user. Must be in 7-bit ASCII. To apply changes, restart the PowerCenter Repository Service.
Database Connection Timeout	Period of time that the PowerCenter Repository Service tries to establish or reestablish a connection to the database system. Default is 180 seconds.
Database Array Operation Size	Number of rows to fetch each time an array database operation is issued, such as insert or fetch. Default is 100. To apply changes, restart the PowerCenter Repository Service.
Database Pool Size	Maximum number of connections to the repository database that the PowerCenter Repository Service can establish. If the PowerCenter Repository Service tries to establish more connections than specified for DatabasePoolSize, it times out the connection after the number of seconds specified for DatabaseConnectionTimeout. Default is 500. Minimum is 20.
Table Owner Name	Name of the owner of the repository tables for a DB2 repository. **Note:** You can use this option for DB2 databases only.

Advanced Properties

Advanced properties control the performance of the PowerCenter Repository Service and the repository database.

The following table describes the advanced properties:

Property	Description
Authenticate MS-SQL User	Uses Windows authentication to access the Microsoft SQL Server database. The user name that starts the PowerCenter Repository Service must be a valid Windows user with access to the Microsoft SQL Server database. To apply changes, restart the PowerCenter Repository Service.
Required Comments for Checkin	Requires users to add comments when checking in repository objects. To apply changes, restart the PowerCenter Repository Service.

Property	Description
Minimum Severity for Log Entries	Level of error messages written to the PowerCenter Repository Service log. Specify one of the following message levels: - Fatal - Error - Warning - Info - Trace - Debug When you specify a severity level, the log includes all errors at that level and above. For example, if the severity level is Warning, fatal, error, and warning messages are logged. Use Trace or Debug if Informatica Global Customer Support instructs you to use that logging level for troubleshooting purposes. Default is INFO.
Resilience Timeout	Period of time that the service tries to establish or reestablish a connection to another service. If blank, the service uses the domain resilience timeout. Default is 180 seconds.
Limit on Resilience Timeout	Maximum amount of time that the service holds on to resources to accommodate resilience timeouts. This property limits the resilience timeouts for client applications connecting to the service. If a resilience timeout exceeds the limit, the limit takes precedence. If blank, the service uses the domain limit on resilience timeouts. Default is 180 seconds. To apply changes, restart the PowerCenter Repository Service.
Repository Agent Caching	Enables repository agent caching. Repository agent caching provides optimal performance of the repository when you run workflows. When you enable repository agent caching, the PowerCenter Repository Service process caches metadata requested by the PowerCenter Integration Service. Default is Yes.
Agent Cache Capacity	Number of objects that the cache can contain when repository agent caching is enabled. You can increase the number of objects if there is available memory on the machine running the PowerCenter Repository Service process. The value must be between 100 and 10,000,000,000. Default is 10,000.
Allow Writes With Agent Caching	Allows you to modify metadata in the repository when repository agent caching is enabled. When you allow writes, the PowerCenter Repository Service process flushes the cache each time you save metadata through the PowerCenter Client tools. You might want to disable writes to improve performance in a production environment where the PowerCenter Integration Service makes all changes to repository metadata. Default is Yes.
Heart Beat Interval	Interval at which the PowerCenter Repository Service verifies its connections with clients of the service. Default is 60 seconds.
Maximum Active Users	Maximum number of connections the repository accepts from repository clients. Default is 200.
Maximum Object Locks	Maximum number of locks the repository places on metadata objects. Default is 50,000.
Database Pool Expiration Threshold	Minimum number of idle database connections allowed by the PowerCenter Repository Service. For example, if there are 20 idle connections, and you set this threshold to 5, the PowerCenter Repository Service closes no more than 15 connections. Minimum is 3. Default is 5.
Database Pool Expiration Timeout	Interval, in seconds, at which the PowerCenter Repository Service checks for idle database connections. If a connection is idle for a period of time greater than this

Property	Description
	value, the PowerCenter Repository Service can close the connection. Minimum is 300. Maximum is 2,592,000 (30 days). Default is 3,600 (1 hour).
Preserve MX Data for Old Mappings	Preserves MX data for old versions of mappings. When disabled, the PowerCenter Repository Service deletes MX data for old versions of mappings when you check in a new version. Default is disabled.

Metadata Manager Service Properties

You can access data lineage analysis for a PowerCenter repository from the PowerCenter Designer. To access data lineage from the Designer, you configure the Metadata Manager Service properties for the PowerCenter Repository Service.

Before you configure data lineage for a PowerCenter repository, complete the following tasks:

- Make sure Metadata Manager is running. Create a Metadata Manager Service in the Administrator tool or verify that an enabled Metadata Manager Service exists in the domain that contains the PowerCenter Repository Service for the PowerCenter repository.
- Load the PowerCenter repository metadata. Create a resource for the PowerCenter repository in Metadata Manager and load the PowerCenter repository metadata into the Metadata Manager warehouse.

The following table describes the Metadata Manager Service properties:

Property	Description
Metadata Manager Service	Name of the Metadata Manager Service used to run data lineage. Select from the available Metadata Manager Services in the domain.
Resource Name	Name of the PowerCenter resource in Metadata Manager.

Custom Properties

Custom properties include properties that are unique to your Informatica environment or that apply in special cases.

A PowerCenter Repository Service does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

PowerCenter Repository Service Process Configuration

Use the Administrator tool to configure the following types of PowerCenter Repository Service process properties:

- Custom properties. Configure PowerCenter Repository Service process properties that are unique to your Informatica environment or that apply in special cases.
- Environment variables. Configure environment variables for each PowerCenter Repository Service process.

To view and update properties, select a PowerCenter Repository Service in the Navigator and click the Processes view.

Custom Properties

Custom properties include properties that are unique to the Informatica environment or that apply in special cases.

A PowerCenter Repository Service process does not have custom properties when you initially create it. Use custom properties only at the request of Informatica Global Customer Support.

Environment Variables

The database client path on a node is controlled by an environment variable.

Set the database client path environment variable for the PowerCenter Repository Service process if the PowerCenter Repository Service process requires a different database client than another PowerCenter Repository Service process that is running on the same node.

The database client code page on a node is usually controlled by an environment variable. For example, Oracle uses NLS_LANG, and IBM DB2 uses DB2CODEPAGE. All PowerCenter Integration Services and PowerCenter Repository Services that run on this node use the same environment variable. You can configure a PowerCenter Repository Service process to use a different value for the database client code page environment variable than the value set for the node.

You can configure the code page environment variable for a PowerCenter Repository Service process when the PowerCenter Repository Service process requires a different database client code page than the PowerCenter Integration Service process running on the same node.

For example, the PowerCenter Integration Service reads from and writes to databases using the UTF-8 code page. The PowerCenter Integration Service requires that the code page environment variable be set to UTF-8. However, you have a Shift-JIS repository that requires that the code page environment variable be set to Shift-JIS. Set the environment variable on the node to UTF-8. Then add the environment variable to the PowerCenter Repository Service process properties and set the value to Shift-JIS.

CHAPTER 19

PowerCenter Repository Management

This chapter includes the following topics:

- PowerCenter Repository Management Overview, 268
- PowerCenter Repository Service and Service Processes, 269
- Operating Mode, 271
- PowerCenter Repository Content, 272
- Enabling Version Control, 273
- Managing a Repository Domain, 274
- Managing User Connections and Locks, 277
- Sending Repository Notifications, 280
- Backing Up and Restoring the PowerCenter Repository, 280
- Copying Content from Another Repository, 282
- Repository Plug-in Registration, 283
- Audit Trails, 284
- Repository Performance Tuning, 284

PowerCenter Repository Management Overview

You use the Administrator tool to manage PowerCenter Repository Services and repository content. A PowerCenter Repository Service manages a single repository.

You can use the Administrator tool to complete the following repository tasks:

- Enable and disable a PowerCenter Repository Service or service process.
- Change the operating mode of a PowerCenter Repository Service.
- Create and delete repository content.
- Back up, copy, restore, and delete a repository.
- Promote a local repository to a global repository.
- Register and unregister a local repository.
- Manage user connections and locks.

- Send repository notification messages.
- Manage repository plug-ins.
- Configure permissions on the PowerCenter Repository Service.
- Upgrade a repository.
- Upgrade a PowerCenter Repository Service and its dependent services to the latest service version.

PowerCenter Repository Service and Service Processes

When you enable a PowerCenter Repository Service, a service process starts on a node designated to run the service. The service is available to perform repository transactions. If you have the high availability option, the service can fail over to another node if the current node becomes unavailable. If you disable the PowerCenter Repository Service, the service cannot run on any node until you reenable the service.

When you enable a service process, the service process is available to run, but it may not start. For example, if you have the high availability option and you configure a PowerCenter Repository Service to run on a primary node and two backup nodes, you enable PowerCenter Repository Service processes on all three nodes. A single process runs at any given time, and the other processes maintain standby status. If you disable a PowerCenter Repository Service process, the PowerCenter Repository Service cannot run on the particular node of the service process. The PowerCenter Repository Service continues to run on another node that is designated to run the service, as long as the node is available.

Enabling and Disabling a PowerCenter Repository Service

You can enable the PowerCenter Repository Service when you create it or after you create it. You need to enable the PowerCenter Repository Service to perform the following tasks in the Administrator tool:

- Assign privileges and roles to users and groups for the PowerCenter Repository Service.
- Create or delete content.
- Back up or restore content.
- Upgrade content.
- Copy content from another PowerCenter repository.
- Register or unregister a local repository with a global repository.
- Promote a local repository to a global repository.
- Register plug-ins.
- Manage user connections and locks.
- Send repository notifications.

You must disable the PowerCenter Repository Service to run it in it exclusive mode.

Note: Before you disable a PowerCenter Repository Service, verify that all users are disconnected from the repository. You can send a repository notification to inform users that you are disabling the service.

Enabling a PowerCenter Repository Service

1. In the Administrator tool , click the **Domain** tab.
2. In the Navigator, select the PowerCenter Repository Service.

3. In the Domain tab **Actions** menu, click **Enable**

   The status indicator at the top of the contents panel indicates when the service is available.

Disabling a PowerCenter Repository Service

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the PowerCenter Repository Service.
3. On the Domain tab **Actions** menu, select **Disable Service**.
4. In the Disable Repository Service, select to abort all service processes immediately or allow services processes to complete.
5. Click **OK**.

Enabling and Disabling PowerCenter Repository Service Processes

A service process is the physical representation of a service running on a node. The process for a PowerCenter Repository Service is the *pmrepagent* process. At any given time, only one service process is running for the service in the domain.

When you create a PowerCenter Repository Service, service processes are enabled by default on the designated nodes, even if you do not enable the service. You disable and enable service processes on the Processes view. You may want to disable a service process to perform maintenance on the node or to tune performance.

If you have the high availability option, you can configure the service to run on multiple nodes. At any given time, a single process is running for the PowerCenter Repository Service. The service continues to be available as long as one of the designated nodes for the service is available. With the high availability option, disabling a service process does not disable the service if the service is configured to run on multiple nodes. Disabling a service process that is running causes the service to fail over to another node.

Enabling a PowerCenter Repository Service Process

1. In the Administrator tool , click the **Domain** tab.
2. In the Navigator, select the PowerCenter Repository Service associated with the service process you want to enable.
3. In the contents panel, click the **Processes** view.
4. Select the process you want to enable.
5. In the Domain tab **Actions** menu, click **Enable Process** to enable the service process on the node.

Disabling a PowerCenter Repository Service Process

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the PowerCenter Repository Service associated with the service process you want to disable.
3. In the contents panel, click the **Processes** view.
4. Select the process you want to disable.
5. On the Domain tab **Actions** menu, select **Disable Process**.
6. In the dialog box that appears, select to abort service processes immediately or allow service processes to complete.
7. Click **OK**.

Operating Mode

You can run the PowerCenter Repository Service in normal or exclusive operating mode. When you run the PowerCenter Repository Service in normal mode, you allow multiple users to access the repository to update content. When you run the PowerCenter Repository Service in exclusive mode, you allow only one user to access the repository. Set the operating mode to exclusive to perform administrative tasks that require a single user to access the repository and update the configuration. If a PowerCenter Repository Service has no content associated with it or if a PowerCenter Repository Service has content that has not been upgraded, the PowerCenter Repository Service runs in exclusive mode only.

When the PowerCenter Repository Service runs in exclusive mode, it accepts connection requests from the Administrator tool and *pmrep*.

Run a PowerCenter Repository Service in exclusive mode to perform the following administrative tasks:

- Delete repository content. Delete the repository database tables for the PowerCenter repository.
- Enable version control. If you have the team-based development option, you can enable version control for the repository. A versioned repository can store multiple versions of an object.
- Promote a PowerCenter repository. Promote a local repository to a global repository to build a repository domain.
- Register a local repository. Register a local repository with a global repository to create a repository domain.
- Register a plug-in. Register or unregister a repository plug-in that extends PowerCenter functionality.
- Upgrade the PowerCenter repository. Upgrade the repository metadata.

Before running a PowerCenter Repository Service in exclusive mode, verify that all users are disconnected from the repository. You must stop and restart the PowerCenter Repository Service to change the operating mode.

When you run a PowerCenter Repository Service in exclusive mode, repository agent caching is disabled, and you cannot assign privileges and roles to users and groups for the PowerCenter Repository Service.

Note: You cannot use *pmrep* to log in to a new PowerCenter Repository Service running in exclusive mode if the Service Manager has not synchronized the list of users and groups in the repository with the list in the domain configuration database. To synchronize the list of users and groups, restart the PowerCenter Repository Service.

Running a PowerCenter Repository Service in Exclusive Mode

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service.
3. In the Properties view, click Edit in the repository properties section.
4. Set the operating mode to Exclusive.
5. Click OK.

   The Administrator tool prompts you to restart the PowerCenter Repository Service.
6. Verify that you have notified users to disconnect from the repository, and click Yes if you want to log out users who are still connected.

   A warning message appears.

7. Choose to allow processes to complete or abort all processes, and then click OK.

   The PowerCenter Repository Service stops and then restarts. The service status at the top of the right pane indicates when the service has restarted. The Disable button for the service appears when the service is enabled and running.

   Note: PowerCenter does not provide resilience for a repository client when the PowerCenter Repository Service runs in exclusive mode.

Running a PowerCenter Repository Service in Normal Mode

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service.
3. In the Properties view, click Edit in the repository properties section.
4. Select Normal as the operating mode.
5. Click OK.

   The Administrator tool prompts you to restart the PowerCenter Repository Service.

   Note: You can also use the *infacmd* UpdateRepositoryService command to change the operating mode.

PowerCenter Repository Content

Repository content are repository tables in the database. You can create or delete repository content for a PowerCenter Repository Service.

Creating PowerCenter Repository Content

You can create repository content for a PowerCenter Repository Service if you did not create content when you created the service or if you deleted the repository content. You cannot create content for a PowerCenter Repository Service that already has content.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a PowerCenter Repository Service that has no content associated with it.
3. On the Domain tab Actions menu, select Repository Content > Create.

   The page displays the options to create content.
4. Optionally, choose to create a global repository.

   Select this option if you are certain you want to create a global repository. You can promote a local repository to a global repository at any time, but you cannot convert a global repository to a local repository.
5. Optionally, enable version control.

   You must have the team-based development option to enable version control. Enable version control if you are certain you want to use a versioned repository. You can convert a non-versioned repository to a versioned repository at any time, but you cannot convert a versioned repository to a non-versioned repository.
6. Click OK.

Deleting PowerCenter Repository Content

Delete repository content when you want to delete all metadata and repository database tables from the repository. When you delete repository content, you also delete all privileges and roles assigned to users for the PowerCenter Repository Service.

You might delete the repository content if the metadata is obsolete. Deleting repository content is an irreversible action. If the repository contains information that you might need later, back up the repository before you delete it.

To delete a global repository, you must unregister all local repositories. Also, you must run the PowerCenter Repository Service in exclusive mode to delete repository content.

Note: You can also use the *pmrep* Delete command to delete repository content.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service from which you want to delete the content.
3. Change the operating mode of the PowerCenter Repository Service to exclusive.
4. On the Domain tab Actions menu, click Repository Content > Delete.
5. Enter your user name, password, and security domain.

   The Security Domain field appears when the Informatica domain contains an LDAP security domain.
6. If the repository is a global repository, choose to unregister local repositories when you delete the content.

   The delete operation does not proceed if it cannot unregister the local repositories. For example, if a Repository Service for one of the local repositories is running in exclusive mode, you may need to unregister that repository before you delete the global repository.
7. Click OK.

   The activity log displays the results of the delete operation.

Upgrading PowerCenter Repository Content

You can upgrade a repository to version 9.0. The options is available for previous versions of the repository.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service for the repository you want to upgrade.
3. On the Domain tab Actions menu, click Repository Contents > Upgrade.
4. Enter the repository administrator user name, password, and security domain.

   The security domain field appears when the Informatica domain contains an LDAP security domain.
5. Click OK.

   The activity log displays the results of the upgrade operation.

Enabling Version Control

If you have the team-based development option, you can enable version control for a new or existing repository. A versioned repository can store multiple versions of objects. If you enable version control, you can maintain multiple versions of an object, control development of the object, and track changes. You can also use labels and deployment groups to associate groups of objects and copy them from one repository to another. After you enable version control for a repository, you cannot disable it.

When you enable version control for a repository, the repository assigns all versioned objects version number 1, and each object has an active status.

You must run the PowerCenter Repository Service in exclusive mode to enable version control for the repository.

1. Ensure that all users disconnect from the PowerCenter repository.
2. In the Administrator tool, click the Domain tab.
3. Change the operating mode of the PowerCenter Repository Service to exclusive.
4. Enable the PowerCenter Repository Service.
5. In the Navigator, select the PowerCenter Repository Service.
6. In the repository properties section of the Properties view, click Edit.
7. Select Version Control.
8. Click OK.

   The Repository Authentication dialog box appears.
9. Enter your user name, password, and security domain.

   The Security Domain field appears when the Informatica domain contains an LDAP security domain.
10. Change the operating mode of the PowerCenter Repository Service to normal.

    The repository is now versioned.

Managing a Repository Domain

A repository domain is a group of linked PowerCenter repositories that consists of one global repository and one or more local repositories. You group repositories in a repository domain to share data and metadata between repositories. When working in a repository domain, you can perform the following tasks:

- Promote metadata from a local repository to a global repository, making it accessible to all local repositories in the repository domain.
- Copy objects from or create shortcuts to metadata in the global repository.
- Copy objects from the local repository to the global repository.

Prerequisites for a PowerCenter Repository Domain

Before building a repository domain, verify that you have the following required elements:

- A licensed copy of Informatica to create the global repository.
- A license for each local repository you want to create.
- A database created and configured for each repository.
- A PowerCenter Repository Service created and configured to manage each repository.

  A PowerCenter Repository Service accesses the repository faster if the PowerCenter Repository Service process runs on the machine where the repository database resides.
- Network connections between the PowerCenter Repository Services and PowerCenter Integration Services.
- Compatible repository code pages.

  To register a local repository, the code page of the global repository must be a subset of each local repository code page in the repository domain. To copy objects from the local repository to the global repository, the code pages of the local and global repository must be compatible.

Building a PowerCenter Repository Domain

Use the following steps as a guideline to connect separate PowerCenter repositories into a repository domain:

1. Create a repository and configure it as a global repository. You can specify that a repository is the global repository when you create the PowerCenter Repository Service. Alternatively, you can promote an existing local repository to a global repository.
2. Register local repositories with the global repository. After a local repository is registered, you can connect to the global repository from the local repository and you can connect to the local repository from the global repository.
3. Create user accounts for users performing cross-repository work. A user who needs to connect to multiple repositories must have privileges for each PowerCenter Repository Service.

   When the global and local repositories exist in different Informatica domains, the user must have an identical user name, password, and security domain in each Informatica domain. Although the user name, password, and security domain must be the same, the user can be a member of different user groups and can have a different set of privileges for each PowerCenter Repository Service.
4. Configure the user account used to access the repository associated with the PowerCenter Integration Service. To run a session that uses a global shortcut, the PowerCenter Integration Service must access the repository in which the mapping is saved and the global repository with the shortcut information. You enable this behavior by configuring the user account used to access the repository associated with the PowerCenter Integration Service. This user account must have privileges for the following services:
   - The local PowerCenter Repository Service associated with the PowerCenter Integration Service
   - The global PowerCenter Repository Service in the domain

Promoting a Local Repository to a Global Repository

You can promote an existing repository to a global repository. After you promote a repository to a global repository, you cannot change it to a local or standalone repository. After you promote a repository, you can register local repositories to create a repository domain.

When registering local repositories with a global repository, the global and local repository code pages must be compatible. Before promoting a repository to a global repository, make sure the repository code page is compatible with each local repository you plan to register.

To promote a repository to a global repository, you need to change the operating mode of the PowerCenter Repository Service to exclusive. If users are connected to the repository, have them disconnect before you run the repository in exclusive mode.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service for the repository you want to promote.
3. If the PowerCenter Repository Service is running in normal mode, change the operating mode to exclusive.
4. If the PowerCenter Repository Service is not enabled, click Enable.
5. In the repository properties section for the service, click Edit.
6. Select Global Repository, and click OK.

   The Repository Authentication dialog box appears.
7. Enter your user name, password, and security domain.

   The Security Domain field appears when the Informatica Domain contains an LDAP security domain.
8. Click OK.

After you promote a local repository, the value of the GlobalRepository property is true in the general properties for the PowerCenter Repository Service.

Registering a Local Repository

You can register local repositories with a global repository to create a repository domain.When you register a local repository, the code pages of the local and global repositories must be compatible. You can copy objects from the local repository to the global repository and create shortcuts. You can also copy objects from the global repository to the local repository.

If you unregister a repository from the global repository and register it again, the PowerCenter Repository Service re-establishes global shortcuts. For example, if you create a copy of the global repository and delete the original, you can register all local repositories with the copy of the global repository. The PowerCenter Repository Service reestablishes all global shortcuts unless you delete objects from the copied repository.

A separate PowerCenter Repository Service manages each repository. For example, if a repository domain has three local repositories and one global repository, it must have four PowerCenter Repository Services. The PowerCenter Repository Services and repository databases do not need to run on the same machine. However, you improve performance for repository transactions if the PowerCenter Repository Service process runs on the same machine where the repository database resides.

You can move a registered local or global repository to a different PowerCenter Repository Service in the repository domain or to a different Informatica domain.

1. In the Navigator, select the PowerCenter Repository Service associated with the local repository.
2. If the PowerCenter Repository Service is running in normal mode, change the operating mode to exclusive.
3. If the PowerCenter Repository Service is not enabled, click Enable.
4. To register a local repository, on the Domain Actions menu, click Repository Domain > Register Local Repository. Continue to the next step. To unregister a local repository, on the Domain Actions menu, click Repository Domain > Unregister Local Repository. Skip to step 10.
5. Select the Informatica domain of the PowerCenter Repository Service for the global repository.

   If the PowerCenter Repository Service is in a domain that does not appear in the list of Informatica domains, click Manage Domain List to update the list.

   The Manage List of Domains dialog box appears.
6. To add a domain to the list, enter the following information:

Field	Description
Domain Name	Name of a Informatica Domain that you want to link to.
Host Name	Machine hosting the master gateway node for the linked domain. The machine hosting the master gateway for the local Informatica Domain must have a network connection to this machine.
Host Port	Gateway port number for the linked domain.

7. Click Add to add more than one domain to the list, and repeat step 6 for each domain.

   To edit the connection information for a linked domain, go to the section for the domain you want to update and click Edit.

   To remove a linked domain from the list, go to the section for the domain you want to remove and click Delete.
8. Click Done to save the list of domains.
9. Select the PowerCenter Repository Service for the global repository.
10. Enter the user name, password, and security domain for the user who manages the global PowerCenter Repository Service.

    The Security Domain field appears when the Informatica Domain contains an LDAP security domain.

11. Enter the user name, password, and security domain for the user who manages the local PowerCenter Repository Service.
12. Click OK.

Viewing Registered Local and Global Repositories

For a global repository, you can view a list of all the registered local repositories. Likewise, if a local repository is registered with a global repository, you can view the name of the global repository and the Informatica domain where it resides.

A PowerCenter Repository Service manages a single repository. The name of a repository is the same as the name of the PowerCenter Repository Service that manages it.

1. In the Navigator, select the PowerCenter Repository Service that manages the local or global repository.
2. On the Domain tab Actions menu, click Repository Domain > View Registered Repositories.

   For a global repository, a list of local repositories appears.

   For a local repository, the name of the global repository appears.

   Note: The Administrator tool displays a message if a local repository is not registered with a global repository or if a global repository has no registered local repositories.

Moving Local and Global Repositories

If you need to move a local or global repository to another Informatica domain, complete the following steps:

1. Unregister the local repositories. For each local repository, follow the procedure to unregister a local repository from a global repository. To move a global repository to another Informatica domain, unregister all local repositories associated with the global repository.
2. Create the PowerCenter Repository Services using existing content. For each repository in the target domain, follow the procedure to create a PowerCenter Repository Service using the existing repository content in the source Informatica domain.

   Verify that users and groups with privileges for the source PowerCenter Repository Service exist in the target domain. The Service Manager periodically synchronizes the list of users and groups in the repository with the users and groups in the domain configuration database. During synchronization, users and groups that do not exist in the target domain are deleted from the repository.

   You can use *infacmd* to export users and groups from the source domain and import them into the target domain.
3. Register the local repositories. For each local repository in the target Informatica domain, follow the procedure to register a local repository with a global repository.

Managing User Connections and Locks

You can use the Administrator tool to manage user connections and locks and perform the following tasks:

- View locks. View object locks and lock type. The PowerCenter repository locks repository objects and folders by user. The repository uses locks to prevent users from duplicating or overwriting work. The repository creates different types of locks depending on the task.
- View user connections. View all user connections to the repository.

- Close connections and release locks. Terminate residual connections and locks. When you close a connection, you release all locks associated with that connection.

Viewing Locks

You can view locks and identify residual locks in the Administrator tool.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the PowerCenter Repository Service with the locks that you want to view.
3. In the contents panel, click the **Connections & Locks** view.
4. In the details panel, click the **Locks** view.

   The following table describes the object lock information:

Column Name	Description
Server Thread ID	Identification number assigned to the repository connection.
Folder	Folder in which the locked object is saved.
Object Type	Type of object, such as folder, version, mapping, or source.
Object Name	Name of the locked object.
Lock Type	Type of lock: in-use, write-intent, or execute.
Lock Name	Name assigned to the lock.

Viewing User Connections

You can view user connection details in the Administrator tool. You might want to view user connections to verify all users are disconnected before you disable the PowerCenter Repository Service.

To view user connection details:

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the PowerCenter Repository Service with the locks that you want to view.
3. In the contents panel, click the **Connections & Locks** view.
4. In the details panel, click the **Properties** view.

   The following table describes the user connection information:

Property	Description
Connection ID	Identification number assigned to the repository connection.
Status	Connection status.
Username	User name associated with the connection.
Security Domain	Security domain of the user.
Application	Repository client associated with the connection.

Property	Description
Service	Service that connects to the PowerCenter Repository Service.
Host Name	Name of the machine running the application.
Host Address	IP address for the host machine.
Host Port	Port number of the machine hosting the repository client used to communicate with the repository.
Process ID	Identifier assigned to the PowerCenter Repository Service process.
Login Time	Time when the user connected to the repository.
Last Active Time	Time of the last metadata transaction between the repository client and the repository.

Closing User Connections and Releasing Locks

Sometimes, the PowerCenter Repository Service does not immediately disconnect a user from the repository. The repository has a residual connection when the repository client or machine is shut down but the connection remains in the repository. This can happen in the following situations:

- Network problems occur.
- A PowerCenter Client, PowerCenter Integration Service, PowerCenter Repository Service, or database machine shuts down improperly.

A residual repository connection also retains all repository locks associated with the connection. If an object or folder is locked when one of these events occurs, the repository does not release the lock. This lock is called a residual lock.

If a system or network problem causes a repository client to lose connectivity to the repository, the PowerCenter Repository Service detects and closes the residual connection. When the PowerCenter Repository Service closes the connection, it also releases all repository locks associated with the connection.

A PowerCenter Integration Service may have multiple connections open to the repository. If you close one PowerCenter Integration Service connection to the repository, you close all connections for that service.

Important: Closing an active connection can cause repository inconsistencies. Close residual connections only.

To close a connection and release locks:

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the PowerCenter Repository Service with the connection you want to close.
3. In the contents panel, click the **Connections & Locks** view.
4. In the contents panel, select a connection.

   The details panel displays connection properties in the properties view and locks in the locks view.
5. In the **Domain** tab **Actions** menu, select **Delete User Connection**.

   The **Delete Selected Connection** dialog box appears.
6. Enter a user name, password, and security domain.

   You can enter the login information associated with a particular connection, or you can enter the login information for the user who manages the PowerCenter Repository Service.

   The **Security Domain** field appears when the Informatica domain contains an LAP security domain.
7. Click **OK**.

The PowerCenter Repository Service closes connections and releases all locks associated with the connections.

Sending Repository Notifications

You create and send notification messages to all users connected to a repository.

You might want to send a message to notify users of scheduled repository maintenance or other tasks that require you to disable a PowerCenter Repository Service or run it in exclusive mode. For example, you might send a notification message to ask users to disconnect before you promote a local repository to a global repository.

1. Select the PowerCenter Repository Service in the Navigator.
2. In the Domain tab Actions menu, select Notify Users.

   The Notify Users window appears.
3. Enter the message text.
4. Click OK.

   The PowerCenter Repository Service sends the notification message to the PowerCenter Client users. A message box informs users that the notification was received. The message text appears on the Notifications tab of the PowerCenter Client Output window.

Backing Up and Restoring the PowerCenter Repository

Regularly back up repositories to prevent data loss due to hardware or software problems. When you back up a repository, the PowerCenter Repository Service saves the repository in a binary file, including the repository objects, connection information, and code page information. If you need to recover the repository, you can restore the content of the repository from this binary file.

If you back up a repository that has operating system profiles assigned to folders, the PowerCenter Repository Service does not back up the folder assignments. After you restore the repository, you must assign the operating system profiles to the folders.

Before you back up a repository and restore it in a different domain, verify that users and groups with privileges for the source PowerCenter Repository Service exist in the target domain. The Service Manager periodically synchronizes the list of users and groups in the repository with the users and groups in the domain configuration database. During synchronization, users and groups that do not exist in the target domain are deleted from the repository.

You can use *infacmd* to export users and groups from the source domain and import them into the target domain.

Backing Up a PowerCenter Repository

When you back up a repository, the PowerCenter Repository Service stores the file in the backup location you specify for the node. You specify the backup location when you set up the node. View the general properties of the node to determine the path of the backup directory. The PowerCenter Repository Service uses the extension .rep for all repository backup files.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service for the repository you want to back up.
3. On the Domain tab Actions menu, select **Repository Contents** > **Back Up**.

4. Enter your user name, password, and security domain.

   The Security Domain field appears when the Informatica domain contains an LDAP security domain.

5. Enter a file name and description for the repository backup file.

   Use an easily distinguishable name for the file. For example, if the name of the repository is DEVELOPMENT, and the backup occurs on May 7, you might name the file DEVELOPMENTMay07.rep. If you do not include the .rep extension, the PowerCenter Repository Service appends that extension to the file name.

6. If you use the same file name that you used for a previous backup file, select whether or not to replace the existing file with the new backup file.

   To overwrite an existing repository backup file, select Replace Existing File. If you specify a file name that already exists in the repository backup directory and you do not choose to replace the existing file, the PowerCenter Repository Service does not back up the repository.

7. Choose to skip or back up workflow and session logs, deployment group history, and MX data. You might want to skip these operations to increase performance when you restore the repository.

8. Click OK.

   The results of the backup operation appear in the activity log.

Viewing a List of Backup Files

You can view the backup files you create for a repository in the backup directory where they are saved. You can also view a list of existing backup files in the Administrator tool. If you back up a repository through *pmrep*, you must provide a file extension of .rep to view it in the Administrator tool.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service for a repository that has been backed up.
3. On the Domain tab Actions menu, select Repository Contents > View Backup Files.

   The list of the backup files shows the repository version and the options skipped during the backup.

Restoring a PowerCenter Repository

You can restore metadata from a repository binary backup file. When you restore a repository, you must have a database available for the repository. You can restore the repository in a database that has a compatible code page with the original database.

If a repository exists at the target database location, you must delete it before you restore a repository backup file.

Informatica restores repositories from the current product version. If you have a backup file from an earlier product version, you must use the earlier product version to restore the repository.

Verify that the repository license includes the license keys necessary to restore the repository backup file. For example, you must have the team-based development option to restore a versioned repository.

1. In the Navigator, select the PowerCenter Repository Service that manages the repository content you want to restore.
2. On the Domain tab Actions menu, click Repository Contents > Restore.

   The Restore Repository Contents options appear.

3. Select a backup file to restore.
4. Select whether or not to restore the repository as new.

   When you restore a repository as new, the PowerCenter Repository Service restores the repository with a new repository ID and deletes the log event files.

Note: When you copy repository content, you create the repository as new.

5. Optionally, choose to skip restoring the workflow and session logs, deployment group history, and Metadata Exchange (MX) data to improve performance.
6. Click OK.

   The activity log indicates whether the restore operation succeeded or failed.

   Note: When you restore a global repository, the repository becomes a standalone repository. After restoring the repository, you need to promote it to a global repository.

Copying Content from Another Repository

Copy content into a repository when no content exists for the repository and you want to use the content from a different repository. Copying repository content provides a quick way to copy the metadata that you want to use as a basis for a new repository. You can copy repository content to preserve the original repository before upgrading. You can also copy repository content when you need to move a repository from development into production.

To copy repository content, you must create the PowerCenter Repository Service for the target repository. When you create the PowerCenter Repository Service, set the creation mode to create the PowerCenter Repository Service without content. Also, you must select a code page that is compatible with the original repository. Alternatively, you can delete the content from a PowerCenter Repository Service that already has content associated with it.

You must copy content into an empty repository. If repository in the target database already has content, the copy operation fails. You must back up the repository the target database and delete its content before copying the repository content.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the PowerCenter Repository Service to which you want to add copied content.

   You cannot copy content to a repository that has content. If necessary, back up and delete existing repository content before copying in the new content.
3. On the Domain Actions menu, click Repository Contents > Copy From.

   The dialog box displays the options for the Copy From operation.
4. Select the name of the PowerCenter Repository Service.

   The source PowerCenter Repository Service and the PowerCenter Repository Service to which you want to add copied content must be in the same domain and it must be of the same service version.
5. Enter a user name, password, and security domain for the user who manages the repository from which you want to copy content.

   The Security Domain field appears when the Informatica domain contains an LDAP security domain.
6. To skip copying the workflow and session logs, deployment group history, and Metadata Exchange (MX) data, select the check boxes in the advanced options. Skipping this data can increase performance.
7. Click OK.

   The activity log displays the results of the copy operation.

Repository Plug-in Registration

Use the Administrator tool to register and remove repository plug-ins. Repository plug-ins are third-party or other Informatica applications that extend PowerCenter functionality by introducing new repository metadata.

For installation issues specific to the plug-in, consult the plug-in documentation.

Registering a Repository Plug-in

Register a repository plug-in to add its functionality to the repository. You can also update an existing repository plug-in.

1. Run the PowerCenter Repository Service in exclusive mode.
2. In the Navigator, select the PowerCenter Repository Service to which you want to add the plug-in.
3. In the contents panel, click the Plug-ins view.
4. In the Domain tab Actions menu, select Register Plug-in.
5. On the Register Plugin page, click the Browse button to locate the plug-in file.
6. If the plug-in was registered previously and you want to overwrite the registration, select the check box to update the existing plug-in registration. For example, you can select this option when you upgrade a plug-in to the latest version.
7. Enter your user name, password, and security domain.

   The Security Domain field appears when the Informatica Domain contains an LDAP security domain.
8. Click OK.

   The PowerCenter Repository Service registers the plug-in with the repository. The results of the registration operation appear in the activity log.
9. Run the PowerCenter Repository Service in normal mode.

Unregistering a Repository Plug-in

To unregister a repository plug-in, the PowerCenter Repository Service must be running in exclusive mode. Verify that all users are disconnected from the repository before you unregister a plug-in.

The list of registered plug-ins for a PowerCenter Repository Service appears on the Plug-ins tab.

If the PowerCenter Repository Service is not running in exclusive mode, the Remove buttons for plug-ins are disabled.

1. Run the PowerCenter Repository Service in exclusive mode.
2. In the Navigator, select the PowerCenter Repository Service from which you want to remove the plug-in.
3. Click the Plug-ins view.

   The list of registered plug-ins appears.
4. Select a plug-in and click the unregister Plug-in button.
5. Enter your user name, password, and security domain.

   The Security Domain field appears when the Informatica Domain contains an LDAP security domain.
6. Click OK.
7. Run the PowerCenter Repository Service in normal mode.

Audit Trails

You can track changes to users, groups, and permissions on repository objects by selecting the SecurityAuditTrail configuration option in the PowerCenter Repository Service properties in the Administrator tool. When you enable the audit trail, the PowerCenter Repository Service logs security changes to the PowerCenter Repository Service log. The audit trail logs the following operations:

- Changing the owner or permissions for a folder or connection object.
- Adding or removing a user or group.

The audit trail does not log the following operations:

- Changing your own password.
- Changing the owner or permissions for a deployment group, label, or query.

Repository Performance Tuning

Informatica includes features that allow you improve the performance of the repository. You can update statistics and skip information when you copy, back up, or restore the repository.

Repository Statistics

Almost all PowerCenter repository tables use at least one index to speed up queries. Most databases keep and use column distribution statistics to determine which index to use to execute SQL queries optimally. Database servers do not update these statistics continuously.

In frequently used repositories, these statistics can quickly become outdated, and SQL query optimizers may not choose the best query plan. In large repositories, choosing a sub-optimal query plan can have a negative impact on performance. Over time, repository operations gradually become slower.

Informatica identifies and updates the statistics of all repository tables and indexes when you copy, upgrade, and restore repositories. You can also update statistics using the *pmrep* UpdateStatistics command.

Repository Copy, Backup, and Restore Processes

Large repositories can contain a large volume of log and historical information that slows down repository service performance. This information is not essential to repository service operation. When you back up, restore, or copy a repository, you can choose to skip the following types of information:

- Workflow and session logs
- Deployment group history
- Metadata Exchange (MX) data

By skipping this information, you reduce the time it takes to copy, back up, or restore a repository.

You can also skip this information when you use the *pmrep* commands.

CHAPTER 20

PowerExchange Listener Service

This chapter includes the following topics:

- PowerExchange Listener Service Overview, 285
- Listener Service Restart and Failover, 286
- DBMOVER Statements for the Listener Service, 286
- Properties of the Listener Service, 287
- Listener Service Management, 288
- Service Status of the Listener Service, 289
- Listener Service Logs, 290
- Creating a Listener Service, 290

PowerExchange Listener Service Overview

The PowerExchange Listener Service is an application service that manages the PowerExchange Listener. The PowerExchange Listener manages communication between a PowerCenter or PowerExchange client and a data source for bulk data movement and change data capture. The PowerCenter Integration Service connects to the PowerExchange Listener through the Listener Service. Use the Administrator tool to manage the service and view service logs.

When managed by the Listener Service, the PowerExchange Listener is also called the Listener Service process.

The Service Manager, Listener Service, and PowerExchange Listener process must reside on the same node in the Informatica domain.

On a Linux, UNIX, or Windows machine, you can use the Listener Service to manage the PowerExchange Listener process instead of issuing PowerExchange commands such as DTLLST to start the Listener process or CLOSE to stop the Listener process.

Perform the following tasks to manage the Listener Service:

- Create a service.
- View the service properties.
- View service logs.
- Enable, disable, and restart the service.

You can use the Administrator tool or the *infacmd* command line program to administer the Listener Service.

Before you create a Listener Service, install PowerExchange and configure a PowerExchange Listener on the node where you want to create the Listener Service. When you create a Listener Service, the Service Manager

associates it with the PowerExchange Listener on the node. When you start or stop the Listener Service, you also start or stop the PowerExchange Listener.

Listener Service Restart and Failover

If you have the PowerCenter high availability option, the Listener Service provides restart and failover capabilities.

If the Listener Service or the Listener Service process fails on the primary node, the Service Manager restarts the service on the primary node.

If the primary node fails, the Listener Service fails over to the backup node, if one is defined. After failover, the Service Manager synchronizes and connects to the PowerExchange Listener on the backup node.

For the PowerExchange service to fail over successfully, the backup node must be able to connect to the data source or target. Configure the PowerExchange Listener and, if applicable, the PowerExchange Logger for Linux, UNIX, and Windows on the backup node as you do on the primary node.

If the PowerExchange Listener fails during a PowerCenter session, the session fails, and you must restart it. For CDC sessions, PWXPC performs warm start processing. For more information, see the *PowerExchange Interfaces Guide for PowerCenter*.

DBMOVER Statements for the Listener Service

Before you create a Listener Service, you must configure one or more PowerExchange Listener processes and configure the PowerCenter Integration Service to connect to a PowerExchange Listener process through a Listener Service.

The following table describes the DBMOVER statements that you define on all machines where a PowerExchange Listener process runs:

Statement	Description
LISTENER	Defines the TCP/IP port on which a named PowerExchange Listener process listens for work requests. The node name in the LISTENER statement must match the name that you provide in the Start Parameters configuration property when you define the Listener Service.
SVCNODE	Specifies the TCP/IP port on which the PowerExchange Listener process listens for commands from the Listener Service. Use the same port number that you specify for the SVCNODE Port Number configuration property for the service.

The following table describes the DBMOVER statement that you define on the PowerCenter Integration Service node:

Statement	Description
NODE	Configures the PowerCenter Integration Service to connect to the PowerExchange Listener process directly or through a Listener Service.

Statement	Description
	When you run a PowerExchange session, the PowerCenter Integration Service connects to the PowerExchange Listener based on the way you configure the NODE statement: - If the NODE statement includes the *service_name* parameter, the PowerCenter Integration Service connects to the Listener through the Listener Service. - If the NODE statement does not include the *service_name* parameter, the PowerCenter Integration Service connects directly to the Listener. It does not connect through the Listener Service.

For more information about customizing the DBMOVER configuration file for bulk data movement or CDC sessions, see the following guides:

- *PowerExchange Bulk Data Movement Guide*
- *PowerExchange CDC Guide for Linux, UNIX, and Windows*

Properties of the Listener Service

To view the properties of a Listener Service, select the service in the Navigator and click the Properties tab.

You can change the properties while the service is running, but you must restart the service for the properties to take effect.

PowerExchange Listener Service General Properties

The following table describes the general properties of a Listener Service:

General Property	Description
Name	Read-only. Name of the Listener Service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Short description of the Listener Service. The description cannot exceed 765 characters.
Location	Domain in which the Listener Service is created.
Node	Primary node to run the Listener Service.
License	License to assign to the service. If you do not select a license now, you can assign a license to the service later. Required before you can enable the service.
Backup Nodes	Nodes used as a backup to the primary node. This property appears only if you have the PowerCenter high availability option.

PowerExchange Listener Service Configuration Properties

The following table describes the configuration properties of a Listener Service:

General Property	Description
Service Process	Read only. Type of PowerExchange process that the service manages. For the Listener Service, the service process is Listener.
Start Parameters	Parameters to include when you start the Listener Service. Separate the parameters with the space character. The *node_name* parameter is required. You can include the following parameters: - *node_name* Required. Node name that identifies the Listener Service. This name must match the name in the LISTENER statement in the DBMOVER configuration file. - config=*directory* Optional. Specifies the full path and file name for a DBMOVER configuration file that overrides the default dbmover.cfg file in the installation directory. This override file takes precedence over any other override configuration file that you optionally specify with the PWX_CONFIG environment variable. - license=*directory/license_key_file* Optional. Specifies the full path and file name for any license key file that you want to use instead of the default license.key file in the installation directory. This override license key file must have a file name or path that is different from that of the default file. This override file takes precedence over any other override license key file that you optionally specify with the PWX_LICENSE environment variable. **Note:** In the config and license parameters, you must provide the full path only if the file does *not* reside in the installation directory. Include quotes around any path and file name that contains spaces.
SVCNODE Port Number	Specifies the port on which the PowerExchange Listener process listens for commands from the Listener Service. Use the same port number that you specify in the SVCNODE statement of the DBMOVER file. If you define more than one Listener Service to run on a node, you must define a unique SVCNODE port number for each service. This port number must uniquely identify the PowerExchange Listener process to its Listener Service.

Listener Service Management

Use the Properties tab in the Administrator tool to configure general or configuration properties for the Listener Service.

Configuring Listener Service General Properties

Use the Properties tab in the Administrator tool to configure Listener Service general properties.

1. In the Navigator, select the PowerExchange Listener Service.

   The PowerExchange Listener Service properties window appears.
2. In the General Properties area of the Properties tab, click **Edit**.

   The Edit PowerExchange Listener Service dialog box appears.
3. Edit the general properties of the service.
4. Click **OK**.

Configuring Listener Service Configuration Properties

Use the Properties tab in the Administrator tool to configure Listener Service configuration properties.

1. In the Navigator, select the PowerExchange Listener Service.
2. In the Configuration Properties area of the Properties tab, click **Edit**.

   The Edit PowerExchange Listener Service dialog box appears.
3. Edit the configuration properties.

Configuring the Listener Service Process Properties

Use the Processes tab in the Administrator tool to configure the environment variables for each service process.

Environment Variables for the Listener Service Process

You can edit environment variables for a Listener Service process.

The following table describes the environment variables for the Listener Service process:

Property	Description
Environment Variables	Environment variables defined for the Listener Service process.

Service Status of the Listener Service

You can enable, disable, or restart a Listener Service from the Administrator tool. You might disable the Listener Service if you need to temporarily restrict users from using the service. You might restart a service if you modified a property.

Enabling the Listener Service

To enable the Listener Service, select the service in the Domain Navigator and click Enable the Service.

Disabling the Listener Service

If you need to temporarily restrict users from using a Listener Service, you can disable it.

1. Select the service in the Domain Navigator, and click **Disable the Service**.
2. Select one of the following options:
   - Complete. Allows all Listener subtasks to run to completion before shutting down the service and the Listener Service process. Corresponds to the PowerExchange Listener CLOSE command.
   - Stop. Waits up to 30 seconds for subtasks to complete, and then shuts down the service and the Listener Service process. Corresponds to the PowerExchange Listener CLOSE FORCE command.
   - Abort. Stops all processes immediately and shuts down the service.
3. Click **OK**.

For more information about the CLOSE and CLOSE FORCE commands, see the *PowerExchange Command Reference*.

Note: After you select an option and click OK, the Administrator tool displays a busy icon until the service stops. If you select the Complete option but then want to disable the service more quickly with the Stop or Abort option, you must issue the infacmd isp disableService command.

Restarting the Listener Service

You can restart a Listener Service that you previously disabled.

To restart the Listener Service, select the service in the Navigator and click Restart.

Listener Service Logs

The Listener Service generates operational and error log events that the Log Manager collects in the domain. You can view Listener Service logs by performing one of the following actions in the Administrator tool:

- In the Logs tab, select the Domain view. You can filter on any of the columns.
- In the Logs tab, click the Service view. In the Service Type column, select PowerExchange Listener Service. In the Service Name list, optionally select the name of the service.
- In the Domain tab, select Actions > View Logs for Service. The Service view of the Logs tab appears.

Messages appear by default in time stamp order, with the most recent messages on top.

Creating a Listener Service

1. Click the Domain tab of the Administrator tool.
2. Click **Actions** > **New** > **PowerExchange Listener Service**.

   The New PowerExchange Listener Service dialog box appears.

   Enter the properties for the service.
3. Click **OK**.
4. Enable the Listener Service to make it available.

CHAPTER 21

PowerExchange Logger Service

This chapter includes the following topics:

- PowerExchange Logger Service Overview, 291
- Logger Service Restart and Failover, 292
- Configuration Statements for the Logger Service, 292
- Properties of the PowerExchange Logger Service, 293
- Logger Service Management, 294
- Service Status of the Logger Service, 295
- Logger Service Logs, 296
- Creating a Logger Service, 296

PowerExchange Logger Service Overview

The Logger Service is an application service that manages the PowerExchange Logger for Linux, UNIX, and Windows. The PowerExchange Logger captures change data from a data source and writes the data to PowerExchange Logger log files. Use the Administrator tool to manage the service and view service logs.

When managed by the Logger Service, the PowerExchange Logger is also called the Logger Service process.

The Service Manager, Logger Service, and PowerExchange Logger must reside on the same node in the Informatica domain.

On a Linux, UNIX, or Windows machine, you can use the Logger Service to manage the PowerExchange Logger process instead of issuing PowerExchange commands such as PWXCCL to start the Logger process or SHUTDOWN to stop the Logger process.

You can run multiple Logger Services on the same node. Create a Logger Service for each PowerExchange Logger process that you want to manage on the node. You must run one PowerExchange Logger process for each source type and instance, as defined in a PowerExchange registration group.

Perform the following tasks to manage the Logger Service:

- Create a service.
- View the service properties.
- View service logs
- Enable, disable, and restart the service.

You can use the Administrator tool or the *infacmd* command line program to administer the Logger Service.

Before you create a Logger Service, install PowerExchange and configure a PowerExchange Logger on the node where you want to create the Logger Service. When you create a Logger Service, the Service Manager associates it with the PowerExchange Logger that you specify. When you start or stop the Logger Service, you also start or stop the Logger Service process.

Logger Service Restart and Failover

If you have the PowerCenter high availability option, the Logger Service provides restart and failover capabilities.

If the Logger Service or the Logger Service process fails on the primary node, the Service Manager restarts the service on the primary node.

If the primary node fails, the Logger Service fails over to the backup node, if one is defined. After failover, the Service Manager synchronizes and connects to the Logger Service process on the backup node.

For the Logger Service to fail over successfully, the Logger Service process on the backup node must be able to connect to the data source. Include the same statements in the DBMOVER and PowerExchange Logger configuration files on each node.

Configuration Statements for the Logger Service

The Logger Service reads configuration information from the DBMOVER and PowerExchange Logger Configuration (pwxccl.cfg) files.

Define the following statement in the DBMOVER file on each node that you configure to run the Logger Service:

Statement	Description
SVCNODE	Service name and TCP/IP port on which the PowerExchange Logger process listens for commands from the Logger Service. The service name must match the service name that you specify in the associated CONDENSENAME statement in the pwxccl.cfg file. The port number must match the port number that you specify for the SVCNODE Port Number configuration property for the service.

Define the following statement in the PowerExchange Logger configuration file on each node that you configure to run the Logger Service:

Statement	Description
CONDENSENAME	Name for the command-handling service for a PowerExchange Logger process to which commands are issued from the Logger Service. Enter a service name up to 64 characters in length. No default is available. The service name must match the service name that is specified in the associated SVCNODE statement in the dbmover.cfg file.

For more information about customizing the DBMOVER and PowerExchange Logger Configuration files for CDC sessions, see the *PowerExchange CDC Guide for Linux, UNIX, and Windows*.

Properties of the PowerExchange Logger Service

To view the properties of a PowerExchange Logger Service, select the service in the Navigator and click the Properties tab.

You can change the properties while the service is running, but you must restart the service for the properties to take effect.

PowerExchange Logger Service General Properties

The following table describes the properties of a Logger Service:

General Property	Description
Name	Read only. Name of the Logger Service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Short description of the Logger Service. The description cannot exceed 765 characters.
Location	Domain in which the Logger Service is created.
Node	Primary node to run the Logger Service.
License	License to assign to the service. If you do not select a license now, you can assign a license to the service later. Required before you can enable the service.
Backup Nodes	Nodes used as a backup to the primary node. This property appears only if you have the PowerCenter high availability option.

PowerExchange Logger Service Configuration Properties

The following table describes the configuration properties of a Logger Service:

General Property	Description
Service Process	Read only. Type of PowerExchange process that the service manages. For the Logger Service, the service process is Logger.
Start Parameters	Optional. Parameters to include when you start the Logger Service. Separate the parameters with the space character. You can include the following parameters: - coldstart={Y|N} Indicates whether to cold start or warm start the Logger Service. Enter Y to cold start the Logger Service. The absence of checkpoint files does not trigger a cold start. If you specify Y and checkpoint files exist, the Logger Service ignores the files. If the CDCT file contains records, the Logger Service deletes these records. Enter N to warm start the Logger Service from the restart point that is indicated in the last checkpoint file. If no checkpoint file exists in the CHKPT_BASENAME directory, the Logger Service ends. Default is N. - config=*directory/pwx_config_file*

General Property	Description
	Specifies the full path and file name for any dbmover.cfg configuration file that you want to use instead of the default dbmover.cfg file. This alternative configuration file takes precedence over any alternative configuration file that you specify in the PWX_CONFIG environment variable. - cs=*directory*/*pwxlogger_config_file* Specifies the path and file name for the Logger Service configuration file. You can also use the cs parameter to specify a Logger Service configuration file that overrides the default pwxccl.cfg file. The override file must have a path or file name that is different from that of the default file. - license=*directory*/*license_key_file* Specifies the full path and file name for any license key file that you want to use instead of the default license.key file. The alternative license key file must have a file name or path that is different from that of the default file. This alternative license key file takes precedence over any alternative license key file that you specify in the PWX_LICENSE environment variable. **Note:** In the config, cs, and license parameters, you must provide the full path only if the file does *not* reside in the installation directory. Include quotes around any path and file name that contains spaces.
SVCNODE Port Number	Specifies the port on which the PowerExchange Logger process listens for commands from the Logger Service. Use the same port number that you specify in the SVCNODE statement of the DBMOVER file. If you define more than one Logger Service to run on a node, you must define a unique SVCNODE port number for each service. This port number must uniquely identify the PowerExchange Logger process to its Logger Service.

Logger Service Management

Use the Properties tab in the Administrator tool to configure general or configuration properties for the Logger Service.

Configuring Logger Service General Properties

Use the Properties tab in the Administrator tool to configure Logger Service general properties.

1. In the Navigator, select the PowerExchange Logger Service.

   The PowerExchange Logger Service properties window appears.
2. In the General Properties area of the Properties tab, click **Edit**.

   The Edit PowerExchange Logger Service dialog box appears.
3. Edit the general properties of the service.
4. Click OK.

Configuring Logger Service Configuration Properties

Use the Properties tab in the Administrator tool to configure Logger Service configuration properties.

1. In the Navigator, select the PowerExchange Logger Service.

   The PowerExchange Logger Service properties window appears.
2. In the Configuration Properties area of the Properties tab, click **Edit**.

   The Edit PowerExchange Logger Service dialog box appears.
3. Edit the configuration properties for the service.

Configuring the Logger Service Process Properties

Use the Processes tab in the Administrator tool to configure the environment variables for each service process.

Environment Variables for the Logger Service Process

You can edit environment variables for a Logger Service process.

The following table describes the environment variables for the Logger Service process:

Property	Description
Environment Variables	Environment variables defined for the Logger Service process.

Service Status of the Logger Service

You can enable, disable, or restart a PowerExchange Logger Service by using the Administrator tool. You can disable a PowerExchange service if you need to temporarily restrict users from using the service. You might restart a service if you modified a property.

Enabling the Logger Service

To enable the Logger Service, select the service in the Navigator and click **Enable the Service**.

Disabling the Logger Service

If you need to temporarily restrict users from using the Logger Service, you can disable it.

1. Select the service in the Domain Navigator, and click **Disable the Service**.
2. Select one of the following options:
   - Complete. Initiates a controlled shutdown of all processes and shuts down the service. Corresponds to the PowerExchange SHUTDOWN command.
   - Abort. Stops all processes immediately and shuts down the service.
3. Click **OK**.

Restarting the Logger Service

You can restart a Logger Service that you previously disabled.

To restart the Logger Service, select the service in the Navigator and click **Restart**.

Logger Service Logs

The Logger Service generates operational and error log events that the Log Manager in the domain collects. You can view Logger Service logs by performing one of the following actions in the Administrator tool:

- In the Logs tab, select the Domain view. You can filter on any of the columns.
- In the Logs tab, click the Service view. In the Service Type column, select PowerExchange Logger Service. In the Service Name list, optionally select the name of the service.
- In the Domain tab, select Actions > View Logs for Service. The Service view of the Logs tab appears.

Messages appear by default in time stamp order, with the most recent messages on top.

Creating a Logger Service

1. Click the Domain tab of the Administrator tool.
2. Click Actions > New > PowerExchange Logger Service.

   The New PowerExchange Logger Service dialog box appears.
3. Enter the service properties.
4. Click OK.
5. Enable the Logger Service to make it available.

CHAPTER 22

Reporting Service

This chapter includes the following topics:

- Reporting Service Overview, 297
- Creating the Reporting Service, 299
- Managing the Reporting Service, 301
- Configuring the Reporting Service, 304
- Granting Users Access to Reports, 307

Reporting Service Overview

The Reporting Service is an application service that runs the Data Analyzer application in an Informatica domain. Create and enable a Reporting Service on the Domain tab of the Administrator tool.

When you create a Reporting Service, choose the data source to report against:

- PowerCenter repository. Choose the associated PowerCenter Repository Service and specify the PowerCenter repository details to run PowerCenter Repository Reports.
- Metadata Manager warehouse. Choose the associated Metadata Manager Service and specify the Metadata Manager warehouse details to run Metadata Manager Reports.
- Data Profiling warehouse. Choose the Data Profiling option and specify the data profiling warehouse details to run Data Profiling Reports.
- Other reporting sources. Choose the Other Reporting Sources option and specify the data warehouse details to run custom reports.

Data Analyzer stores metadata for schemas, metrics and attributes, queries, reports, user profiles, and other objects in the Data Analyzer repository. When you create a Reporting Service, specify the Data Analyzer repository details. The Reporting Service configures the Data Analyzer repository with the metadata corresponding to the selected data source.

You can create multiple Reporting Services on the same node. Specify a data source for each Reporting Service. To use multiple data sources with a single Reporting Service, create additional data sources in Data Analyzer. After you create the data sources, follow the instructions in the *Data Analyzer Schema Designer Guide* to import table definitions and create metrics and attributes for the reports.

When you enable the Reporting Service, the Administrator tool starts Data Analyzer. Click the URL in the Properties view to access Data Analyzer.

The name of the Reporting Service is the name of the Data Analyzer instance and the context path for the Data Analyzer URL. The Data Analyzer context path can include only alphanumeric characters, hyphens (-), and underscores (_). If the name of the Reporting Service includes any other character, PowerCenter replaces the

invalid characters with an underscore and the Unicode value of the character. For example, if the name of the Reporting Service is ReportingService#3, the context path of the Data Analyzer URL is the Reporting Service name with the # character replaced with _35. For example:

```
http://<HostName>:<PortNumber>/ReportingService_353
```

PowerCenter Repository Reports

When you choose the PowerCenter repository as a data source, you can run the PowerCenter Repository Reports from Data Analyzer.

PowerCenter Repository Reports are prepackaged dashboards and reports that allow you to analyze the following types of PowerCenter repository metadata:

- Source and target metadata. Includes shortcuts, descriptions, and corresponding database names and field-level attributes.
- Transformation metadata in mappings and mapplets. Includes port-level details for each transformation.
- Mapping and mapplet metadata. Includes the targets, transformations, and dependencies for each mapping.
- Workflow and worklet metadata. Includes schedules, instances, events, and variables.
- Session metadata. Includes session execution details and metadata extensions defined for each session.
- Change management metadata. Includes versions of sources, targets, labels, and label properties.
- Operational metadata. Includes run-time statistics.

Metadata Manager Repository Reports

When you choose the Metadata Manager warehouse as a data source, you can run the Metadata Manager Repository Reports from Data Analyzer.

Metadata Manager is the PowerCenter metadata management and analysis tool.

You can create a single Reporting Service for a Metadata Manager warehouse.

Data Profiling Reports

When you choose the Data Profiling warehouse as a data source, you can run the Data Profiling reports from Data Analyzer.

Use the Data Profiling dashboard to access the Data Profiling reports. Data Analyzer provides the following types of reports:

- Composite reports. Display a set of sub-reports and the associated metadata. The sub-reports can be multiple report types in Data Analyzer.
- Metadata reports. Display basic metadata about a data profile. The Metadata reports provide the source-level and column-level functions in a data profile, and historic statistics on previous runs of the same data profile.
- Summary reports. Display data profile results for source-level and column-level functions in a data profile.

Other Reporting Sources

When you choose other warehouses as data sources, you can run other reports from Data Analyzer. Create the reports in Data Analyzer and save them in the Data Analyzer repository.

Data Analyzer Repository

When you run reports for any data source, Data Analyzer uses the metadata in the Data Analyzer repository to determine the location from which to retrieve the data for the report and how to present the report.

Use the database management system client to create the Data Analyzer repository database. When you create the Reporting Service, specify the database details and select the application service or data warehouse for which you want to run the reports. When you enable the Reporting Service, PowerCenter imports the metadata for schemas, metrics and attributes, queries, reports, user profiles, and other objects to the repository tables.

Note: If you create a Reporting Service for another reporting source, you need to create or import the metadata for the data source manually.

Creating the Reporting Service

Before you create a Reporting Service, complete the following tasks:

- Create the Data Analyzer repository. Create a database for the Data Analyzer repository. If you create a Reporting Service for an existing Data Analyzer repository, you can use the existing database. When you enable a Reporting Service that uses an existing Data Analyzer repository, PowerCenter does not import the metadata for the prepackaged reports.
- Create PowerCenter Repository Services and Metadata Manager Services. To create a Reporting Service for the PowerCenter Repository Service or Metadata Manager Service, create the application service in the domain.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, click **Actions** > **New Reporting Service**.

   The New Reporting Service dialog box appears.
3. Enter the general properties for the Reporting Service.

   The following table describes the Reporting Service general properties:

Property	Description
Name	Name of the Reporting Service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the Reporting Service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the Reporting Service after you create it.
License	License that allows the use of the service. Select from the list of licenses available in the domain.
Primary Node	Node on which the service process runs. Since the Reporting Service is not highly available, it can run on one node.
Enable HTTP on port	The TCP port that the Reporting Service uses. Enter a value between 1 and 65535. Default value is 16080.

Property	Description
Enable HTTPS on port	The SSL port that the Reporting Service uses for secure connections. You can edit the value if you have configured the HTTPS port for the node where you create the Reporting Service. Enter a value between 1 and 65535 and ensure that it is not the same as the HTTP port. If the node where you create the Reporting Service is not configured for the HTTPS port, you cannot configure HTTPS for the Reporting Service. Default value is 16443.
Advanced Data Source Mode	Edit mode that determines where you can edit *Datasource* properties. When enabled, the edit mode is advanced, and the value is true. In advanced edit mode, you can edit *Datasource* and *Dataconnector* properties in the Administrator tool and the Data Analyzer instance. When disabled, the edit mode is basic, and the value is false. In basic edit mode, you can edit *Datasource* properties in the Administrator tool. **Note:** After you enable the Reporting Service in advanced edit mode, you cannot change it back to basic edit mode.

4. Click **Next**.
5. Enter the repository properties.

   The following table describes the repository properties:

Property	Description
Database Type	The type of database that contains the Data Analyzer repository.
Repository Host	The name of the machine that hosts the database server.
Repository Port	The port number on which you configure the database server listener service.
Repository Name	The name of the database server.
SID/Service Name	For database type Oracle only. Indicates whether to use the SID or service name in the JDBC connection string. For Oracle RAC databases, select from Oracle SID or Oracle Service Name. For other Oracle databases, select Oracle SID.
Repository Username	Account for the Data Analyzer repository database. Set up this account from the appropriate database client tools.
Repository Password	Repository database password corresponding to the database user.
Tablespace Name	Tablespace name for DB2 repositories. When you specify the tablespace name, the Reporting Service creates all repository tables in the same tablespace. Required if you choose DB2 as the Database Type. **Note:** Data Analyzer does not support DB2 partitioned tablespaces for the repository.
Additional JDBC Parameters	Enter additional JDBC options.

6. Click **Next**.
7. Enter the data source properties.

The following table describes the data source properties:

Property	Description
Reporting Source	Source of data for the reports. Choose from one of the following options: - Data Profiling - PowerCenter Repository Services - Metadata Manager Services - Other Reporting Sources
Data Source Driver	The database driver to connect to the data source.

Data Source JDBC URL	Displays the JDBC URL based on the database driver you select. For example, if you select the Oracle driver as your data source driver, the data source JDBC URL displays the following: jdbc:informatica:oracle://[host]:1521;SID=[sid];.
	Enter the database host name and the database service name.
	For an Oracle data source driver, specify the SID or service name of the Oracle instance to which you want to connect. To indicate the service name, modify the JDBC URL to use the ServiceName parameter:
	jdbc:informatica:oracle://[host]:1521;ServiceName=[Service Name];
	To configure Oracle RAC as a data source, specify the following URL:
	jdbc:informatica:oracle://[hostname]:1521;ServiceName=[Service Name];
	AlternateServers=(server2:1521);LoadBalancing=true

Data Source User Name	User name for the data source database. Enter the PowerCenter repository user name, the Metadata Manager repository user name, or the data warehouse user name based on the service you want to report on.
Data Source Password	Password corresponding to the data source user name.
Data Source Test Table	Displays the table name used to test the connection to the data source. The table name depends on the data source driver you select.

8. Click **Finish**.

Managing the Reporting Service

Use the Administrator tool to manage the Reporting Service and the Data Analyzer repository content.

You can use the Administrator tool to complete the following tasks:

- Configure the edit mode.
- Enable and disable a Reporting Service.
- Create contents in the repository.
- Back up contents of the repository.
- Restore contents to the repository.
- Delete contents from the repository.
- Upgrade contents of the repository.
- View last activity logs.

Note: You must disable the Reporting Service in the Administrator tool to perform tasks related to repository content.

Configuring the Edit Mode

To configure the edit mode for *Datasource*, set the Data Source Advanced Mode to false for basic mode or to true for advanced mode.

The following table describes the properties of basic and advanced mode in the Data Analyzer instance:

Component	Function	Basic Mode	Advanced Mode
Datasource	Edit the Administrator tool configured properties	No	Yes
	Enable/disable	Yes	Yes
Dataconnector	Activate/deactivate	Yes	Yes
	Edit user/group assignment	No	Yes
	Edit Primary Data Source	No	Yes
	Edit Primary Time Dimension	Yes	Yes
	Add Schema Mappings	No	Yes

Basic Mode

When you configure the Data Source Advanced Mode to be false for basic mode, you can manage *Datasource* in the Administrator tool. *Datasource* and *Dataconnector* properties are read-only in the Data Analyzer instance. You can edit the Primary Time Dimension Property of the data source. By default, the edit mode is basic.

Advanced Mode

When you configure the Data Source Advanced Mode to be true for advanced mode, you can manage *Datasource* and *Dataconnector* in the Administrator tool and the Data Analyzer instance. You cannot return to the basic edit mode after you select the advanced edit mode. *Dataconnector* has a primary data source that can be configured to JDBC, Web Service, or XML data source types.

Enabling and Disabling a Reporting Service

Use the Administrator tool to enable, disable, or recycle the Reporting Service. Disable a Reporting Service to perform maintenance or to temporarily restrict users from accessing Data Analyzer. When you disable the Reporting Service, you also stop Data Analyzer. You might recycle a service if you modified a property. When you recycle the service, the Reporting Service is disabled and enabled.

When you enable a Reporting Service, the Administrator tool starts Data Analyzer on the node designated to run the service. Click the URL in the Properties view to open Data Analyzer in a browser window and run the reports.

You can also launch Data Analyzer from the PowerCenter Client tools, from Metadata Manager, or by accessing the Data Analyzer URL from a browser.

To enable the service, select the service in the Navigator and click **Actions** > **Enable**.

To disable the service, select the service in the Navigator and click **Actions** > **Disable**.

Note: Before you disable a Reporting Service, ensure that all users are disconnected from Data Analyzer.

To recycle the service, select the service in the Navigator and click **Actions** > **Recycle**.

Creating Contents in the Data Analyzer Repository

You can create content for the Data Analyzer repository after you create the Reporting Service. You cannot create content for a repository that already includes content. In addition, you cannot enable a Reporting Service that manages a repository without content.

The database account you use to connect to the database must have the privileges to create and drop tables and indexes and to select, insert, update, or delete data from the tables.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the Reporting Service that manages the repository for which you want to create content.
3. Click **Actions** > **Repository Contents** > **Create**.
4. Select the user assigned the Administrator role for the domain.
5. Click OK.

   The activity log indicates the status of the content creation action.
6. Enable the Reporting Service after you create the repository content.

Backing Up Contents of the Data Analyzer Repository

To prevent data loss due to hardware or software problems, back up the contents of the Data Analyzer repository.

When you back up a repository, the Reporting Service saves the repository to a binary file, including the repository objects, connection information, and code page information. If you need to recover the repository, you can restore the content of the repository from the backup file.

When you back up the Data Analyzer repository, the Reporting Service stores the file in the backup location specified for the node where the service runs. You specify the backup location when you set up the node. View the general properties of the node to determine the path of the backup directory.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the Reporting Service that manages the repository content you want to back up.
3. Click **Actions** > **Repository Contents** > **Back Up**.
4. Enter a file name for the repository backup file.

   The backup operation copies the backup file to the following location:

   ```
   <node_backup_directory>/da_backups/
   ```

   Or you can enter a full directory path with the backup file name to copy the backup file to a different location.
5. To overwrite an existing file, select Replace Existing File.
6. Click OK.

   The activity log indicates the results of the backup action.

Restoring Contents to the Data Analyzer Repository

You can restore metadata from a repository backup file. You can restore a backup file to an empty database or an existing database. If you restore the backup file on an existing database, the restore operation overwrites the existing contents.

The database account you use to connect to the database must have the privileges to create and drop tables and indexes and to select, insert, update, or delete data from the tables.

To restore contents to the Data Analyzer repository:

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the Reporting Service that manages the repository content you want to restore.
3. Click **Actions** > **Repository Contents** > **Restore**.
4. Select a repository backup file, or select other and provide the full path to the backup file.
5. Click OK.

   The activity log indicates the status of the restore operation.

Deleting Contents from the Data Analyzer Repository

Delete repository content when you want to delete all metadata and repository database tables from the repository.

You can delete the repository content if the metadata is obsolete. Deleting repository content is an irreversible action. If the repository contains information that you might need later, back up the repository before you delete it.

To delete the contents of the Data Analyzer repository:

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the Reporting Service that manages the repository content you want to delete.
3. Click **Actions** > **Repository Contents** > **Delete**.
4. Verify that you backed up the repository before you delete the contents.
5. Click OK.

   The activity log indicates the status of the delete operation.

Upgrading Contents of the Data Analyzer Repository

When you create a Reporting Service, you can specify the details of an existing version of the Data Analyzer repository. You need to upgrade the contents of the repository to ensure that the repository contains the objects and metadata of the latest version.

Viewing Last Activity Logs

You can view the status of the activities that you perform on the Data Analyzer repository contents. The activity logs contain the status of the last activity that you performed on the Data Analyzer repository.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the Reporting Service for which you want to view the last activity log.
3. Click **Actions** > **Last Activity Log**.

   The Last Activity Log displays the activity status.

Configuring the Reporting Service

After you create a Reporting Service, you can configure it. Use the Administrator tool to view or edit the following Reporting Service properties:

- General Properties. Include the Data Analyzer license key used and the name of the node where the service runs.

- Reporting Service Properties. Include the TCP port where the Reporting Service runs, the SSL port if you have specified it, and the Data Source edit mode.
- Data Source Properties. Include the data source driver, the JDBC URL, and the data source database user account and password.
- Repository Properties. Include the Data Analyzer repository database user account and password.

To view and update properties, select the Reporting Service in the Navigator. In the Properties view, click Edit in the properties section that you want to edit.

General Properties

You can view and edit the general properties after you create the Reporting Service.

Click Edit in the General Properties section to edit the general properties.

The following table describes the general properties:

Property	Description
Name	Name of the Reporting Service.
Description	Description of the Reporting Service.
License	License that allows you to run the Reporting Service. To apply changes, restart the Reporting Service.
Node	Node on which the Reporting Service runs. You can move a Reporting Service to another node in the domain. Informatica disables the Reporting Service on the original node and enables it in the new node. You can see the Reporting Service on both the nodes, but it runs only on the new node. If you move the Reporting Service to another node, you must reapply the custom color schemes to the Reporting Service. Informatica does not copy the color schemes to the Reporting Service on the new node, but retains them on the original node.

Reporting Service Properties

You can view and edit the Reporting Service properties after you create the Reporting Service.

Click Edit in the Reporting Service Properties section to edit the properties.

The following table describes the Reporting Service properties:

Property	Description
HTTP Port	The TCP port that the Reporting Service uses. You can change this value. To apply changes, restart the Reporting Service.
HTTPS Port	The SSL port that the Reporting Service uses for secure connections. You can edit the value if you have configured the HTTPS port for the node where you create the Reporting Service. If the node where you create the Reporting Service is not configured for the HTTPS port, you cannot configure HTTPS for the Reporting Service. To apply changes, restart the Reporting Service.
Data Source Advanced Mode	Edit mode that determines where you can edit Datasource properties. When enabled, the edit mode is advanced, and the value is true. In advanced edit mode, you can edit Datasource and Dataconnector properties in the Data Analyzer instance. When disabled, the edit mode is basic, and the value is false. In basic edit mode, you can edit Datasource properties in the Administrator tool.

Property	Description
	Note: After you enable the Reporting Service in advanced edit mode, you cannot change it back to basic edit mode.

Note: If multiple Reporting Services run on the same node, you need to stop all the Reporting Services on that node to update the port configuration.

Data Source Properties

You must specify a reporting source for the Reporting Service. The Reporting Service creates the following objects in Data Analyzer for the reporting source:

- A data source with the name *Datasource*
- A data connector with the name *Dataconnector*

Use the Administrator tool to manage the data source and data connector for the reporting source. To view or edit the *Datasource* or *Dataconnector* in the advanced mode, click the data source or data connector link in the Administrator tool.

You can create multiple data sources in Data Analyzer. You manage the data sources you create in Data Analyzer within Data Analyzer. Changes you make to data sources created in Data Analyzer will not be lost when you restart the Reporting Service.

The following table describes the data source properties that you can edit:

Property	Description
Reporting Source	The service which the Reporting Service uses as the data source.
Data Source Driver	The driver that the Reporting Service uses to connect to the data source.
Data Source JDBC URL	The JDBC connect string that the Reporting Service uses to connect to the data source.
Data Source User Name	The account for the data source database.
Data Source Password	Password corresponding to the data source user.
Data Source Test Table	The test table that the Reporting Service uses to verify the connection to the data source.

Code Page Override

By default, when you create a Reporting Service to run reports against a PowerCenter repository or Metadata Manager warehouse, the Service Manager adds the CODEPAGEOVERRIDE parameter to the JDBC URL. The Service Manager sets the parameter to a code page that the Reporting Service uses to read data in the PowerCenter repository or Metadata Manager warehouse.

If you use a PowerCenter repository or Metadata Manager warehouse as a reporting data source and the reports do not display correctly, verify that the code page set in the JDBC URL for the Reporting Service matches the code page for the PowerCenter Service or Metadata Manager Service.

Repository Properties

Repository properties provide information about the database that stores the Data Analyzer repository metadata. Specify the database properties when you create the Reporting Service. After you create a Reporting Service, you can modify some of these properties.

Note: If you edit a repository property or restart the system that hosts the repository database, you need to restart the Reporting Service.

Click Edit in the Repository Properties section to edit the properties.

The following table describes the repository properties that you can edit:

Property	Description
Database Driver	The JDBC driver that the Reporting Service uses to connect to the Data Analyzer repository database. To apply changes, restart the Reporting Service.
Repository Host	Name of the machine that hosts the database server. To apply changes, restart the Reporting Service.
Repository Port	The port number on which you have configured the database server listener service. To apply changes, restart the Reporting Service.
Repository Name	The name of the database service. To apply changes, restart the Reporting Service.
SID/Service Name	For repository type Oracle only. Indicates whether to use the SID or service name in the JDBC connection string. For Oracle RAC databases, select from Oracle SID or Oracle Service Name. For other Oracle databases, select Oracle SID.
Repository User	Account for the Data Analyzer repository database. To apply changes, restart the Reporting Service.
Repository Password	Data Analyzer repository database password corresponding to the database user. To apply changes, restart the Reporting Service.
Tablespace Name	Tablespace name for DB2 repositories. When you specify the tablespace name, the Reporting Service creates all repository tables in the same tablespace. To apply changes, restart the Reporting Service.
Additional JDBC Parameters	Enter additional JDBC options.

Granting Users Access to Reports

Limit access to Data Analyzer to secure information in the Data Analyzer repository and data sources. To access Data Analyzer, each user needs an account to perform tasks and access data. Users can perform tasks based on their privileges.

You can grant access to users through the following components:

- User accounts. Create users in the Informatica domain. Use the Security tab of the Administrator tool to create users.
- Privileges and roles. You assign privileges and roles to users and groups for a Reporting Service. Use the Security tab of the Administrator tool to assign privileges and roles to a user.
- Permissions. You assign Data Analyzer permissions in Data Analyzer.

CHAPTER 23

SAP BW Service

This chapter includes the following topics:

- SAP BW Service Overview, 308
- Creating the SAP BW Service, 309
- Enabling and Disabling the SAP BW Service, 310
- Configuring the SAP BW Service Properties, 311
- Configuring the Associated Integration Service, 312
- Configuring the SAP BW Service Processes, 312
- Viewing Log Events, 313

SAP BW Service Overview

If you are using PowerExchange for SAP NetWeaver BI, use the Administrator tool to manage the SAP BW Service. The SAP BW Service is an application service that performs the following tasks:

- Listens for RFC requests from SAP NetWeaver BI.
- Initiates workflows to extract from or load to SAP NetWeaver BI.
- Sends log events to the PowerCenter Log Manager.

Use the Administrator tool to complete the following SAP BW Service tasks:

- Create the SAP BW Service.
- Enable and disable the SAP BW Service.
- Configure the SAP BW Service properties.
- Configure the associated PowerCenter Integration Service.
- Configure the SAP BW Service processes.
- Configure permissions on the SAP BW Service.
- View messages that the SAP BW Service sends to the PowerCenter Log Manager.

Load Balancing for the SAP NetWeaver BI System and the SAP BW Service

You can configure the SAP NetWeaver BI system to use load balancing. To support an SAP NetWeaver BI system configured for load balancing, the SAP BW Service records the host name and system number of the SAP NetWeaver BI server requesting data from PowerCenter. The SAP BW Service passes this information to the

PowerCenter Integration Service. The PowerCenter Integration Service uses this information to load data to the same SAP NetWeaver BI server that made the request. For more information about configuring the SAP NetWeaver BI system to use load balancing, see the SAP NetWeaver BI documentation.

You can also configure the SAP BW Service in PowerCenter to use load balancing. If the load on the SAP BW Service becomes too high, you can create multiple instances of the SAP BW Service to balance the load. To run multiple SAP BW Services configured for load balancing, create each service with a unique name but use the same values for all other parameters. The services can run on the same node or on different nodes. The SAP NetWeaver BI server distributes data to the multiple SAP BW Services in a round-robin fashion.

Creating the SAP BW Service

Use the Administrator tool to create the SAP BW Service.

1. In the Administrator tool, click Create > SAP BW Service.

   The Create New SAP BW Service window appears.

2. Configure the SAP BW Service options.

   The following table describes the information to enter in the Create New SAP BW Service window:

Property	Description
Name	Name of the SAP BW Service. The characters must be compatible with the code page of the associated repository. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the SAP BW Service. The description cannot exceed 765 characters.
Location	Name of the domain and folder in which the SAP BW Service is created. the Administrator tool creates the SAP BW Service in the domain where you are connected. Click Select Folder to select a new folder in the domain.
License	PowerCenter license.
Node	Node on which this service runs.
SAP Destination R Type	Type R DEST entry in the saprfc.ini file created for the SAP BW Service.
Associated Integration Service	PowerCenter Integration Service associated with the SAP BW Service.
Repository User Name	Account used to access the repository.
Repository Password	Password for the user.

3. Click OK.

   The SAP BW Service properties window appears.

Enabling and Disabling the SAP BW Service

Use the Administrator tool to enable and disable the SAP BW Service. You might disable the SAP BW Service if you need to perform maintenance on the machine. Enable the disabled SAP BW Service to make it available again.

Before you enable the SAP BW Service, you must define PowerCenter as a logical system in SAP NetWeaver BI.

When you enable the SAP BW Service, the service starts. If the service cannot start, the domain tries to restart the service based on the restart options configured in the domain properties.

If the service is enabled but fails to start after reaching the maximum number of attempts, the following message appears:

```
The SAP BW Service <service name> is enabled.
The service did not start. Please check the logs for more information.
```

You can review the logs for this SAP BW Service to determine the reason for failure and fix the problem. After you fix the problem, disable and re-enable the SAP BW Service to start it.

When you enable the SAP BW Service, it tries to connect to the associated PowerCenter Integration Service. If the PowerCenter Integration Service is not enabled and the SAP BW Service cannot connect to it, the SAP BW Service still starts successfully. When the SAP BW Service receives a request from SAP NetWeaver BI to start a PowerCenter workflow, the service tries to connect to the associated PowerCenter Integration Service again. If it cannot connect, the SAP BW Service returns the following message to the SAP NetWeaver BI system:

```
The SAP BW Service could not find Integration Service <service name> in domain <domain name>.
```

To resolve this problem, verify that the PowerCenter Integration Service is enabled and that the domain name and PowerCenter Integration Service name entered in the 3rd Party Selection tab of the InfoPackage are valid. Then restart the process chain in the SAP NetWeaver BI system.

When you disable the SAP BW Service, choose one of the following options:

- Complete. Disables the SAP BW Service after all service processes complete.
- Abort. Aborts all processes immediately and then disables the SAP BW Service. You might choose abort if a service process stops responding.

Enabling the SAP BW Service

1. In the Domain Navigator of the Administrator tool, select the SAP BW Service.
2. Click Actions > Enable.

Disabling the SAP BW Service

1. In the Domain Navigator of the Administrator tool, select the SAP BW Service.
2. Click Actions > Disable.

   The Disable SAP BW Service window appears.
3. Choose the disable mode and click OK.

Configuring the SAP BW Service Properties

Use the Properties tab in the Administrator tool to configure general properties for the SAP BW Service and to configure the node on which the service runs.

1. Select the SAP BW Service in the Domain Navigator.

   The SAP BW Service properties window appears.
2. In the Properties tab, click Edit for the general properties to edit the description.
3. Select the node on which the service runs.
4. To edit the properties of the service, click Edit for the category of properties you want to update.
5. Update the values of the properties.

General Properties

The following table describes the general properties for an SAP BW service:

Property	Description
Name	Name of the SAP BW Service. The characters must be compatible with the code page of the associated repository. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the SAP BW Service. The description cannot exceed 255 characters.
License	PowerCenter license.
Node	Node on which this service runs.

SAP BW Service Properties

The following table describes the general properties for an SAP BW service:

Property	Description
SAP Destination R Type	Type R DEST entry in the saprfc.ini file created for the SAP BW Service. Edit this property if you have created a different type R DEST entry in sapfrc.ini for the SAP BW Service.
RetryPeriod	Number of seconds the SAP BW Service waits before trying to connect to the SAP NetWeaver BI system if a previous connection failed. The SAP BW Service tries to connect five times. Between connection attempts, it waits the number of seconds you specify. After five unsuccessful attempts, the SAP BW Service shuts down. Default is 5.

Configuring the Associated Integration Service

Use the Associated Integration Service tab in the Administrator Tool to configure connection information for the repository database and PowerCenter Integration Service.

1. Select the SAP BW Service in the Domain Navigator.

   The SAP BW Service properties window appears.
2. Click Associated Integration Service.
3. Click Edit.
4. Edit the following properties:

Property	Description
Associated Integration Service	PowerCenter Integration Service name to which the SAP BW Service connects.
Repository User Name	Account used to access the repository.
Repository Password	Password for the user.

5. Click OK.

Configuring the SAP BW Service Processes

Use the Processes tab in the Administrator tool to configure the temporary parameter file directory that the SAP BW Service uses when you filter data to load into SAP NetWeaver BI.

1. Select the SAP BW Service in the Navigator.

   The SAP BW Service properties window appears.
2. Click Processes.
3. Click Edit.
4. Edit the following property:

Property	Description
ParamFileDir	Temporary parameter file directory. The SAP BW Service stores SAP NetWeaver BI data selection entries in the parameter file when you filter data to load into SAP NetWeaver BI. The directory must exist on the node running the SAP BW Service. Verify that the directory you specify has read and write permissions enabled. The default directory is /Infa_Home/server/infa_shared/BWParam.

Viewing Log Events

The SAP BW Service sends log events to the Log Manager. The SAP BW Service captures log events that track interactions between PowerCenter and SAP NetWeaver BI. You can view SAP BW Service log events in the following locations:

- The Administrator tool. On the Logs tab, enter search criteria to find log events that the SAP BW Service captures when extracting from or loading into SAP NetWeaver BI.
- SAP NetWeaver BI Monitor. In the Monitor - Administrator Workbench window, you can view log events that the SAP BW Service captures for an InfoPackage that is included in a process chain to load data into SAP NetWeaver BI. SAP NetWeaver BI pulls the messages from the SAP BW Service and displays them in the monitor. The SAP BW Service must be running to view the messages in the SAP NetWeaver BI Monitor.

To view log events about how the PowerCenter Integration Service processes an SAP NetWeaver BI workflow, view the session or workflow log.

CHAPTER 24

Web Services Hub

This chapter includes the following topics:

- Web Services Hub Overview, 314
- Creating a Web Services Hub, 315
- Enabling and Disabling the Web Services Hub, 316
- Configuring the Web Services Hub Properties, 317
- Configuring the Associated Repository, 321

Web Services Hub Overview

The Web Services Hub Service is an application service in the Informatica domain that exposes PowerCenter functionality to external clients through web services. It receives requests from web service clients and passes them to the PowerCenter Integration Service or PowerCenter Repository Service. The PowerCenter Integration Service or PowerCenter Repository Service processes the requests and sends a response to the Web Services Hub. The Web Services Hub sends the response back to the web service client.

The Web Services Hub Console does not require authentication. You do not need to log in when you start the Web Services Hub Console. On the Web Services Hub Console, you can view the properties and the WSDL of any web service. You can test any web service running on the Web Services Hub. However, when you test a protected service you must run the login operation before you run the web service.

You can use the Administrator tool to complete the following tasks related to the Web Services Hub:

- Create a Web Services Hub. You can create multiple Web Services Hub Services in a domain.
- Enable or disable the Web Services Hub. You must enable the Web Services Hub to run web service workflows. You can disable the Web Services Hub to prevent external clients from accessing the web services while performing maintenance on the machine or modifying the repository.
- Configure the Web Services Hub properties. You can configure Web Services Hub properties such as the length of time a session can remain idle before time out and the character encoding to use for the service.
- Configure the associated repository. You must associate a repository with a Web Services Hub. The Web Services Hub exposes the web-enabled workflows in the associated repository.
- View the logs for the Web Services Hub. You can view the event logs for the Web Services Hub in the Log Viewer.
- Remove a Web Services Hub. You can remove a Web Services Hub if it becomes obsolete.

Creating a Web Services Hub

Create a Web Services Hub to run web service workflows so that external clients can access PowerCenter functionality as web services.

You must associate a PowerCenter repository with the Web Services Hub before you run it. You can assign the PowerCenter repository when you create the Web Services Hub or after you create the Web Services Hub. The PowerCenter repository that you assign to the Web Services Hub is called the associated repository. The Web Services Hub runs web service workflows that are in the associated repository.

By default, the Web Services Hub has the same code page as the node on which it runs. When you associate a PowerCenter repository with the Web Services Hub, the code page of the Web Services Hub must be a subset of the code page of the associated repository.

If the domain contains multiple nodes and you create a secure Web Services Hub, you must generate the SSL certificate for the Web Services Hub on a gateway node and import the certificate into the certificate file of the same gateway node.

1. In the Administrator tool, select the Domain tab.
2. On the Navigator Actions menu, click New > Web Services Hub.

   The New Web Services Hub Service window appears.
3. Configure the properties of the Web Services Hub.

   The following table describes the properties for a Web Services Hub:

Property	Description
Name	Name of the Web Services Hub. The characters must be compatible with the code page of the associated repository. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the Web Services Hub. The description cannot exceed 765 characters.
Location	Domain folder in which the Web Services Hub is created. Click Browse to select the folder in the domain where you want to create the Web Services Hub.
License	License to assign to the Web Services Hub. If you do not select a license now, you can assign a license to the service later. Required before you can enable the Web Services Hub.
Node	Node on which the Web Services Hub runs. A Web Services Hub runs on a single node. A node can run more than one Web Services Hub.
Associated Repository Service	PowerCenter Repository Service to which the Web Services Hub connects. The repository must be enabled before you can associate it with a Web Services Hub. If you do not select an associated repository when you create a Web Services Hub, you can add an associated repository later.
Repository User Name	User name to access the repository.
Repository Password	Password for the user.
Security Domain	Security domain for the user. Appears when the Informatica domain contains an LDAP security domain.

Property	Description
URLScheme	Indicates the security protocol that you configure for the Web Services Hub: - HTTP. Run the Web Services Hub on HTTP only. - HTTPS. Run the Web Services Hub on HTTPS only. - HTTP and HTTPS. Run the Web Services Hub in HTTP and HTTPS modes.
HubHostName	Name of the machine hosting the Web Services Hub.
HubPortNumber (http)	Port number for the Web Services Hub on HTTP. Required if you choose to run the Web Services Hub on HTTP. Default is 7333.
HubPortNumber (https)	Port number for the Web Services Hub on HTTPS. Appears when the URL scheme selected includes HTTPS. Required if you choose to run the Web Services Hub on HTTPS. Default is 7343.
KeystoreFile	Path and file name of the keystore file that contains the keys and certificates required if you use the SSL security protocol with the Web Services Hub. Required if you run the Web Services Hub on HTTPS.
Keystore Password	Password for the keystore file. The value of this property must match the password you set for the keystore file. If this property is empty, the Web Services Hub assumes that the password for the keystore file is the default password *changeit*.
InternalHostName	Host name on which the Web Services Hub listens for connections from the PowerCenter Integration Service. If not specified, the default is the Web Services Hub host name. **Note:** If the host machine has more than one network card that results in multiple IP addresses for the host machine, set the value of InternalHostName to the internal IP address.
InternalPortNumber	Port number on which the Web Services Hub listens for connections from the PowerCenter Integration Service. Default is 15555.

4. Click Create.

After you create the Web Services Hub, the Administrator tool displays the URL for the Web Services Hub Console. If you run the Web Services Hub on HTTP and HTTPS, the Administrator tool displays the URL for both.

If you configure a logical URL for an external load balancer to route requests to the Web Services Hub, the Administrator tool also displays the URL.

Click the service URL to start the Web Services Hub Console from the Administrator tool. If the Web Services Hub is not enabled, you cannot connect to the Web Services Hub Console.

Related Topics:

- "Running the Web Services Report for a Secure Web Services Hub" on page 411

Enabling and Disabling the Web Services Hub

Use the Administrator tool to enable or disable a Web Services Hub. You can disable a Web Services Hub to perform maintenance or to temporarily restrict users from accessing web services. Enable a disabled Web Services Hub to make it available again.

The PowerCenter Repository Service associated with the Web Services Hub must be running before you enable the Web Services Hub. If a Web Services Hub is associated with multiple PowerCenter Repository Services, at least one of the PowerCenter Repository Services must be running before you enable the Web Services Hub.

If you enable the service but it fails to start, review the logs for the Web Services Hub to determine the reason for the failure. After you resolve the problem, you must disable and then enable the Web Services Hub to start it again.

When you disable a Web Services Hub, you must choose the mode to disable it in. You can choose one of the following modes:

- Stop. Stops all web enabled workflows and disables the Web Services Hub.
- Abort. Aborts all web-enabled workflows immediately and disables the Web Services Hub.

To disable or enable a Web Services Hub:

1. In the Administrator tool, select the Domain tab.
2. In the Navigator, select the Web Services Hub.

   When a Web Services Hub is running, the Disable button is available.
3. To disable the service, click the Disable the Service button.

   The Disable Web Services Hub window appears.
4. Choose the disable mode and click OK.

   The Service Manager disables the Web Services Hub. When a service is disabled, the Enable button is available.
5. To enable the service, click the Enable the Service button.
6. To disable the Web Services Hub with the default disable mode and then immediately enable the service, click the Restart the Service button.

   By default, when you restart a Web Services Hub, the disable mode is Stop.

Configuring the Web Services Hub Properties

After you create a Web Services Hub, you can configure it. Use the Administrator tool to view or edit the following Web Services Hub properties:

- General properties. Configure general properties such as license and node.
- Service properties. Configure service properties such as host name and port number.
- Advanced properties. Configure advanced properties such as the level of errors written to the Web Services Hub logs.
- Custom properties. Include properties that are unique to the Informatica environment or that apply in special cases. A Web Services Hub does not have custom properties when you create it. Create custom properties only in special circumstances and only on advice from Informatica Global Customer Support.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a Web Services Hub.
3. To view the properties of the service, click the Properties view.
4. To edit the properties of the service, click Edit for the category of properties you want to update.

   The Edit Web Services Hub Service window displays the properties in the category.
5. Update the values of the properties.

General Properties

Select the node on which to run the Web Services Hub. You can run multiple Web Services Hub on the same node.

Disable the Web Services Hub before you assign it to another node. To edit the node assignment, select the Web Services Hub in the Navigator, click the Properties tab, and then click Edit in the Node Assignments section. Select a new node.

When you change the node assignment for a Web Services Hub, the host name for the web services running on the Web Services Hub changes. You must update the host name and port number of the Web Services Hub to match the new node. Update the following properties of the Web Services Hub:

- HubHostName
- InternalHostName

To access the Web Services Hub on a new node, you must update the client application to use the new host name. For example, you must regenerate the WSDL for the web service to update the host name in the endpoint URL. You must also regenerate the client proxy classes to update the host name.

The following table describes the general properties for a Web Services Hub:

Property	Description
Name	Name of the Web Services Hub service.
Description	Description of the Web Services Hub.
License	License assigned to the Web Services Hub.
Node	Node on which the Web Services Hub runs.

Service Properties

You must restart the Web Services Hub before changes to the service properties can take effect.

The following table describes the service properties for a Web Services Hub:

Property	Description
HubHostName	Name of the machine hosting the Web Services Hub. Default is the name of the machine where the Web Services Hub is running. If you change the node on which the Web Services Hub runs, update this property to match the host name of the new node. To apply changes, restart the Web Services Hub.
HubPortNumber (http)	Port number for the Web Services Hub running on HTTP. Required if you run the Web Services Hub on HTTP. Default is 7333. To apply changes, restart the Web Services Hub.
HubPortNumber (https)	Port number for the Web Services Hub running on HTTPS. Required if you run the Web Services Hub on HTTPS. Default is 7343. To apply changes, restart the Web Services Hub.
CharacterEncoding	Character encoding for the Web Services Hub. Default is UTF-8. To apply changes, restart the Web Services Hub.
URLScheme	Indicates the security protocol that you configure for the Web Services Hub: - HTTP. Run the Web Services Hub on HTTP only. - HTTPS. Run the Web Services Hub on HTTPS only. - HTTP and HTTPS. Run the Web Services Hub in HTTP and HTTPS modes.

Property	Description
	If you run the Web Services Hub on HTTPS, you must provide information on the keystore file. To apply changes, restart the Web Services Hub.
InternalHostName	Host name on which the Web Services Hub listens for connections from the Integration Service. If you change the node assignment of the Web Services Hub, update the internal host name to match the host name of the new node. To apply changes, restart the Web Services Hub.
InternalPortNumber	Port number on which the Web Services Hub listens for connections from the Integration Service. Default is 15555. To apply changes, restart the Web Services Hub.
KeystoreFile	Path and file name of the keystore file that contains the keys and certificates required if you use the SSL security protocol with the Web Services Hub. Required if you run the Web Services Hub on HTTPS.
KeystorePass	Password for the keystore file. The value of this property must match the password you set for the keystore file.

Advanced Properties

The following table describes the advanced properties for a Web Services Hub:

Property	Description
HubLogicalAddress	URL for the third party load balancer that manages the Web Services Hub. This URL is published in the WSDL for all web services that run on a Web Services Hub managed by the load balancer.
DTMTimeout	Length of time, in seconds, that the Web Services Hub tries to connect or reconnect to the DTM to run a session. Default is 60 seconds.
SessionExpiryPeriod	Number of seconds that a session can remain idle before the session times out and the session ID becomes invalid. The Web Services Hub resets the start of the timeout period every time a client application sends a request with a valid session ID. If a request takes longer to complete than the amount of time set in the SessionExpiryPeriod property, the session can time out during the operation. To avoid timing out, set the SessionExpiryPeriod property to a higher value. The Web Services Hub returns a fault response to any request with an invalid session ID. Default is 3600 seconds. You can set the SessionExpiryPeriod between 1 and 2,592,000 seconds.
MaxISConnections	Maximum number of connections to the PowerCenter Integration Service that can be open at one time for the Web Services Hub. Default is 20.
Log Level	Level of Web Services Hub error messages to include in the logs. These messages are written to the Log Manager and log files. Specify one of the following severity levels: - Fatal. Writes FATAL code messages to the log. - Error. Writes ERROR and FATAL code messages to the log. - Warning. Writes WARNING, ERROR, and FATAL code messages to the log. - Info. Writes INFO, WARNING, and ERROR code messages to the log. - Trace. Writes TRACE, INFO, WARNING, ERROR, and FATAL code messages to the log. - Debug. Writes DEBUG, INFO, WARNING, ERROR, and FATAL code messages to the log. Default is INFO.

Property	Description
MaxConcurrentRequests	Maximum number of request processing threads allowed, which determines the maximum number of simultaneous requests that can be handled. Default is 100.
MaxQueueLength	Maximum queue length for incoming connection requests when all possible request processing threads are in use. Any request received when the queue is full is rejected. Default is 5000.
MaxStatsHistory	Number of days that Informatica keeps statistical information in the history file. Informatica keeps a history file that contains information regarding the Web Services Hub activities. The number of days you set in this property determines the number of days available for which you can display historical statistics in the Web Services Report page of the Administrator tool.
Maximum Heap Size	Amount of RAM allocated to the Java Virtual Machine (JVM) that runs the Web Services Hub. Use this property to increase the performance. Append one of the following letters to the value to specify the units: - b for bytes. - k for kilobytes. - m for megabytes. - g for gigabytes. Default is 512 megabytes.
JVM Command Line Options	Java Virtual Machine (JVM) command line options to run Java-based programs. When you configure the JVM options, you must set the Java SDK classpath, Java SDK minimum memory, and Java SDK maximum memory properties. You must set the following JVM command line option: - Dfile.encoding. File encoding. Default is UTF-8.

Use the MaxConcurrentRequests property to set the number of clients that can connect to the Web Services Hub and the MaxQueueLength property to set the number of client requests the Web Services Hub can process at one time.

You can change the parameter values based on the number of clients you expect to connect to the Web Services Hub. In a test environment, set the parameters to smaller values. In a production environment, set the parameters to larger values. If you increase the values, more clients can connect to the Web Services Hub, but the connections use more system resources.

Custom Properties

You can edit custom properties for a Web Services Hub.

The following table describes the custom properties:

Property	Description
Custom Property Name	Configure a custom property that is unique to your environment or that you need to apply in special cases. Enter the property name and an initial value. Use custom properties only if Informatica Global Customer Support instructs you to do so.

Configuring the Associated Repository

To expose web services through the Web Services Hub, you must associate the Web Services Hub with a repository. The code page of the Web Services Hub must be a subset of the code page of the associated repository.

When you associate a repository with a Web Services Hub, you specify the PowerCenter Repository Service and the user name and password used to connect to the repository. The PowerCenter Repository Service that you associate with a Web Services Hub must be in the same domain as the Web Services Hub.

You can associate more than one repository with a Web Services Hub. When you associate more than one repository with a Web Services Hub, the Web Services Hub can run web services located in any of the associated repositories.

You can associate more than one Web Services Hub with a PowerCenter repository. When you associate more than one Web Services Hub with a PowerCenter repository, multiple Web Services Hub Services can provide the same web services. Different Web Services Hub Services can run separate instances of a web service. You can use an external load balancer to manage the Web Services Hub Services.

When you associate a Web Services Hub with a PowerCenter Repository Service, the Repository Service does not have to be running. After you start the Web Services Hub, it periodically checks whether the PowerCenter Repository Services have started. The PowerCenter Repository Service must be running before the Web Services Hub can run a web service workflow.

Adding an Associated Repository

If you associate multiple PowerCenter repositories with a Web Services Hub, external clients can access web services from different repositories through the same Web Services Hub.

1. On the Navigator of the Administrator tool, select the Web Services Hub.
2. Click the Associated Repository tab.
3. Click Add.

   The Select Repository section appears.
4. Enter the properties for the associated repository.

Property	Description
Associated Repository Service	Name of the PowerCenter Repository Service to which the Web Services Hub connects. To apply changes, restart the Web Services Hub.
Repository User Name	User name to access the repository.
Repository Password	Password for the user.
Security Domain	Security domain for the user. Appears when the Informatica domain contains an LDAP security domain.

5. Click OK to save the associated repository properties.

Editing an Associated Repository

If you want to change the repository that associated with the Web Services Hub, edit the properties of the associated repository.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the Web Services Hub for which you want to change an associated repository.
3. Click the Associated Repository view.
4. In the section for the repository you want to edit, click Edit.

   The Edit associated repository window appears.
5. Edit the properties for the associated repository.

Property	Description
Associated Repository Service	Name of the PowerCenter Repository Service to which the Web Services Hub connects. To apply changes, restart the Web Services Hub.
Repository User Name	User name to access the repository.
Repository Password	Password for the user.
Security Domain	Security domain for the user. Appears when the Informatica domain contains an LDAP security domain.

6. Click OK to save the changes to the associated repository properties.

CHAPTER 25

Connection Management

This chapter includes the following topics:

- Connection Management Overview, 323
- Connection Pooling, 324
- Creating a Connection, 327
- Configuring Pooling for a Connection, 328
- Viewing a Connection, 329
- Editing and Testing a Connection, 329
- Deleting a Connection, 330
- Connection Properties, 330
- Pooling Properties, 338

Connection Management Overview

A connection is a repository object that defines a connection in the domain configuration repository.

The Data Integration Service uses the database connections to process integration objects for the Developer tool and the Analyst tool. Integration objects include mappings, data profiles, scorecards, and SQL data services.

Connections are organized into the following connection types:

- Relational database connections. DB2, DB2 for i5/OS, DB2 for z/OS, ODBC, Oracle, and Microsoft SQL Server.
- Nonrelational database connections. Adabas, IMS, Sequential, and VSAM.
- Enterprise application connection. SAP.
- Web service connection.

You can configure connection pooling to optimize processing for the Data Integration Service. Connection pooling is a framework to cache connections.

Tools Reference for Creating and Managing Connections

You can use the Analyst tool, Developer tool, Administrator tool, and the infacmd isp command to create and manage connections.

You complete the following tasks to manage connections:

- View

- Edit
- Manage permissions
- Test
- Delete

You cannot use connections that you create in the Administrator tool, Developer tool, or Analyst tool in PowerCenter sessions.

Use the following tools to complete the following tasks for the following types of connections:

Tool or Command	Connection Type	Tasks
Administrator Tool	Relational database connections	Create and manage.
	Nonrelational database, enterprise application, and web service connections	Manage. You cannot test these types of connections.
Analyst Tool	The following relational data connections: - DB2 - ODBC - Oracle - Microsoft SQL Server	Create and delete.
Developer Tool	All	Create and manage. For a connection of any type that was created in another tool or through the infacmd isp CreateConnection command, you can manage the connection.
infacmd isp commands	All	Create and manage. For a connection of any type that was created in another tool, you can manage the connection.

Connection Pooling

Connection pooling is a framework to cache database connection information that is used by the Data Integration Service. It increases performance through the reuse of cached connection information.

Each Data Integration Service maintains a connection pool library. Each connection pool in the library contains connection instances for one connection object. A connection instance is a representation of a physical connection to a database.

A connection instance can be active or idle. An active connection instance is a connection instance that the Data Integration Service is using to connect to a database. A Data Integration Service can create an unlimited number of active connection instances.

An idle connection instance is a connection instance in the connection pool that is not in use. The connection pool retains idle connection instances based on the pooling properties that you configure. You configure the minimum idle connections, the maximum idle connections, and the maximum idle connection time.

When the Data Integration Service runs a data integration task, it requests a connection instance from the pool. If an idle connection instance exists, the connection pool releases it to the Data Integration Service. If the

connection pool does not have an idle connection instance, the Data Integration Service creates an active connection instance.

When the Data Integration Service completes the task, it releases the active connection instance to the pool as an idle connection instance. If the connection pool contains the maximum number of idle connection instances, the Data Integration Service drops the active connection instance instead of releasing it to the pool.

The Data Integration Service drops an idle connection instance from the pool when the following conditions are true:

- A connection instance reaches the maximum idle time.
- The connection pool exceeds the minimum number of idle connections.

When you start the Data Integration Service, it drops all connections in the pool.

Note: By default, connection pooling is enabled for Microsoft SQL Server, IBM DB2, and Oracle connections. By default, connection pooling is disabled for DB2 for i5/OS, DB2 for z/OS, IMS, Sequential, and VSAM connections. If connection pooling is disabled, the Data Integration Service creates a connection instance each time it processes an integration object. It drops the instance when it finishes processing the integration object.

Example of Connection Pooling

The administrator configures the following pooling parameters for a connection:

- Connection Pooling: Enabled
- Minimum Connections: 5
- Connection Pool Size: 15
- Maximum Idle Time: 120 seconds

When the Data Integration Service receives a request to run 40 data integration tasks, it uses the following process to maintain the connection pool:

1. The Data Integration Service receives a request to process 40 integration objects at 1:00 p.m., and it creates 40 connection instances.
2. The Data Integration Service completes processing at 1:30 p.m., and it releases 15 connections to the connection pool as idle connections.
3. It drops 25 connections because they exceed the connection pool size.
4. At 1:32 p.m., the maximum idle time is met for the idle connections, and the Data Integration Service drops 10 idle connections.
5. The Data Integration Service maintains five idle connections because the minimum connection pool size is five.

Considerations for PowerExchange Connection Pooling

Certain considerations apply to pooling the following types of PowerExchange connections:

- DB2 for i5/OS
- DB2 for z/OS
- IMS
- Sequential
- VSAM

PowerExchange Connection Pooling Behavior

PowerExchange connection pooling behaves differently from pooling for other connection types in the following ways:

- The Data Integration Service connects to a PowerExchange data source through the PowerExchange Listener. For PowerExchange connections, a connection pool is a set of connections to a PowerExchange Listener, as defined by a NODE statement in the DBMOVER file on the Data Integration Service machine. For example, if a connection pool exists for NODE1, the pool is used for all PowerExchange connections to NODE1.

  If you defined multiple connection objects for the same PowerExchange Listener, PowerExchange determines the size of the connection pool for the Listener by adding the connection pool size that you specified for each connection object.
- When PowerExchange needs a connection to a Listener, it tries to find a pooled connection with matching characteristics, including user ID and password. If PowerExchange cannot find a pooled connection with matching charactistics, it modifies and reuses a pooled connection to the Listener, if possible. For example, if PowerExchange needs a connection for USER1 on NODE1 and finds only a pooled connection for USER2 on NODE1, PowerExchange reuses the connection, signs off USER2, and signs on USER1.
- In the 9.0.1 release, PowerExchange connection pooling maintains network connections only. Files and databases are closed after each request.
- PowerExchange maintains separate internal pools for data and metadata requests. For example, if you specify a value of 3 for the Connection Pool Size property for a connection, PowerExchange creates an internal pool for data with a pool size of 3 and an internal pool for metadata with a pool size of 3.
- Pooling is disabled by default for PowerExchange connections. Before you enable pooling, verify that the value of MASTASKS in the DBMOVER file is great enough to accommodate the maximum number of connections in the pool for the Listener task.

Connection Pooling Considerations for PowerExchange Netport Jobs

The following considerations apply to connection pooling for PowerExchange netport jobs:

- Depending on the data source, the netport JCL might reference a data set or other resource exclusively. Because a pooled netport connection can persist for some time after the data processing has finished, you might encounter concurrency issues. If you cannot change the netport JCL to reference resources nonexclusively, consider disabling connection pooling.
- Because the PSB is scheduled for a longer period of time when netport connections are pooled, resource constraints can occur in the following cases:
  - Another netport job on another port might want to to read a separate database in the same PSB, but the scheduling limit is reached.
  - The netport runs as a DL/1 job, and after the mapping finishes running, you attempt to restart the database within the IMS/DC environment. The attempt to restart the database will fail, because the database is still allocated to the netport DL/1 region.
  - Processing in a second mapping or a z/OS job flow relies on the database being available when the first mapping has finished running. If pooling is enabled, there is no guarantee that the database is available.

  For IMS netport jobs, because you can include at most ten NETPORT statements in a DBMOVER file, and because PowerExchange data maps cannot include PCB and PSB values that PowerExchange can use dynamically, you might need to build a PSB that includes multiple IMS databases that a PowerCenter workflow accesses. In this case, resource constraint issues are exacerbated as netport jobs are pooled that tie up multiple IMS databases for long periods of time.
- Depending on the data source, the netport JCL might include a user name and password that are used for authentication and authorization. Because job-level credentials cannot be changed after the job is submitted, PowerExchange connection pooling does not reuse netport connections unless the credentials match.

DBMOVER Statements for PowerExchange Connection Pooling

Include the following DBMOVER statements to configure PowerExchange connection pooling:

MAXTASKS

Defines the maximum number of tasks that can run concurrently in a PowerExchange Listener. Default is 30. Ensure that MAXTASKS is large enough to accommodate the maximum size of the connection pool.

Include the MAXTASKS statement in the DBMOVER configuration file on the PowerExchange Listener machine.

TCPIP_SHOW_POOLING

Writes diagnostic information to the PowerExchange log file. If you define TCPIP_SHOW_POOLING=Y in the DBMOVER file on the Data Integration Service machine, PowerExchange writes message PWX-33805 to the PowerExchange log file each time a connection is returned to the PowerExchange connection pool. The PowerExchange connection pool is the set of connection pools for each PowerExchange connection.

Message PWX-33805 provides the following information:

- Size. Total size of the PowerExchange connection pool.
- Hits. Number of times that PowerExchange found a connection in the PowerExchange connection pool that it could reuse.
- Partial hits. Number of times that PowerExchange found a connection in the PowerExchange connection pool that it could modify and reuse.
- Misses. Number of times that PowerExchange could not find a connection in the PowerExchange connection pool that it could reuse.
- Expired. Number of connections that were discarded from the PowerExchange connection pool because the maximum idle time was exceeded.
- Discarded pool full. Number of connections that were discarded from the PowerExchange connection pool because the pool was full.
- Discarded error. Number of connections that were discarded from the PowerExchange connection pool due to an error condition.

Include the TCPIP_SHOW_POOLING statement in the DBMOVER configuration file on the client machine.

Creating a Connection

In the Administrator tool, you can create relational database connections.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.
3. In the Navigator, select the domain.
4. In the Navigator, click **Actions** > **New** > **Connection**.

   The **New Connection** dialog box appears.
5. In the **New Connection** dialog box, select one of the following connection types:
   - DB2
   - DB2 for i5/OS

- DB2 for z/OS
- ODBC
- ORACLE
- SQLSERVER

6. Click **OK**.

   The **New Connection - Step 1 of 2** dialog box appears.
7. Configure the database connection properties and click **Next**.

   The connection name must be unique.

   The **New Connection - Step 2 of 2** dialog box appears.
8. Optionally, configure the connection pooling properties.
9. Optionally, click **Test Connection** to test the connection.
10. Click **Finish**.

Related Topics:

- "Relational Database Connection Properties" on page 330
- "DB2 for i5/OS Connection Properties" on page 332
- "DB2 for z/OS Connection Properties" on page 334
- "Nonrelational Database Connection Properties" on page 336
- "Pooling Properties" on page 338

Configuring Pooling for a Connection

Configure pooling for a connection in the Administrator tool.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.
3. In the Navigator, select a connection.

   The contents panel shows the connection properties.
4. In the contents panel, click the **Pooling** view.
5. In the **Pooling Properties** area, click **Edit**.

   The **Edit Pooling Properties** dialog box appears.
6. Edit the pooling properties and click **OK**.

Related Topics:

- “Pooling Properties” on page 338

Viewing a Connection

View connections in the Administrator tool.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.

   The Navigator shows all connections in the domain.
3. In the Navigator, select the domain.

   The contents panel shows all connections for the domain.
4. To filter the connections that appear in the contents panel, enter filter criteria and click the Filter button.

   The contents panel shows the connections that meet the filter criteria.
5. To remove the filter criteria, click the Reset Filters button.

   The contents panel shows all connections in the domain.
6. To sort the connections, click in the header for the column by which you want to sort the connections.

   By default, connections are sorted by name.
7. To add or remove columns from the contents panel, right-click a column header.

   If you have Read permission on the connection, you can view the data in the **Created By** column. Otherwise, this column is empty.
8. To view the connection details, select a connection in the Navigator.

   The contents panel shows the connection details.

Editing and Testing a Connection

In the Administrator tool, you can edit connections that you created in the Administrator tool, the Analyst tool, the Developer tool, or by running the infacmd isp CreateConnection command. You can test relational database connections except for ODBC connections.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.

   The Navigator shows all connections in the domain.
3. In the Navigator, select a connection.

   The contents panel shows properties for the connection.
4. In the contents panel, select the **Properties** view or the **Pooling** view.
5. To edit properties in a section, click **Edit**.

   Edit the properties and click **OK**.

6. To test a database connection, select the connection in the Navigator.

   Note: You cannot test ODBC connections.

   Click **Actions** > **Test Connection** on the **Domain** tab.

   A message box displays the result of the test.

Deleting a Connection

You can delete a database connection in the Administrator tool.

When you delete a connection in the Administrator tool, you also delete it from the Developer tool and the Analyst tool.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.

   The Navigator shows all connections in the domain.
3. In the Navigator, select a connection.
4. In the Navigator, click **Actions** > **Delete**.

Connection Properties

To configure connection properties, use the Administrator tool.

To view and edit connection properties, click the **Connections** tab. In the Navigator, select a connection. In the contents panel, click the **Properties** view. The contents panel shows the properties for the connection.

You can edit properties to change the connection. For example, you can change the user name and password for the connection, the metadata access and data access connection strings, and advanced properties.

You can edit properties for the following types of connections in the Administrator tool:

- Relational database connections. DB2, DB2 for i5/OS, DB2 for z/OS, ODBC, Oracle, and Microsoft SQL Server.
- Nonrelational database connections. Adabas, IMS, Sequential, and VSAM.
- Enterprise application connection. SAP.
- Web service connection.

Relational Database Connection Properties

The relational database connection properties differ based on the database type.

The following table describes the properties that appear in the **Properties** view for a DB2, Microsoft SQL Server, ODBC, or Oracle connection:

Property	Description
Database Type	The database type.
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with the @ character. It also cannot contain spaces or the following special characters: ` `~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	The description of the connection. The description cannot exceed 765 characters.
Use trusted connection	Microsoft SQL Server. Enables the application service to use Windows authentication to access the database. The user name that starts the application service must be a valid Windows user with access to the database. By default, this option is cleared.
User Name	The database user name.
Password	The password for the database user name.

Metadata Access Properties: Connection String	The JDBC connection URL used to access metadata from the database.
	- IBM DB2:
	`jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>`
	- Oracle:
	`jdbc:informatica:oracle://<host_name>:<port>;SID=<database name>`
	- Microsoft SQL Server:
	`jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name>`
	Not applicable for ODBC.

Data Access Properties: Connection String	The connection string used to access data from the database.
	- IBM DB2:
	`<database name>`
	- Microsoft SQL Server:
	`<server name>@<database name>`
	- ODBC:
	`<data source name>`
	- Oracle: `<database name>.world` from the TNSNAMES entry.

Code Page	The code page used to read from a source database or write to a target database or file.
Domain Name	Microsoft SQL Server on Windows. The name of the domain.
Packet Size	Microsoft SQL Server. The packet sized used to transmit data. Used to optimize the native drivers for Microsoft SQL Server.
Owner Name	Microsoft SQL Server. The name of the owner of the schema.
Schema Name	Microsoft SQL Server. The name of the schema in the database. You must specify the schema name for the Profiling Warehouse and staging database if the schema name is different than the database user name.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the connection environment SQL each time it connects to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the transaction environment SQL at the beginning of each transaction.

Property	Description
Retry Period	The number of seconds that the Data Integration Service tries to reconnect to the database if the connection fails. If the Data Integration Service cannot connect to the database in the retry period, the integration object fails. Default is 0.
Enable Parallel Mode	Oracle. Enables parallel processing when loading data into a table in bulk mode. By default, this option is cleared.
Tablespace	IBM DB2. The tablespace name of the database.
Support mixed case identifiers	Enables the Developer tool and Analyst tool to place quotes around table, view, schema, synonym and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. Also, use if the object names contain SQL keywords, such as WHERE. By default, this option is cleared.
SQL identifier character to use	The type of quote character used for the **Support mixed case identifiers** property. Select the quote character based on the database in the connection. The options are: - DOUBLE_QUOTE - SINGLE_QUOTE - BACK_QUOTE - SQUARE_BRACKETS - QUOTE_EMPTY
ODBC Provider	ODBC. The type of database to which ODBC connects. For pushdown optimization, specify the database type to enable the Data Integration Service to generate native database SQL. The options are: - Other - Sybase - Microsoft_SQL_Server Default is Other.

Related Topics:

- "DB2 for i5/OS Connection Properties" on page 332
- "DB2 for z/OS Connection Properties" on page 334

DB2 for i5/OS Connection Properties

To access tables in DB2 for i5/OS, use a DB2 for i5/OS connection.

The following table describes database connection properties that appear in the **Properties** view for a DB2 for i5/OS database connection:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	The description of the connection. The description cannot exceed 255 characters.
Connection Type	The connection type (DB2I).
User Name	The database user name.

Property	Description
Password	The password for the database user name.
Code Page	The code page used to read from a source database or write to a target database or file.
Database Name	The database instance name.
Location	The location of the PowerExchange Listener node that can connect to DB2. The location is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
Environment SQL	The SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Array Size	The number of records of the storage array size for each thread. Use if the number of worker threads is greater than 0. Default is 25.
Encryption Level	The level of encryption that the Data Integration Service uses. If you select RC2 or DES for Encryption Type, select one of the following values to indicate the encryption level: - 1. Uses a 56-bit encryption key for DES and RC2. - 2. Uses 168-bit triple encryption key for DES. Uses a 64-bit encryption key for RC2. - 3. Uses 168-bit triple encryption key for DES. Uses a 128-bit encryption key for RC2. Ignored if you do not select an encryption type. Default is 1.
Encryption Type	The type of encryption that the Data Integration Service uses. Select one of the following values: - None - RC2 - DES Default is None.
Interpret as Rows	Interprets the pacing size as rows or kilobytes. Select to represent the pacing size in number of rows. If you clear this option, the pacing size represents kilobytes. Default is Disabled.
Pacing Size	The amount of data that the source system can pass to the PowerExchange Listener. Configure the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. The lower the value, the faster the performance. Enter 0 for maximum performance. Default is 0.
Reject File	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the write mode is asynchronous with fault tolerance. To prevent the creation of the reject files, specify PWXDISABLE.
Write Mode	Mode in which the Data Integration Service sends data to the PowerExchange Listener. Configure one of the following write modes: - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select if error recovery is a priority. This option might decrease performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option when you can reload the target table if an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also provides the ability to detect errors. This provides the speed of Confirm Write Off with the data integrity of Confirm Write On. Default is CONFIRMWRITEON.

Property	Description
Compression	Enables compression of source data when reading from the database.
Database File Overrides	Specifies the i5/OS database file override. The format is: `from_file/to_library/to_file/to_member` Where: - *from_file* is the file to be overridden - *to_library* is the new library to use - *to_file* is the file in the new library to use - *to_member* is optional and is the member in the new library and file to use. *FIRST is used if nothing is specified. You can specify up to eight unique file overrides on a connection. A single override applies to a single source or target. When you specify more than one file override, enclose the string of file overrides in double quotes and include a space between each file override. **Note:** If you specify both Library List and Database File Overrides and a table exists in both, Database File Overrides takes precedence.
Isolation Level	Commit scope of the transaction. Select one of the following values: - None - CS. Cursor stability. - RR. Repeatable read. - CHG. Change. - ALL Default is CS.
Library List	List of libraries that PowerExchange searches to qualify the table name for Select, Insert, Delete, or Update statements. PowerExchange searches the list if the table name is unqualified. Separate libraries with semicolons. **Note:** If you specify both Library List and Database File Overrides and a table exists in both, Database File Overrides takes precedence.

DB2 for z/OS Connection Properties

Use a DB2 for z/OS connection to access tables in DB2 for z/OS.

The following table describes database connection properties that appear in the **Properties** view of the DB2 for z/OS database connection:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with the @ character. It also cannot contain spaces or the following special characters: `` ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( ) ] [ ``
Description	Description of the connection. The description cannot exceed 255 characters.
Connection Type	Connection type (DB2Z).
User Name	Database user name.
Password	Password for the database user name.
Code Page	Code page used to read from a source database or write to a target database or file.

Property	Description
DB2 Subsystem ID	Name of the DB2 subsystem.
Location	Location of the PowerExchange Listener node that can connect to DB2. The location is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Array Size	Number of records of the storage array size for each thread. Use if the number of worker threads is greater than 0. Default is 25.
Correlation ID	Value to be concatenated to prefix PWX to form the DB2 correlation ID for DB2 requests.
Encryption Level	Level of encryption that the Data Integration Service uses. If you select RC2 or DES for Encryption Type, select one of the following values to indicate the encryption level: - 1. Uses a 56-bit encryption key for DES and RC2. - 2. Uses 168-bit triple encryption key for DES. Uses a 64-bit encryption key for RC2. - 3. Uses 168-bit triple encryption key for DES. Uses a 128-bit encryption key for RC2. Ignored if you do not select an encryption type. Default is 1.
Encryption Type	Type of encryption that the Data Integration Service uses. Select one of the following values: - None - RC2 - DES Default is None.
Interpret as Rows	Interprets the pacing size as rows or kilobytes. Select to represent the pacing size in number of rows. If you clear this option, the pacing size represents kilobytes. Default is Disabled.
Offload Processing	Moves data processing for bulk data from the source system to the Data Integration Service machine. Default is No.
Pacing Size	Amount of data that the source system can pass to the PowerExchange Listener. Configure the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. The lower the value, the faster the performance. Enter 0 for maximum performance. Default is 0.
Reject File	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the write mode is asynchronous with fault tolerance. To prevent the creation of the reject files, specify PWXDISABLE.
Worker Threads	Number of threads that the Data Integration Services uses to process data. For optimal performance, do not exceed the number of installed or available processors on the Data Integration Service machine. Default is 0.

Property	Description
Write Mode	Mode in which the Data Integration Service sends data to the PowerExchange Listener. Configure one of the following write modes: - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select if error recovery is a priority. This option might decrease performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option when you can reload the target table if an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also provides the ability to detect errors. This provides the speed of Confirm Write Off with the data integrity of Confirm Write On. Default is CONFIRMWRITEON.
Compression	Compresses source data when reading from the database.

Nonrelational Database Connection Properties

Use an Adabas, IMS, sequential, or VSAM connection to access the corresponding nonrelational database or data set.

The following table describes the properties that appear in the **Properties** view of the connection:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with the @ character. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the connection. The description cannot exceed 255 characters.
Connection Type	Connection type, which is one of the following values: - ADABAS - IMS - SEQ - VSAM
Location	Location of the PowerExchange Listener node that can connect to IMS. The location is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
User Name	Database user name.
Password	Password for the database user name.
Code Page	Code page used to read from a source database or write to a target database or file.
Array Size	Number of records of the storage array size for each thread. Use if the number of worker threads is greater than 0. Default is 25.

Property	Description
Encryption Level	Level of encryption that the Data Integration Service uses. If you select RC2 or DES for Encryption Type, select one of the following values to indicate the encryption level: - 1. Uses a 56-bit encryption key for DES and RC2. - 2. Uses 168-bit triple encryption key for DES. Uses a 64-bit encryption key for RC2. - 3. Uses 168-bit triple encryption key for DES. Uses a 128-bit encryption key for RC2. Ignored if you do not select an encryption type. Default is 1.
Encryption Type	Type of encryption that the Data Integration Service uses. Select one of the following values: - None - RC2 - DES Default is None.
Write Mode	Mode in which the Data Integration Service sends data to the PowerExchange Listener. Configure one of the following write modes: - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select if error recovery is a priority. This option might decrease performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option when you can reload the target table if an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also provides the ability to detect errors. This provides the speed of Confirm Write Off with the data integrity of Confirm Write On. Default is CONFIRMWRITEON.
Offload Processing	Moves data processing for bulk data from the source system to the Data Integration Service machine. Default is No.
Interpret as Rows	Interprets the pacing size as rows or kilobytes. Select to represent the pacing size in number of rows. If you clear this option, the pacing size represents kilobytes. Default is Disabled.
Worker Threads	Number of threads that the Data Integration Services uses on the Data Integration Service machine to process data. For optimal performance, do not exceed the number of installed or available processors on the Data Integration Service machine. Default is 0.
Compression	Compresses source data when reading from the data source.
Pacing Size	Amount of data that the source system can pass to the PowerExchange Listener. Configure the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. The lower the value, the greater the performance. Enter 0 for maximum performance. Default is 0.

Rules and Guidelines to Update Connection Properties

When you edit a database connection, some updates take effect immediately. Some updates require you to restart the Data Integration Service.

Use the following rules and guidelines when you update connection properties:

- If you change the user name, password, or the connection string, the updated connection takes effect immediately. Subsequent connection requests use the updated information. If connection pooling is enabled, the connection pool library drops all idle connections and restarts the connection pool. It does not return active connection instances to the connection pool when complete.
- If you change any other property, you must restart the Data Integration Service to apply the updates.

Pooling Properties

To manage the pool of idle connection instances, configure connection pooling properties.

The following table describes database connection pooling properties that you can edit in the **Pooling** view for a database connection:

Property	Description
Enable Connection Pooling	Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instance in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. To delete the pool of idle connections, you must restart the Data Integration Service. Default is enabled for Microsoft SQL Server, IBM DB2, Oracle, and ODBC connections. Default is disabled for DB2 for i5/OS, DB2 for z/OS, IMS, Sequential, and VSAM connections.
Minimum # of Connections	The minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.
Maximum # of Connections	The maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
Maximum Idle Time	The number of seconds that a connection that exceeds the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idle time when it does not exceed the minimum number of idle connection instances. Default is 120.

CHAPTER 26

Domain Object Export and Import

This chapter includes the following topics:

- Domain Object Export and Import Overview, 339
- Export Process, 340
- View Domain Objects, 340
- Import Process, 347

Domain Object Export and Import Overview

You can use the command line to migrate objects between two different domains of the same version.

You might migrate domain objects from a development environment to a test or production environment.

To export and import domain objects, use the following infacmd isp commands:

ExportDomainObjects

Exports native users, native groups, roles, and connections to an XML file.

ImportDomainObjects

Imports native users, native groups, roles, and connections into an Informatica domain.

You can use an infacmd control file to filter the objects during the export or import.

You can also use the command line to generate a readable XML file from an export file. You can edit the readable XML file and update the changes to the export XML file.

Use the following infacmd xrf commands:

generateReadableViewXML

Generates a readable XML file from an export XML file.

updateExportXML

Creates a new export XML file with the changes that you made to the readable XML file.

Export Process

You can use the command line to export domain objects from a domain.

Perform the following tasks to export domain objects:

1. Determine the domain objects that you want to export.
2. If you do not want to export all domain objects, create an export control file to filter the objects that are exported.
3. Run the infacmd isp exportDomainObjects command to export the domain objects.

The command exports the domain objects to an export file. You can use this file to import the objects into another domain.

Rules and Guidelines for Exporting Domain Objects

Review the following rules and guidelines before you export domain objects.

- When you export a user, by default, you do not export the user password. If you do not export the password, the administrator must reset the password for the user after the user is imported into the domain. However, when you run the infacmd isp exportDomainObjects command, you can choose to export an encrypted version of the password.
- When you export a user, you do not export the associated groups of the user. If applicable, assign the user to the group after you import the user and group.
- When you export a group, you export all sub-groups and users in the group.
- You cannot export the Administrator user, the Administrator role, the Everyone group, or LDAP users or groups. To replicate LDAP users and groups in an Informatica domain, import the LDAP users and groups directly from the LDAP directory service.
- To export native users and groups from domains of different versions, use the infacmd isp exportUsersAndGroups command.
- When you export a connection, by default, you do not export the connection password. If you do not export the password, the administrator must reset the password for the connection after the connection is imported into the domain. However, when you run the infacmd isp exportDomainObjects command, you can choose to export an encrypted version of the password.

View Domain Objects

You can view domain object names and properties in the export XML file.

Run infacmd xrf generateReadableViewXML command, to create a readable XML from the export file.

The following section provides a sample readable XML file.

```
<global:View xmlns:global="http://global" xmlns:connection="http://connection"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
  http://connection connection.xsd http://global globalSchemaDomain.xsd http://global
  globalSchema.xsd">
  <NativeUser isAdmin="false" name="admin" securityDomain="Native" viewId="0">
    <UserInfo email="" fullName="admin" phone="" viewId="1"/>
  </NativeUser>
  <User isAdmin="false" name="User1" securityDomain="Native" viewId="15">
    <UserInfo email="" fullName="NewUSer" phone="" viewId="16"/>
  </User>
  <Group name="TestGroup1" securityDomain="Native" viewId="182">
```

```
    <UserRef name="User1" securityDomain="Native" viewId="183"/>
    <UserRef name="User6" securityDomain="Native" viewId="188"/>
  </Group>
  <Role customRole="false" name="Administrator" viewId="242">
    <Description viewId="243">Provides all privilege and permission access to an Informatica service.</
Description>
    <ServicePrivilegeDefinition name="PwxListenerService" viewId="244">
      <Privilege category="" isEnabled="true" name="close" viewId="245"/>
      <Privilege category="" isEnabled="true" name="closeforce" viewId="246"/>
      <Privilege category="" isEnabled="false" name="Management Commands" viewId="249"/>
      <Privilege category="" isEnabled="false" name="Informational Commands" viewId="250"/>
    </ServicePrivilegeDefinition>
  </Role>
  <Connection connectionString="inqa85sql25@qa90" connectionType="SQLServerNativeConnection"
    domainName="" environmentSQL="" name="conn4" ownerName=""
    schemaName="" transactionSQL="" userName="dummy" viewId="7512">
    <ConnectionPool maxIdleTime="120" minConnections="0" usePool="true" viewId="7514"/>
  </Connection>
 </global:View>
```

Viewable Domain Object Names

You can view the following domain object names and properties in the readable XML file.

User

Property	Type
name	string
securityDomain	string
disable	boolean
admin	boolean
UserInfo	List<UserInfo>

UserInfo

Property	Type
description	string
email	string
fullName	string
phone	string

Role

Property	Type
name	string
description	string

customRole	boolean
servicePrivilege	List<ServicePrivilegeDef>

ServicePrivilegeDef

Property	Type
name	string
privileges	List<Privilege>

Privilege

Property	Type
name	string
enable	boolean
category	string

Group

Property	Type
name	string
securityDomain	string
description	string
UserRefs	List<UserRef>

GroupRef

Property	Type
name	string
securityDomain	string

UserRef

- name
- securityDomain

ConnectInfo

Property	Type
name	string
connectionType	string
ConnectionPoolAttributes	List<ConnectionPoolAttributes>

ConnectionPoolAttributes

Property	Type
maxIdleTime	int
minConnections	int
poolSize	int
usePool	boolean

Supported Connection Types

- DB2iNativeConnection
- DB2NativeConnection
- DB2zNativeConnection
- JDBCConnection
- ODBCNativeConnection
- OracleNativeConnection
- PWXMetaConnection
- SAPConnection
- SDKConnection
- SQLServerNativeConnection
- SybaseNativeConnection
- TeradataNativeConnection
- URLLocation
- WebServiceConnection
- NRDBMetaConnection
- NRDBNativeConnection
- RelationalBaseSDKConnection

DB2iNativeConnection Properties

- connectionType
- connectionString

- username
- environmentSQL
- libraryList
- location
- databaseFileOverrides

DB2NativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- tableSpace
- transactionSQL

DB2zNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- location

JDBCConnection Properties

- connectionType
- connectionString
- username
- dataStoreType

ODBCNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL
- odbcProvider

OracleNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL

PWXMetaConnection Properties

- connectionType

- databaseName
- userName
- dataStoreType
- dbType
- hostName
- location
- port

SAPConnection Properties

- connectionType
- userName
- description
- dataStoreType

SDKConnection Properties

- connectionType
- sdkConnectionType
- dataSourceType

SQLServerNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL
- domainName
- ownerName
- schemaName

TeradataNativeConnection Properties

- connectionType
- username
- environmentSQL
- transactionSQL
- dataSourceName
- databaseName

TeradataNativeConnection Properties

- connectionType
- username
- environmentSQL
- transactionSQL
- connectionString

URLLocation Properties

- connectionType
- locatorURL

WebServiceConnection Properties

- connectionType
- url
- userName
- wsseType
- httpAuthenticationType

NRDBNativeConnection Properties

- connectionType
- userName
- location

NRDBMetaConnection Properties

- connectionType
- username
- location
- dataStoreType
- hostName
- port
- databaseType
- databaseName
- extensions

RelationalBaseSDKConnection Properties

- connectionType
- databaseName
- connectionString
- domainName
- environmentSQL
- hostName
- owner
- ispSvcName
- metadataDataStorageType
- metadataConnectionString
- metadataConnectionUserName

Import Process

You can use the command line to import domain objects from an export file into a domain.

Perform the following tasks to import domain objects:

1. Review the domain objects in the export file and determine the objects that you want to import.
2. If you do not want to import all domain objects in the export file, create an import control file to filter the objects that are imported.
3. Run the infacmd isp importDomainObjects command to import the domain objects into the specified domain.
4. After you import the objects, you may still have to create other domain objects such as application services and folders.

Rules and Guidelines for Importing Domain Objects

Review the following rules and guidelines before you import domain objects.

- When you import a group, you import all sub-groups and users in the group.
- To import native users and groups from domains of different versions, use the infacmd isp importUsersAndGroups command.
- After you import a user or group, you cannot rename the user or group.
- You import roles independently of users and groups. Assign roles to users and groups after you import the roles, users, and groups.

Conflict Resolution

A conflict occurs when you try to import an object with a name that exists for an object in the target domain. Configure the conflict resolution to determine how to handle conflicts during the import.

You can define a conflict resolution strategy through the command line or control file when you import the objects. The control file takes precedence if you define conflict resolution in the command line and control file. The import fails if there is a conflict and you did not define a conflict resolution strategy.

You can configure one of the following conflict resolution strategies:

Reuse

Reuses the object in the target domain.

Rename

Renames the source object. You can provide a name in the control file, or else the name is generated. A generated name has a number appended to the end of the name.

Replace

Replaces the target object with the source object.

Merge

Merges the source and target objects into one group. This option is applicable for groups. For example, if you merge groups with the same name, users and sub-groups from both groups are merged into the group in the target domain.

CHAPTER 27

Managing the Grid

This chapter includes the following topics:

- Managing the Grid Overview, 348
- Configuring the Grid, 348
- Configuring the PowerCenter Integration Service, 349
- Configuring Resources, 350
- Troubleshooting the Grid, 352

Managing the Grid Overview

A grid is an alias assigned to a group of nodes that run sessions and workflows. When you run a workflow on a grid, you improve scalability and performance by distributing Session and Command tasks to service processes running on nodes in the grid. When you run a session on a grid, you improve scalability and performance by distributing session threads to multiple DTM processes running on nodes in the grid.

To run a workflow or session on a grid, you assign resources to nodes, create and configure the grid, and configure the PowerCenter Integration Service to run on a grid.

To manage a grid, complete the following tasks:

1. Create a grid and assign nodes to the grid.
2. Configure the PowerCenter Integration Service to run on a grid. You configure the PowerCenter Integration Service to run on a grid, and you configure the service processes for the nodes in the grid.
3. Assign resources to nodes. You assign resources to a node to allow the PowerCenter Integration Service to match the resources required to run a task or session thread with the resources available on a node.

After you configure the grid and PowerCenter Integration Service, you configure a workflow to run on the PowerCenter Integration Service assigned to a grid.

Configuring the Grid

To configure a grid, create the grid and assign nodes to the grid. You can assign a node to more than one grid.

1. In the Administrator tool, select Create > Grid.

   The Create Grid window appears.

2. Edit the following properties:

Property	Description
Name	Name of the grid. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the grid. The description cannot exceed 765 characters.
Nodes	Select nodes to assign to the grid.
Path	Location in the Navigator.

Configuring the PowerCenter Integration Service

To configure the PowerCenter Integration Service, you assign the grid to the PowerCenter Integration Service and configure the service process for each node in the grid. If the PowerCenter Integration Service uses operating system profiles, all nodes on the grid must run on UNIX.

Configuring the PowerCenter Integration Service to Run on a Grid

You configure the PowerCenter Integration Service by assigning the grid to the PowerCenter Integration Service.

To assign the grid to a PowerCenter Integration Service:

1. In the Administrator tool, select the PowerCenter Integration Service Properties tab.
2. Edit the grid and node assignments, and select Grid.
3. Select the grid you want to assign to the PowerCenter Integration Service.

Configuring the Service Processes

When you run a session or a workflow on a grid, a service process runs on each node in the grid. Each service process running on a node must be compatible or configured the same. It must also have access to the directories and input files used by the PowerCenter Integration Service.

To ensure consistent results, complete the following tasks:

- Verify the shared storage location. Verify that the shared storage location is accessible to each node in the grid. If the PowerCenter Integration Service uses operating system profiles, the operating system user must have access to the shared storage location.
- Configure the service process. Configure $PMRootDir to the shared location on each node in the grid. Configure service process variables with identical absolute paths to the shared directories on each node in the grid. If the PowerCenter Integration Service uses operating system profiles, the service process variables you define in the operating system profile override the service process variable setting for every node. The operating system user must have access to the $PMRootDir configured in the operating system profile on every node in the grid.

Complete the following process to configure the service processes:

1. Select the PowerCenter Integration Service in the Navigator.
2. Click the Processes tab.

   The tab displays the service process for each node assigned to the grid.
3. Configure $PMRootDir to point to the shared location.
4. Configure the following service process settings for each node in the grid:
   - Code pages. For accurate data movement and transformation, verify that the code pages are compatible for each service process. Use the same code page for each node where possible.
   - Service process variables. Configure the service process variables the same for each service process. For example, the setting for $PMCacheDir must be identical on each node in the grid.
   - Directories for Java components. Point to the same Java directory to ensure that java components are available to objects that access Java, such as Custom transformations that use Java coding.

Configuring Resources

Informatica resources are the database connections, files, directories, node names, and operating system types required by a task. You can configure the PowerCenter Integration Service to check resources. When you do this, the Load Balancer matches the resources available to nodes in the grid with the resources required by the workflow. It dispatches tasks in the workflow to nodes where the required resources are available. If the PowerCenter Integration Service is not configured to run on a grid, the Load Balancer ignores resource requirements.

For example, if a session uses a parameter file, it must run on a node that has access to the file. You create a resource for the parameter file and make it available to one or more nodes. When you configure the session, you assign the parameter file resource as a required resource. The Load Balancer dispatches the Session task to a node that has the parameter file resource. If no node has the parameter file resource available, the session fails.

Resources for a node can be predefined or user-defined. Informatica creates predefined resources during installation. Predefined resources include the connections available on a node, node name, and operating system type. When you create a node, all connection resources are available by default. Disable the connection resources that are not available on the node. For example, if the node does not have Oracle client libraries, disable the Oracle Application connections. If the Load Balancer dispatches a task to a node where the required resources are not available, the task fails. You cannot disable or remove node name or operating system type resources.

User-defined resources include file/directory and custom resources. Use file/directory resources for parameter files or file server directories. Use custom resources for any other resources available to the node, such as database client version.

The following table lists the types of resources you use in Informatica:

Type	Predefined/ User-Defined	Description
Connection	Predefined	Any resource installed with PowerCenter, such as a plug-in or a connection object. A connection object may be a relational, application, FTP, external loader, or queue connection. When you create a node, all connection resources are available by default. Disable the connection resources that are not available to the node.

Type	Predefined/ User-Defined	Description
		Any Session task that reads from or writes to a relational database requires one or more connection resources. The Workflow Manager assigns connection resources to the session by default.
Node Name	Predefined	A resource for the name of the node. A Session, Command, or predefined Event-Wait task requires a node name resource if it must run on a specific node.
Operating System Type	Predefined	A resource for the type of operating system on the node. A Session or Command task requires an operating system type resource if it must run a specific operating system.
Custom	User-defined	Any resource for all other resources available to the node, such as a specific database client version. For example, a Session task requires a custom resource if it accesses a Custom transformation shared library or if it requires a specific database client version.
File/Directory	User-defined	Any resource for files or directories, such as a parameter file or a file server directory. For example, a Session task requires a file resource if it accesses a session parameter file.

You configure resources required by Session, Command, and predefined Event-Wait tasks in the task properties.

You define resources available to a node on the Resources tab of the node in the Administrator tool.

Note: When you define a resource for a node, you must verify that the resource is available to the node. If the resource is not available and the PowerCenter Integration Service runs a task that requires the resource, the task fails.

Viewing Resources in a Domain

You can view the resources available to all nodes in a domain on the Resources view of the domain. The Administrator tool displays a column for each node. It displays a checkmark when a resource is available for a node.

Assigning Connection Resources

You can assign the connection resources available to a node in the Administrator tool.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. In the contents panel, click the **Resources** view.
4. Click on a resource that you want to edit.
5. On the Domain tab **Actions** menu, click **Enable Selected Resource** or **Disable Selected Resource**.

Defining Custom and File/Directory Resources

You can define custom and file/directory resources available to a node in the Administrator tool. When you define a custom or file/directory resource, you assign a resource name. The resource name is a logical name that you create to identify the resource.

You assign the resource to a PowerCenter task or PowerCenter mapping object instance using this name. To coordinate resource usage, you may want to use a naming convention for file/directory and custom resources.

To define a custom or file/directory resource:

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select a node.
3. In the contents panel, click the **Resources** view.
4. On the Domain tab **Actions** menu, click **New Resource**.
5. Enter a name for the resource.

   The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : / ? . , < > | ! ( )] [
6. Select a resource type.
7. Click OK.

   To remove a custom or file/directory resource, select a resource and click **Delete Selected Resource** on the Domain tab **Actions** menu.

Resource Naming Conventions

Using resources with PowerCenter requires coordination and communication between the domain administrator and the workflow developer. The domain administrator defines resources available to nodes. The workflow developer assigns resources required by Session, Command, and predefined Event-Wait tasks. To coordinate resource usage, you can use a naming convention for file/directory and custom resources.

Use the following naming convention:

```
resourcetype_description
```

For example, multiple nodes in a grid contain a session parameter file called sales1.txt. Create a file resource for it named sessionparamfile_sales1 on each node that contains the file. A workflow developer creates a session that uses the parameter file and assigns the sessionparamfile_sales1 file resource to the session.

When the PowerCenter Integration Service runs the workflow on the grid, the Load Balancer distributes the session assigned the sessionparamfile_sales1 resource to nodes that have the resource defined.

Troubleshooting the Grid

I changed the nodes assigned to the grid, but the PowerCenter Integration Service to which the grid is assigned does not show the latest PowerCenter Integration Service processes.

When you change the nodes in a grid, the Service Manager performs the following transactions in the domain configuration database:

1. Updates the grid based on the node changes. For example, if you added a node, the node appears in the grid.
2. Updates the PowerCenter Integration Services to which the grid is assigned. All nodes in the grid appear as service processes for the PowerCenter Integration Service.

If the Service Manager cannot update a PowerCenter Integration Service and the latest service processes do not appear for the PowerCenter Integration Service, reassign the grid to the PowerCenter Integration Service.

CHAPTER 28

Load Balancer

This chapter includes the following topics:

- Load Balancer Overview, 353
- Configuring the Dispatch Mode, 354
- Service Levels, 355
- Configuring Resources, 356
- Calculating the CPU Profile, 357
- Defining Resource Provision Thresholds, 357

Load Balancer Overview

The Load Balancer is a component of the PowerCenter Integration Service that dispatches tasks to PowerCenter Integration Service processes running on nodes in a grid. It matches task requirements with resource availability to identify the best PowerCenter Integration Service process to run a task. It can dispatch tasks on a single node or across nodes.

You can configure Load Balancer settings for the domain and for nodes in the domain. The settings you configure for the domain apply to all PowerCenter Integration Services in the domain.

You configure the following settings for the domain to determine how the Load Balancer dispatches tasks:

- Dispatch mode. The dispatch mode determines how the Load Balancer dispatches tasks. You can configure the Load Balancer to dispatch tasks in a simple round-robin fashion, in a round-robin fashion using node load metrics, or to the node with the most available computing resources.
- Service level. Service levels establish dispatch priority among tasks that are waiting to be dispatched. You can create different service levels that a workflow developer can assign to workflows.

You configure the following Load Balancer settings for each node:

- Resources. When the PowerCenter Integration Service runs on a grid, the Load Balancer can compare the resources required by a task with the resources available on each node. The Load Balancer dispatches tasks to nodes that have the required resources. You assign required resources in the task properties. You configure available resources using the Administrator tool or *infacmd*.
- CPU profile. In adaptive dispatch mode, the Load Balancer uses the CPU profile to rank the computing throughput of each CPU and bus architecture in a grid. It uses this value to ensure that more powerful nodes get precedence for dispatch.
- Resource provision thresholds. The Load Balancer checks one or more resource provision thresholds to determine if it can dispatch a task. The Load Balancer checks different thresholds depending on the dispatch mode.

Configuring the Dispatch Mode

The Load Balancer uses the dispatch mode to select a node to run a task. You configure the dispatch mode for the domain. Therefore, all PowerCenter Integration Services in a domain use the same dispatch mode.

When you change the dispatch mode for a domain, you must restart each PowerCenter Integration Service in the domain. The previous dispatch mode remains in effect until you restart the PowerCenter Integration Service.

You configure the dispatch mode in the domain properties.

The Load Balancer uses the following dispatch modes:

- Round-robin. The Load Balancer dispatches tasks to available nodes in a round-robin fashion. It checks the Maximum Processes threshold on each available node and excludes a node if dispatching a task causes the threshold to be exceeded. This mode is the least compute-intensive and is useful when the load on the grid is even and the tasks to dispatch have similar computing requirements.
- Metric-based. The Load Balancer evaluates nodes in a round-robin fashion. It checks all resource provision thresholds on each available node and excludes a node if dispatching a task causes the thresholds to be exceeded. The Load Balancer continues to evaluate nodes until it finds a node that can accept the task. This mode prevents overloading nodes when tasks have uneven computing requirements.
- Adaptive. The Load Balancer ranks nodes according to current CPU availability. It checks all resource provision thresholds on each available node and excludes a node if dispatching a task causes the thresholds to be exceeded. This mode prevents overloading nodes and ensures the best performance on a grid that is not heavily loaded.

The following table compares the differences among dispatch modes:

Dispatch Mode	Checks resource provision thresholds?	Uses task statistics?	Uses CPU profile?	Allows bypass in dispatch queue?
Round-Robin	Checks maximum processes.	No	No	No
Metric-Based	Checks all thresholds.	Yes	No	No
Adaptive	Checks all thresholds.	Yes	Yes	Yes

Round-Robin Dispatch Mode

In round-robin dispatch mode, the Load Balancer dispatches tasks to nodes in a round-robin fashion. The Load Balancer checks the Maximum Processes resource provision threshold on the first available node. It dispatches the task to this node if dispatching the task does not cause this threshold to be exceeded. If dispatching the task causes this threshold to be exceeded, the Load Balancer evaluates the next node. It continues to evaluate nodes until it finds a node that can accept the task.

The Load Balancer dispatches tasks for execution in the order the Workflow Manager or scheduler submits them. The Load Balancer does not bypass any task in the dispatch queue. Therefore, if a resource-intensive task is first in the dispatch queue, all other tasks with the same service level must wait in the queue until the Load Balancer dispatches the resource-intensive task.

Metric-Based Dispatch Mode

In metric-based dispatch mode, the Load Balancer evaluates nodes in a round-robin fashion until it finds a node that can accept the task. The Load Balancer checks the resource provision thresholds on the first available node. It dispatches the task to this node if dispatching the task causes none of the thresholds to be exceeded. If

dispatching the task causes any threshold to be exceeded, or if the node is out of free swap space, the Load Balancer evaluates the next node. It continues to evaluate nodes until it finds a node that can accept the task.

To determine whether a task can run on a particular node, the Load Balancer collects and stores statistics from the last three runs of the task. It compares these statistics with the resource provision thresholds defined for the node. If no statistics exist in the repository, the Load Balancer uses the following default values:

- 40 MB memory
- 15% CPU

The Load Balancer dispatches tasks for execution in the order the Workflow Manager or scheduler submits them. The Load Balancer does not bypass any tasks in the dispatch queue. Therefore, if a resource intensive task is first in the dispatch queue, all other tasks with the same service level must wait in the queue until the Load Balancer dispatches the resource intensive task.

Adaptive Dispatch Mode

In adaptive dispatch mode, the Load Balancer evaluates the computing resources on all available nodes. It identifies the node with the most available CPU and checks the resource provision thresholds on the node. It dispatches the task if doing so does not cause any threshold to be exceeded. The Load Balancer does not dispatch a task to a node that is out of free swap space.

In adaptive dispatch mode, the Load Balancer can use the CPU profile to rank nodes according to the amount of computing resources on the node.

To identify the best node to run a task, the Load Balancer also collects and stores statistics from the last three runs of the task and compares them with node load metrics. If no statistics exist in the repository, the Load Balancer uses the following default values:

- 40 MB memory
- 15% CPU

In adaptive dispatch mode, the order in which the Load Balancer dispatches tasks from the dispatch queue depends on the task requirements and dispatch priority. For example, if multiple tasks with the same service level are waiting in the dispatch queue and adequate computing resources are not available to run a resource intensive task, the Load Balancer reserves a node for the resource intensive task and keeps dispatching less intensive tasks to other nodes.

Service Levels

Service levels establish priorities among tasks that are waiting to be dispatched.

When the Load Balancer has more tasks to dispatch than the PowerCenter Integration Service can run at the time, the Load Balancer places those tasks in the dispatch queue. When multiple tasks are waiting in the dispatch queue, the Load Balancer uses service levels to determine the order in which to dispatch tasks from the queue.

Service levels are domain properties. Therefore, you can use the same service levels for all repositories in a domain. You create and edit service levels in the domain properties or using *infacmd*.

When you create a service level, a workflow developer can assign it to a workflow in the Workflow Manager. All tasks in a workflow have the same service level. The Load Balancer uses service levels to dispatch tasks from the dispatch queue. For example, you create two service levels:

- Service level “Low” has dispatch priority 10 and maximum dispatch wait time 7,200 seconds.
- Service level “High” has dispatch priority 2 and maximum dispatch wait time 1,800 seconds.

When multiple tasks are in the dispatch queue, the Load Balancer dispatches tasks with service level High before tasks with service level Low because service level High has a higher dispatch priority. If a task with service level Low waits in the dispatch queue for two hours, the Load Balancer changes its dispatch priority to the maximum priority so that the task does not remain in the dispatch queue indefinitely.

The Administrator tool provides a default service level named Default with a dispatch priority of 5 and maximum dispatch wait time of 1800 seconds. You can update the default service level, but you cannot delete it.

When you remove a service level, the Workflow Manager does not update tasks that use the service level. If a workflow service level does not exist in the domain, the Load Balancer dispatches the tasks with the default service level.

Related Topics:

- "Service Level Management" on page 46

Creating Service Levels

Create service levels in the Administrator tool.

1. In the Administrator tool, select a domain in the Navigator.
2. Click the **Properties** tab.
3. In the Service Level Management area, click Add.
4. Enter values for the service level properties.
5. Click **OK**.
6. To remove a service level, click the Remove button for the service level you want to remove.

Related Topics:

- "Service Level Management" on page 46

Configuring Resources

When you configure the PowerCenter Integration Service to run on a grid and to check resource requirements, the Load Balancer dispatches tasks to nodes based on the resources available on each node. You configure the PowerCenter Integration Service to check available resources in the PowerCenter Integration Service properties in Informatica Administrator.

You assign resources required by a task in the task properties in the PowerCenter Workflow Manager.

You define the resources available to each node in the Administrator tool. Define the following types of resources:

- Connection. Any resource installed with PowerCenter, such as a plug-in or a connection object. When you create a node, all connection resources are available by default. Disable the connection resources that are not available to the node.
- File/Directory. A user-defined resource that defines files or directories available to the node, such as parameter files or file server directories.
- Custom. A user-defined resource that identifies any other resources available to the node. For example, you may use a custom resource to identify a specific database client version.

Enable and disable available resources on the Resources tab for the node in the Administrator tool or using *infacmd*.

Calculating the CPU Profile

In adaptive dispatch mode, the Load Balancer uses the CPU profile to rank the computing throughput of each CPU and bus architecture in a grid. This ensures that nodes with higher processing power get precedence for dispatch. This value is not used in round-robin or metric-based dispatch modes.

The CPU profile is an index of the processing power of a node compared to a baseline system. The baseline system is a Pentium 2.4 GHz computer running Windows 2000. For example, if a SPARC 480 MHz computer is 0.28 times as fast as the baseline computer, the CPU profile for the SPARC computer should be set to 0.28.

By default, the CPU profile is set to 1.0. To calculate the CPU profile for a node, select the node in the Navigator and click **Actions** > **Recalculate CPU Profile Benchmark**. To get the most accurate value, calculate the CPU profile when the node is idle. The calculation takes approximately five minutes and uses 100% of one CPU on the machine.

You can also calculate the CPU profile using *infacmd*. Or, you can edit the node properties and update the value manually.

Defining Resource Provision Thresholds

The Load Balancer dispatches tasks to PowerCenter Integration Service processes running on a node. It can continue to dispatch tasks to a node as long as the resource provision thresholds defined for the node are not exceeded. When the Load Balancer has more Session and Command tasks to dispatch than the PowerCenter Integration Service can run at a time, the Load Balancer places the tasks in the dispatch queue. It dispatches tasks from the queue when a PowerCenter Integration Service process becomes available.

You can define the following resource provision thresholds for each node in a domain:

- Maximum CPU run queue length. The maximum number of runnable threads waiting for CPU resources on the node. The Load Balancer does not count threads that are waiting on disk or network I/Os. If you set this threshold to 2 on a 4-CPU node that has four threads running and two runnable threads waiting, the Load Balancer does not dispatch new tasks to this node.

  This threshold limits context switching overhead. You can set this threshold to a low value to preserve computing resources for other applications. If you want the Load Balancer to ignore this threshold, set it to a high number such as 200. The default value is 10.

  The Load Balancer uses this threshold in metric-based and adaptive dispatch modes.

- Maximum memory %. The maximum percentage of virtual memory allocated on the node relative to the total physical memory size. If you set this threshold to 120% on a node, and virtual memory usage on the node is above 120%, the Load Balancer does not dispatch new tasks to the node.

  The default value for this threshold is 150%. Set this threshold to a value greater than 100% to allow the allocation of virtual memory to exceed the physical memory size when dispatching tasks. If you want the Load Balancer to ignore this threshold, set it to a high number such as 1,000.

  The Load Balancer uses this threshold in metric-based and adaptive dispatch modes.

- Maximum processes. The maximum number of running processes allowed for each PowerCenter Integration Service process that runs on the node. This threshold specifies the maximum number of running Session *or* Command tasks allowed for each PowerCenter Integration Service process that runs on the node. For example, if you set this threshold to 10 when two PowerCenter Integration Services are running on the node, the maximum number of Session tasks allowed for the node is 20 and the maximum number of Command tasks allowed for the node is 20. Therefore, the maximum number of processes that can run simultaneously is 40.

  The default value for this threshold is 10. Set this threshold to a high number, such as 200, to cause the Load Balancer to ignore it. To prevent the Load Balancer from dispatching tasks to the node, set this threshold to 0.

  The Load Balancer uses this threshold in all dispatch modes.

You define resource provision thresholds in the node properties.

CHAPTER 29

License Management

This chapter includes the following topics:

- License Management Overview, 359
- Types of License Keys, 361
- Creating a License Object, 361
- Assigning a License to a Service, 362
- Unassigning a License from a Service, 363
- Updating a License, 363
- Removing a License, 364
- License Properties, 364

License Management Overview

The Service Manager on the master gateway node manages Informatica licenses.

A PowerCenter license enables you to perform the following tasks:

- Run application services. Application services include the Analyst Service, Content Management Service, Data Integration Service, Model Repository Service, Listener Service, Logger Service, PowerCenter Repository Service, PowerCenter Integration Service, Reporting Service, Metadata Manager Service, SAP BW Service, and Web Services Hub.
- Use PowerCenter features. Features include connectivity, Metadata Exchange options, and other options such as session on grid and high availability.

When you install Informatica, the installation program creates a license object in the domain based on the license key you used to install.

You assign a license object to each application service to enable the service. For example, you must assign a license to the PowerCenter Integration Service before you can use the PowerCenter Integration Service to run a workflow.

You can create additional license objects in the domain. You may have multiple license objects that fulfill the requirements specified in your contract. For example, you may have two license objects, where each object allows you to run services on a different operating system. You might also use multiple license objects if you want the same domain to manage different projects. You may want to use a different set of features for each project.

License Validation

The Service Manager validates application service processes when they start. The Service Manager validates the following information for each service process:

- Product version. Verifies that you are running the appropriate version of the application service.
- Platform. Verifies that the application service is running on a licensed operating system.
- Expiration date. Verifies that the license is not expired. If the license expires, no application service assigned to the license can start. You must assign a valid license to the application services to start them.
- PowerCenter options. Determines the options that the application service has permission to use. For example, the Service Manager verifies if the PowerCenter Integration Service can use the Session on Grid option.
- Connectivity. Verifies connections that the application service has permission to use. For example, the Service Manager verifies that PowerCenter can connect to a IBM DB2 database.
- Metadata Exchange options. Determines the Metadata Exchange options that are available for use. For example, the Service Manager verifies that you have access to the Metadata Exchange for Business Objects Designer.

Licensing Log Events

The Service Manager generates log events and writes them to the Log Manager. It generates log events for the following actions:

- You create or delete a license.
- You apply an incremental license key to a license.
- You assign an application service to a license.
- You unassign a license from an application service.
- The license expires.
- The Service Manager encounters an error, such as a validation error.

The log events include the user name and the time associated with the event.

You must have permission on the domain to view the logs for Licensing events. The Licensing events appear in the domain logs.

License Management Tasks

You can perform the following tasks to manage the licenses:

- Create the license in the Administrator tool. You use a license key to create a license in the Administrator tool.
- Assign a license to each application service. Assign a license to each application service to enable the service.
- Unassign a license from an application service. Unassign a license from an application service if you want to discontinue the service or migrate the service from a development environment to a production environment. After you unassign a license from a service, you cannot enable the service until you assign another valid license to it.
- Update the license. Update the license to add PowerCenter options to the existing license.
- Remove the license. Remove a license if it is obsolete.
- Configure user permissions on a license.
- View license details. You may need to review the licenses to determine details, such as expiration date and the maximum number of licensed CPUs. You may want to review these details to ensure you are in compliance with the license. Use the Administrator tool to determine the details for each license.

- Monitor license usage and licensed options. You can monitor the usage of logical CPUs and PowerCenter Repository Services. You can monitor the number of software options purchased for a license and the number of times a license exceeds usage limits in the License Management Report.

You can perform all of these tasks in the Administrator tool or by using *infacmd isp* commands.

Types of License Keys

Informatica provides license keys in license files. The license key is encrypted. When you create the license from the license key file, the Service Manager decrypts the license key and enables the purchased options.

You create a license from a license key file. You apply license keys to the license to enable additional options. Informatica uses the following types of license keys:

- Original keys. Informatica generates an original key based on your contract. Informatica may provide multiple original keys depending on your contract.
- Incremental keys. Informatica generates incremental keys based on updates to an existing license, such as an extended license period or an additional option.

Original Keys

Original keys identify the contract, product, and licensed features. Licensed features include the Informatica edition, deployment type, number of authorized CPUs, and authorized Informatica options and connectivity. You use the original keys to install Informatica and create licenses for services. You must have a license key to install Informatica. The installation program creates a license object for the domain in the Administrator tool. You can use other original keys to create more licenses in the same domain. You use a different original license key for each license object.

Incremental Keys

You use incremental license keys to update an existing license. You add an incremental key to an existing license to add or remove options, such as PowerCenter options, connectivity, and Metadata Exchange options. For example, if an existing license does not allow high availability, you can add an incremental key with the high availability option to the existing license.

The Service Manager updates the license expiration date if the expiration date of an incremental key is later than the expiration date of an original key. The Service Manager uses the latest expiration date. A license object can have different expiration dates for options in the license. For example, the IBM DB2 relational connectivity option may expire on 12/01/2006, and the session on grid option may expire on 04/01/06.

The Service Manager validates the incremental key against the original key used to create the license. An error appears if the keys are not compatible.

Creating a License Object

You can create a license object in a domain and assign the license to application services. You can create the license in the Administrator tool using a license key file. The license key file contains an encrypted original key. You use the original key to create the license.

You can also use the *infacmd isp* AddLicense command to add a license to the domain.

Use the following guidelines to create a license:

- Use a valid license key file. The license key file must contain an original license key. The license key file must not be expired.
- You cannot use the same license key file for multiple licenses. Each license must have a unique original key.
- Enter a unique name for each license. You create a name for the license when you create the license. The name must be unique among all objects in the domain.
- Put the license key file in a location that is accessible by the Administrator tool computer. When you create the license object, you must specify the location of the license key file.

After you create the license, you can change the description. To change the description of a license, select the license in Navigator of the Administrator tool, and then click Edit.

1. In the Administrator tool, click **Create** > **License.**

   The **Create License** window appears.
2. Enter the following options:

Option	Description
Name	Name of the license. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the license. The description cannot exceed 765 characters.
Path	Path of the domain in which you create the license. Read-only field. Optionally, click **Browse** and select a domain in the **Select Folder** window. Optionally, click **Create Folder** to create a folder for the domain.
License File	File containing the original key. Click **Browse** to locate the file.

   If you try to create a license using an incremental key, a message appears that states you cannot apply an incremental key before you add an original key.

   You must use an original key to create a license.
3. Click **Create**.

Assigning a License to a Service

Assign a license to an application service before you can enable the service. When you assign a license to a service, the Service Manager updates the license metadata. You can also use the *infacmd isp* AssignLicense command to assign a license to a service.

1. Select the license in the **Navigator** of the Administrator tool.
2. Click the **Assigned Services** tab.
3. In the **License** tab, click **Actions** > **Edit Assigned Services.**

   The **Assign or Unassign this license to the services** window appears.
4. Select the services under **Unassigned Services**, and click Add.

Use Ctrl-click to select multiple services. Use Shift-click to select a range of services. Optionally, click **Add all** to assign all services.

5. Click **OK**.

Rules and Guidelines for Assigning a License to a Service

Use the following rules and guidelines when you assign licenses:

- You can assign licenses to disabled services.
- If you want to assign a license to a service that has a license assigned to it, you must first unassign the existing license from the service.
- To start a service with backup nodes, you must assign it to a license with high availability.
- To restart a service automatically, you must assign the service to a license with high availability.

Unassigning a License from a Service

You might need to unassign a license from a service if the service becomes obsolete or if you want to discontinue a service. You might want to discontinue a service if you are using more CPUs than you are licensed to use.

You can use the Administrator tool or the *infacmd isp* UnassignLicense command to unassign a license from a service.

You must disable a service before you can unassign a license from it. After you unassign the license from the service, you cannot enable the service. You must assign a valid license to the service to reenable it.

You must disable the service before you can unassign the license. If you try to unassign a license from an enabled service, a message appears that states you cannot remove the service because it is running.

1. Select the license in the **Navigator** of the Administrator tool.
2. Click the **Assigned Services** tab.
3. In the **License** tab, click **Actions** > **Edit Assigned Services.**

   The **Assign or Unassign this license to the services** window apears.
4. Select the service under **Assigned Service**s, and then click **Remove**. Optionally, click **Remove all** to unassign all assigned services.
5. Click **OK**.

Updating a License

You can use an incremental key to update a license. When you add an incremental key to a license, the Service Manager adds or removes licensed options and updates the license expiration date.

You can also use the *infacmd isp* UpdateLicense command to add an incremental key to a license.

Use the following guidelines to update a license:

- Verify that the license key file is accessible by the Administrator tool computer. When you update the license object, you must specify the location of the license key file.

- The incremental key must be compatible with the original key. An error appears if the keys are not compatible.

The Service Manager validates the incremental key against the original key based on the following information:

- Serial number
- Deployment type
- Distributor
- Informatica edition
- Informatica version

1. Select a **license** in the Navigator.
2. Click the **Properties** tab.
3. In the **License** tab, click **Actions** > **Add Incremental Key.**

   The **Update License** window appears.
4. Enter the license file name that contains the incremental keys. Optionally, click **Browse** to select the file.
5. Click **OK**.
6. In the **License Details** section of the **Properties** tab, click **Edit** to edit the description of the license.
7. Click **OK**.

Related Topics:

- "License Details" on page 365

Removing a License

You can remove a license from a domain using the Administrator tool or the *infacmd isp* RemoveLicense command.

Before you remove a license, disable all services assigned to the license. If you do not disable the services, all running service processes abort when you remove the license. When you remove a license, the Service Manager unassigns the license from each assigned service and removes the license from the domain. To re-enable a service, assign another license to it.

If you remove a license, you can still view License Usage logs in the Log Viewer for this license, but you cannot run the License Report on this license.

To remove a license from the domain:

1. Select the license in the **Navigator** of the Administrator tool.
2. Click **Actions** > **Delete.**

License Properties

You can view license details using the Administrator tool or the *infacmd isp* ShowLicense command. The license details are based on all license keys applied to the license. The Service Manager updates the existing license details when you add a new incremental key to the license.

You might review license details to determine options that are available for use. You may also review the license details and license usage logs when monitoring licenses. For example, you can determine the number of CPUs your company is licensed to use for each operating system.

To view license details, select the license in the **Navigator**.

The Administrator tool displays the license properties in the following sections:

- License Details. View license details on the **Properties** tab. Shows license attributes, such as the license object name, description, and expiration date.
- Supported Platforms. View supported platforms on the **Properties** tab. Shows the operating systems and how many CPUs are supported for each operating system.
- Repositories. View the licensed repositories on the **Properties** tab. Shows the maximum number of licensed repositories.
- PowerCenter Options. View the PowerCenter options on the **Options** tab. Shows all licensed PowerCenter options, such as session on grid, high availability, and pushdown optimization.
- Connections. View the licensed connections on the **Options** tab. Shows all licensed connections. The license enables you to use connections, such as DB2 and Oracle database connections.
- Metadata Exchange Options. View the Metadata Exchange options on the **Options** tab. Shows a list of all licensed Metadata Exchange options, such as Metadata Exchange for Business Objects Designer.

You can also run the License Management Report to monitor licenses.

License Details

You can use the license details to view high-level information about the license. Use this license information when you audit the licensing usage.

The general properties for the license appear in the **License Details** section of the **Properties** tab.

The following table describes the general properties for a license:

Property	Description
Name	Name of the license.
Description	Description of the license.
Location	Path to the license in the Navigator.
Edition	PowerCenter Advanced edition.
Software Version	Version of PowerCenter.
Distributed By	Distributor of the PowerCenter product.
Issued On	Date when the license is issued to the customer.
Expires On	Date when the license expires.
Validity Period	Period for which the license is valid.

Property	Description
Serial Number	Serial number of the license. The serial number identifies the customer or project. If you have multiple PowerCenter installations, there is a separate serial number for each project. The original and incremental keys for a license have the same serial number.
Deployment Level	Level of deployment. Values are "Development" and "Production."

You can also use the license event logs to view audit summary reports. You must have permission on the domain to view the logs for license events.

Supported Platforms

You assign a license to each service. The service can run on any operating system supported by the license. One PowerCenter license can support multiple operating system platforms.

The supported platforms for the license appear in the Supported Platforms section of the **Properties** tab.

The following table describes the supported platform properties for a license:

Property	Description
Description	Name of the supported operating system.
Logical CPUs	Number of CPUs you can run on the operating system.
Issued On	Date on which the license was issued for this option.
Expires	Date on which the license expires for this option.

Repositories

The maximum number of active repositories for the license appear in the Repositories section of the Properties tab.

The following table describes the repository properties for a license:

Property	Description
Description	Name of the repository.
Instances	Number of repository instances running on the operating system.
Issued On	Date on which the license was issued for this option.
Expires	Date on which the license expires for this option.

PowerCenter Options

The license enables you to use PowerCenter options such as data cleansing, data federation, and pushdown optimization.

The options for the license appear in the PowerCenter Options section of the **Options** tab.

Connections

The license enables you to use connections such as DB2 and Oracle database connections. The license also enables you to use PowerExchange products such as PowerExchange for Web Services.

The connections for the license appear in the Connections section of the **Options** tab.

Metadata Exchange Options

The license enables you to use Metadata Exchange options such as Metadata Exchange for Business Objects Designer and Metadata Exchange for Microstrategy.

The Metadata Exchange options for the license appear in the Metadata Exchange Options section of the **Options** tab.

CHAPTER 30

Log Management

This chapter includes the following topics:

- Log Management Overview, 368
- Log Manager Architecture, 369
- Log Location, 370
- Log Management Configuration, 370
- Using the Logs Tab, 372
- Log Events, 376

Log Management Overview

The Service Manager provides accumulated log events for the domain, application services, users, sessions, and workflows. To perform the logging function, the Service Manager runs a Log Manager and a Log Agent.

The Log Manager runs on the master gateway node. It collects and processes log events for Service Manager domain operations, application services, and user activity. The log events contain operational and error messages for a domain. The Service Manager and the application services send log events to the Log Manager. When the Log Manager receives log events, it generates log event files. You can view service log events in the Administrator tool based on criteria you provide.

The Log Agent runs on the nodes to collect and process log events for session and workflows. Log events for workflows include information about tasks performed by the PowerCenter Integration Service, workflow processing, and workflow errors. Log events for sessions include information about the tasks performed by the PowerCenter Integration Service, session errors, and load summary and transformation statistics for the session. You can view log events for the last workflow run with the Log Events window in the PowerCenter Workflow Monitor.

Log event files are binary files that the Administrator tool Logs Viewer uses to display log events. When you view log events in the Administrator tool, the Log Manager uses the log event files to display the log events for the domain, application services, and user activity.

You can use the Administrator tool to perform the following tasks with the Log Manager:

- Configure the log location. Configure the node that runs the Log Manager, the directory path for log event files, purge options, and time zone for log events.
- Configure log management. Configure the Log Manager to purge logs or purge logs manually. Save log events to XML, text, or binary files. Configure the time zone for the time stamp in the log event files.
- View log events. View domain function, application service, and user activity log events on the Logs tab. Filter log events by domain, application service type, and user.

Log Manager Architecture

The Service Manager on the master gateway node controls the Log Manager. The Log Manager starts when you start the Informatica services. After the Log Manager starts, it listens for log events from the Service Manager and application services. When the Log Manager receives log events, it generates log event files.

The Log Manager stores session and workflow logs in a separate location from the domain, application service, and user activity logs. The PowerCenter Integration Service writes session and workflow log events to binary files on the node where the PowerCenter Integration Service process runs.

The Log Manager performs the following tasks to process session and workflow logs:

1. During a session or workflow, the PowerCenter Integration Service writes binary log files on the node. It sends information about the logs to the Log Manager.
2. The Log Manager stores information about workflow and session logs in the domain database. The domain database stores information such as the path to the log file location, the node that contains the log, and the PowerCenter Integration Service that created the log.
3. When you view a session or workflow in the Log Events window, the Log Manager retrieves the information from the domain database to determine the location of the session or workflow logs.
4. The Log Manager dispatches a Log Agent to retrieve the log events on each node to display in the Log Events window.

You view session and workflow logs in the Log Events window of the PowerCenter Workflow Monitor.

The Log Manager creates the following types of log files:

- Log events files. Stores log events in binary format. The Log Manager creates log event files to display log events in the Logs tab. When you view events in the Administrator tool, the Log Manager retrieves the log events from the event nodes.

  The Log Manager stores the files by date and by node. You configure the directory path for the Log Manager in the Administrator tool when you configure gateway nodes for the domain. By default, the directory path is the server\logs directory.
- Guaranteed Message Delivery files. Stores domain, application service, and user activity log events. The Service Manager writes the log events to temporary Guaranteed Message Delivery files and sends the log events to the Log Manager.

  If the Log Manager becomes unavailable, the Guaranteed Message Delivery files stay in the server\tomcat\logs directory on the node where the service runs. When the Log Manager becomes available, the Service Manager for the node reads the log events in the temporary files, sends the log events to the Log Manager, and deletes the temporary files.

Log Manager Recovery

When a service generates log events, it sends them to the Log Manager on the master gateway node. When you have the high availability option and the master gateway node becomes unavailable, the application services send log events to the Log Manager on a new master gateway node.

The Service Manager, the application services, and the Log Manager perform the following tasks:

1. An application service process writes log events to a Guaranteed Message Delivery file.
2. The application service process sends the log events to the Service Manager on the gateway node for the domain.
3. The Log Manager processes the log events and writes log event files. The application service process deletes the temporary file.

4. If the Log Manager is unavailable, the Guaranteed Message Delivery files stay on the node running the service process. The Service Manager for the node sends the log events in the Guaranteed Message Delivery files when the Log Manager becomes available, and the Log Manager writes log event files.

Troubleshooting the Log Manager

Domain and application services write log events to Service Manager log files when the Log Manager cannot process log events. The Service Manager log files are located in the server\tomcat\logs directory. The Service Manager log files include catalina.out, localhost_<date>.txt, and node.log. Services write log events to different log files depending on the type of error.

Use the Service Manager log files to troubleshoot issues when the Log Manager cannot process log events. You will also need to use these files to troubleshoot issues when you contact Informatica Global Customer Support.

Note: You can troubleshoot an Informatica installation by reviewing the log files generated during installation. You can use the installation summary log file to find out which components failed during installation.

Log Location

The Service Manager on the master gateway node writes domain, application service, and user activity log event files to the log file directory. When you configure a node to serve as a gateway, you must configure the directory where the Service Manager on this node writes the log event files. Each gateway node must have access to the directory path.

You configure the log location in the Log and Gateway Configuration area on the Properties view for the domain. Configure a directory location that is accessible to the gateway node during installation or when you define the domain. By default, the directory path is the server\logs directory. Store the logs on a shared disk when you have more than one gateway node. If the Log Manager is unable to write to the directory path, it writes log events to node.log on the master gateway node.

When you configure the log location, the Administrator tool validates the directory as you update the configuration. If the directory is invalid, the update fails. The Log Manager verifies that the log directory has read/write permissions on startup. Log files might contain inconsistencies if the log directory is not shared in a highly available environment.

If you have multiple Informatica domains, you must configure a different directory path for the Log Manager in each domain. Multiple domains cannot use the same shared directory path.

Note: When you change the directory path, you must restart Informatica Services on the node you changed.

Log Management Configuration

The Service Manager and the application services continually send log events to the Log Manager. As a result, the directory location for the logs can grow to contain a large number of log events.

You can purge logs events periodically to manage the amount of log events stored by the Log Manager. You can export logs before you purge them to keep a backup of the log events.

Purging Log Events

You can automatically or manually purge log events. The Service Manager purges log events from the log directory according to the purge properties you configure in the Log Management dialog box. You can manually purge log events to override the automatic purge properties.

Purging Log Events Automatically

The Service Manager purges log events from the log directory according to the purge properties. The default value for preserving logs is 30 days and the default maximum size for log event files is 200 MB.

When the number of days or the size of the log directory exceeds the limit, the Log Manager deletes the log event files, starting with the oldest log events. The Log Manager periodically verifies the purge options and purges log events. The Log Manager does not purge session and workflow log files.

Purging Log Events Manually

You can purge log events for the domain, application services, or user activity. When you purge log events, the Log Manager removes the log event files from the log directory. The Log Manager does not remove log event files currently being written to the logs.

Optionally, you can use the *infacmd* PurgeLog command to purge log events.

The following table lists the purge log options:

Option	Description
Log Type	Type of log events to purge. You can purge domain, service, user activity or all log events.
Service Type	When you purge application service log events, you can purge log events for a particular application service type or all application service types.
Purge Entries	Date range of log events you want to purge. You can select the following options: - All Entries. Purges all log events. - Before Date. Purges log events that occurred before this date. Use the yyyy-mm-dd format when you enter a date. Optionally, you can use the calendar to choose the date. To use the calendar, click the date field.

Time Zone

When the Log Manager creates log event files, it generates a time stamp based on the time zone for each log event. When the Log Manager creates log folders, it labels folders according to a time stamp. When you export or purge log event files, the Log Manager uses this property to calculate which log event files to purge or export. Set the time zone to the location of the machine that stores the log event files.

Verify that you do not lose log event files when you configure the time zone for the Log Manager. If the application service that sends log events to the Log Manager is in a different time zone than the master gateway node, you may lose log event files you did not intend to delete. Configure the same time zone for each gateway node.

Note: When you change the time zone, you must restart Informatica Services on the node that you changed.

Configuring Log Management Properties

Configure the Log Management properties in the Log Management dialog box.

1. In the Administrator tool, click the Logs tab.

2. On the Log Actions menu, click Log Management.
3. Enter the number of days for the Log Manager to preserve log events.
4. Enter the maximum disk size for the directory that contains the log event files.
5. Enter the time zone in the following format:

   ```
   GMT(+|-)<hours>:<minutes>
   ```

   For example: GMT+08:00
6. Click OK.

Using the Logs Tab

You can view domain, application service, and user activity log events in the Logs tab of the Administrator tool. When you view log events in the Logs tab, the Log Manager displays the generated log event files in the log directory. When an error message appears in the Administrator tool, the error provides a link to the Logs tab.

You can use the Logs tab to perform the following tasks:

- View log events and the Administrator tool operational errors. View log events for the domain, an application service, or user activity.
- Filter log event results. After you display the log events, you can display log events that match filter criteria.
- Configure columns. Configure the columns you want the Logs tab to display.
- Save log events. You can save log events in XML, text, and binary format.
- Purge log events. You can manually purge log events.
- Copy log event rows. You can copy log event rows.

Viewing Log Events

To view log events in the Logs tab of the Administrator tool, select the Domain, Service, or User Activity view. Next, configure the filter options. You can filter log events based on attributes such as log type, domain function category, application service type, application service name, user, message code, activity code, timestamp, and severity level. The available options depend on whether you choose to view domain, application service, or user activity log events.

To view more information about a log event, click the log event in the search results. On AIX and Linux, if the Log Manager receives an internal error message from the PowerCenter Integration Service, it writes a stack trace to the log event window.

You can view logs to get more information about errors that you receive while working in the Administrator tool.

1. In the Administrator Tool, click the Logs tab.
2. In the contents panel, select Domain, Service, or User Activity view.
3. Configure the filter criteria to view a specific type of log event.

The following table lists the query options:

Log Type	Option	Description
Domain	Category	Category of domain service you want to view.
Service	Service Type	Application service you want to view.
Service	Service Name	Name of the application service for which you want to view log events. You can choose a single application service name or all application services.
Domain, Service	Severity	The Log Manager returns log events with this severity level.
User Activity	User	User name for the Administrator tool user.
User Activity	Security Domain	Security domain to which the user belongs.
Domain, Service, User Activity	Timestamp	Date range for the log events that you want to view. You can choose the following options: - Blank. View all log events. - Within Last Day - Within Last Month - Custom. Specify the start and end date. Default is Within Last Day.
Domain, Service	Thread	Filter criteria for text that appears in the thread data. You can use wildcards (*) in this text field.
Domain, Service	Message Code	Filter criteria for text that appears in the message code. You can also use wildcards (*) in this text field.
Domain, Service	Message	Filter criteria for text that appears in the message. You can also use wildcards (*) in this text field.
Domain, Service	Node	Name of the node for which you want to view log events.
Domain, Service	Process	Process identification number for the Windows or UNIX service process that generated the log event. You can use the process identification number to identify log events from a process when an application service runs multiple processes on the same node.
User Activity	Activity Code	Filter criteria for text that appears in the activity code. You can also use wildcards (*) in this text field.
User Activity	Activity	Filter criteria for text that appears in the activity. You can also use wildcards (*) in this text field.

4. Click the Filter button.

   The Log Manager retrieves the log events and displays them in the Logs tab with the most recent log events first.

5. Click the Reset Filter button to view a different set of log events.

   Tip: To search for logs related to an error or fatal log event, note the timestamp of the log event. Then, reset the filter and use a custom filter to search for log events during the timestamp of the event.

Configuring Log Columns

You can configure the Logs tab to display the following columns:

- Category
- Service Type
- Service Name
- Severity
- User
- Security Domain
- Timestamp
- Thread
- Message Code
- Message
- Node
- Process
- Activity Code
- Activity

Note: The columns appear based on the query options that you choose. For example, when you display a service type, the service name appears in the Logs tab.

1. In the Administrator Tool, click the **Logs** tab.
2. Select the **Domain**, **Service**, or **User Activity** view.
3. To add a column, right-click a column name, select **Columns**, and then the name of the column you want to add.
4. To remove a column, right-click a column name, select **Columns**, and then clear the checkmark next to the name of the column you want to remove.
5. To move a column, select the column name, and then drag it to the location where you want it to appear.

   The Log Manager updates the Logs tab columns with your selections.

Saving Log Events

You can save the log events that you filter and view in the Log Viewer. When you save log events, the Log Manager saves whatever logs that you are viewing based on the filter criteria. To save log events to a file, click Save Logs on the Log Actions menu.

The Log Manager does not delete the log events when you save them. The Administrator Tool prompts you to save or open the saved log events file.

Optionally, you can use the *infacmd* isp GetLog command to retrieve log events.

The format you choose to save log events to depends on how you plan to use the exported log events file:

- XML file. Use XML format if you want to analyze the log events in an external tool that uses XML or if you want to use XML tools, such as XSLT.
- Text file. Use a text file if you want to analyze the log events in a text editor.
- Binary file. Use binary format to back up the log events in binary format. You might need to use this format to send log events to Informatica Global Customer Support.

Exporting Log Events

You can export the log events to an XML, text, or binary file. To export log events to a file, click Export Logs on the Log Actions menu.

When you export log events, you can choose which logs you want to save. When you choose Service logs, you can export logs for a particular service type. You can choose the sort order of the log events in the export file.

The Log Manager does not delete the log events when you export them. The Administrator tool prompts you to save or open the exported log events file.

Optionally, you can use the *infacmd* GetLog command to retrieve log events.

The format you choose to export log events depends on how you plan to use the exported log events file:

- XML file. Use XML format if you want to analyze the log events in an external tool that uses XML or if you want to use XML tools, such as XSLT.
- Text file. Use a text file if you want to analyze the log events in a text editor.
- Binary file. Use binary format to back up the log events in binary format. You might need to use this format to send log events to Informatica Global Customer Support.

The following table describes the export log options for each log type:

Option	Log Type	Description
Type	Domain, Service, User Activity	Type of logs you want to export.
Service Type	Service	Type of application service for which to export log events. You can export log events for PowerCenter Repository Service, PowerCenter Integration Service, Metadata Manager Service, Reporting Service, SAP BW Service, or Web Services Hub. You can also export log events for all service types.
Export Entries	Domain, Service, User Activity	Date range of log events you want to export. You can select the following options: - All Entries. Exports all log events. - Before Date. Exports log events that occurred before this date. Use the yyyy-mm-dd format when you enter a date. Optionally, you can use the calendar to choose the date. To use the calendar, click the date field.
Export logs in descending chronological order	Domain, Service, User Activity	Exports log events starting with the most recent log events.

XML Format

When you export log events to an XML file, the Log Manager exports each log event as a separate element in the XML file. The following example shows an excerpt from a log events XML file:

```
<log xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:common="http://www.informatica.com/pcsf/common"
xmlns:metadata="http://www.informatica.com/pcsf/metadata" xmlns:domainservice="http://
www.informatica.com/pcsf/domainservice" xmlns:logservice="http://www.informatica.com/pcsf/logservice"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098642698" severity="3"
messageCode="AUTHEN_USER_LOGIN_SUCCEEDED" message="User Admin successfully logged in." user="Admin"
stacktrace="" service="authenticationservice" serviceType="PCSF" clientNode="sapphire" pid="0"
threadName="http-8080-Processor24" context="" />
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098517000" severity="3"
```

```
messageCode="LM_36854" message="Connected to node [garnet] on outbound connection [id = 2]." user=""
stacktrace="" service="Copper" serviceType="IS" clientNode="sapphire" pid="4484" threadName="4528"
context="" />
```

Text Format

When you export log events to a text file, the Log Manager exports the log events in Information and Content Exchange (ICE) Protocol. The following example shows an excerpt from a log events text file:

```
2006-02-27 12:29:41 : INFO : (2628 | 2768) : (IS | Copper) : sapphire : LM_36522 : Started process [pid
= 2852] for task instance Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor - Master.
2006-02-27 12:29:41 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 : Starting process
[Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor - Master].
2006-02-27 12:29:36 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : LM_36522 : Started process [pid
= 2632] for task instance Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer.
2006-02-27 12:29:35 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 : Starting process
[Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer].
```

Binary Format

When you export log events to a binary file, the Log Manager exports the log events to a file that Informatica Global Customer Support can import. You cannot view the file unless you convert it to text. You can use the *infacmd* ConvertLogFile command to convert binary log files to text files, XML files, or readable text on the screen.

Viewing Administrator Tool Log Errors

If you receive an error while starting, updating, or removing services in the Administrator tool, an error message in the contents panel of the service provides a link to the Logs tab. Click the link in the error message to access detail information about the error in the Logs tab.

Log Events

The Service Manager and application services send log events to the Log Manager. The Log Manager generates log events for each service type.

You can view the following log event types on the Logs tab:

- Domain log events. Log events generated from the Service Manager functions.
- Analyst Service log events. Log events about each Analyst Service running in the domain.
- Data Integration Service log events. Log events about each Data Integration Service running in the domain.
- Metadata Manager Service log events. Log events about each Metadata Manager Service running in the domain.
- Model Repository log events. Log events about each Model Repository Service running in the domain.
- PowerCenter Integration Service log events. Log events about each PowerCenter Integration Service running in the domain.
- PowerCenter Repository Service log events. Log events from each PowerCenter Repository Service running in the domain.
- Reporting Service log events. Log events from each Reporting Service running in the domain.
- SAP BW Service log events. Log events about the interaction between the PowerCenter and the SAP NetWeaver BI system.

- Web Services Hub log events. Log events about the interaction between applications and the Web Services Hub.
- User activity log events. Log events about domain and security management tasks that a user completes.

Log Event Components

The Log Manager uses a common format to store and display log events. You can use the components of the log events to troubleshoot Informatica.

Each log event contains the following components:

- Service type, category, or user. The Logs tab categorizes events by domain category, service type, or user. If you view application service logs, the Logs tab displays the application service names. When you view domain logs, the Logs tab displays the domain categories in the log. When you view user activity logs, the Logs tab displays the users in the log.
- Message or activity. Message or activity text for the log event. Use the message text to get more information about the log events for domain and application services. Use the activity text to get more information about log events for user activity. Some log events contain embedded log event in the message texts. For example, the following log events contains an embedded log event:

  ```
  Client application [PmDTM], connection [59]: recv failed.
  ```

  In this log event, the following log event is the embedded log event:

  ```
  [PmDTM], connection [59]: recv failed.
  ```

  When the Log Manager displays the log event, the Log Manager displays the severity level for the embedded log event.
- Security domain. When you view user activity logs, the Logs tab displays the security domain for each user.
- Message or activity code. Log event code.
- Process. The process identification number for the Windows or UNIX service process that generated the log event. You can use the process identification number to identify log events from a process when an application service runs multiple processes on the same node.
- Node. Name of the node running the process that generated the log event.
- Thread. Identification number or name of a thread started by a service process.
- Time stamp. Date and time the log event occurred.
- Severity. The severity level for the log event. When you view log events, you can configure the Logs tab to display log events for a specific severity level.

Domain Log Events

Domain log events are log events generated from the domain functions the Service Manager performs. Use the domain log events to view information about the domain and troubleshoot issues. You can use the domain log events to troubleshoot issues related to the startup and initialization of nodes and application services for the domain.

Domain log events include log events from the following functions:

- Authorization. Log events that occur when the Service Manager authorizes user requests for services. Requests can come from the Administrator tool.
- Domain Configuration. Log events that occur when the Service Manager manages the domain configuration metadata.
- Node Configuration. Log events that occur as the Service Manager manages node configuration metadata in the domain.

- Licensing. Log events that occur when the Service Manager registers license information.
- License Usage. Log events that occur when the Service Manager verifies license information from application services.
- Log Manager. Log events from the Log Manager. The Log Manager runs on the master gateway node. It collects and processes log events for Service Manager domain operations and application services.
- Log Agent. Log events from the Log Agent. The Log Agent runs on all nodes that process workflows and sessions in the domain. It collects and processes log events from workflows and sessions.
- Monitoring. Log events about Domain Functions.
- User Management. Log events that occur when the Service Manager manages users, groups, roles, and privileges.
- Service Manager. Log events from the Service Manager and signal exceptions from DTM processes. The Service Manager manages all domain operations. If the error severity level of a node is set to Debug, when a service starts the log events include the environment variables used by the service.

Analyst Service Log Events

Analyst Service log events contain the following information:

- Managing projects. Log events about managing projects in the Informatica Analyst, such as creating objects, folders, and projects. Log events about creating profiles, scorecards, and reference tables.
- Running jobs. Log events about running profiles and scorecards. Logs about previewing data.
- User permissions. Log events about managing user permissions on projects.

Data Integration Service Log Events

Data Integration Service logs contain logs about the following events:

- Configuration. Log events about system or service configuration changes, application deployment or removal, and logs about the associated profiling warehouse.
- Data Integration Service processes. Log events about application deployment, data object cache refresh, and user requests to run mappings or jobs.
- System failures. Log events about failures that cause the Data Integration service to be unavailable, such as Model Repository connection failures or the service failure to start.

Listener Service Log Events

The PowerExchange Listener logs contain information about the application service that manages the PowerExchange Listener.

The Listener Service logs contain the following information:

- Client communication. Log events for communication between a PowerCenter or PowerExchange client and a data source.
- Listener service. Log events about the Listener service, including configuring, enabling, and disabling the service.
- Listener service operations. Log events for operations such as managing bulk data movement and change data capture.

Logger Service Log Events

The PowerExchange Logger Service writes logs about the application service that manages the PowerExchange Logger.

The Logger Service logs contain the following information:

- Connections. Log events about connections between the Logger Service and the source databases.
- Logger service. Log events about the Logger Service, including configuring, enabling, and disabling the service.
- Logger service operations. Log events for operations such as capturing changed data and writing the data to PowerExchange Logger files.

Model Repository Service Log Events

Model Repository Service log events contain the following information:

- Model Repository connections. Log events for connections to the repository from the Informatica Developer, Informatica Analyst, and Data Integration Service.
- Model Repository Service. Log events about Model Repository service, including enabling, disabling, starting, and stopping the service.
- Repository operations. Log events for repository operations such as creating and deleting repository content, and adding deployed applications.
- User permissions. Log events about managing user permissions on the repository.

Metadata Manager Service Log Events

The Metadata Manager Service log events contain information about each Metadata Manager Service running in the domain.

Metadata Manager Service log events contain the following information:

- Repository operations. Log events for accessing metadata in the Metadata Manager repository.
- Configuration. Log events about the configuration of the Metadata Manager Service.
- Run-time processes. Log events for running a Metadata Manager Service, such as missing native library files.
- PowerCenter Integration Service log events. Session and workflow status for sessions and workflows that use a PowerCenter Integration Service process to load data to the Metadata Manager warehouse or to extract source metadata.

To view log events about how the PowerCenter Integration Service processes a PowerCenter workflow to load data into the Metadata Manager warehouse, you must view the session or workflow log.

PowerCenter Integration Service Log Events

The PowerCenter Integration Service log events contain information about each PowerCenter Integration Service running in the domain.

PowerCenter Integration Service log events contain the following information:

- PowerCenter Integration Service processes. Log events about the PowerCenter Integration Service processes, including service ports, code page, operating mode, service name, and the associated repository and PowerCenter Repository Service status.
- Licensing. Log events for license verification for the PowerCenter Integration Service by the Service Manager.

PowerCenter Repository Service Log Events

The PowerCenter Repository Service log events contain information about each PowerCenter Repository Service running in the domain.

PowerCenter Repository Service log events contain the following information:

- PowerCenter Repository connections. Log events for connections to the repository from PowerCenter client applications, including user name and the host name and port number for the client application.
- PowerCenter Repository objects. Log events for repository objects locked, fetched, inserted, or updated by the PowerCenter Repository Service.
- PowerCenter Repository Service processes. Log events about PowerCenter Repository Service processes, including starting and stopping the PowerCenter Repository Service and information about repository databases used by the PowerCenter Repository Service processes. Also includes repository operating mode, the nodes where the PowerCenter Repository Service process runs, initialization information, and internal functions used.
- Repository operations. Log events for repository operations, including creating, deleting, restoring, and upgrading repository content, copying repository contents, and registering and unregistering local repositories.
- Licensing. Log events about PowerCenter Repository Service license verification.
- Security audit trails. Log events for changes to users, groups, and permissions. To include security audit trails in the PowerCenter Repository Service log events, you must enable the SecurityAuditTrail general property for the PowerCenter Repository Service in the Administrator tool.

Reporting Service Log Events

The Reporting Service log events contain information about each Reporting Service running in the domain.

Reporting Service log events contain the following information:

- Reporting Service processes. Log events about starting and stopping the Reporting Service.
- Repository operations. Log events for the Data Analyzer repository operations. This includes information on creating, deleting, backing up, restoring, and upgrading the repository content, and upgrading users and groups.
- Licensing. Log events about Reporting Service license verification.
- Configuration. Log events about the configuration of the Reporting Service.

SAP BW Service Log Events

The SAP BW Service log events contain information about the interaction between PowerCenter and the SAP NetWeaver BI system.

SAP NetWeaver BI log events contain the following log events for an SAP BW Service:

- SAP NetWeaver BI system log events. Requests from the SAP NetWeaver BI system to start a workflow and status information from the ZPMSENDSTATUS ABAP program in the process chain.
- PowerCenter Integration Service log events. Session and workflow status for sessions and workflows that use a PowerCenter Integration Service process to load data to or extract data from SAP NetWeaver BI.

To view log events about how the PowerCenter Integration Service processes an SAP NetWeaver BI workflow, you must view the session or workflow log.

Web Services Hub Log Events

The Web Services Hub log events contain information about the interaction between applications and the Web Services Hub.

Web Services Hub log events contain the following log events:

- Web Services processes. Log events about web service processes, including starting and stopping Web Services Hub, web services requests, the status of the requests, and error messages for web service calls. Log events include information about which service workflows are fetched from the repository.
- PowerCenter Integration Service log events. Workflow and session status for service workflows including invalid workflow errors.

User Activity Log Events

User activity log events describe all domain and security management tasks that a user completes. Use the user activity log events to determine when a user created, updated, or removed services, nodes, users, groups, or roles.

The Service Manager writes user activity log events when the Service Manager needs to authorize a user to perform one of the following domain actions:

- Adds, updates, or removes an application service.
- Enables or disables a service process.
- Starts, stops, enables, or disables a service.
- Adds, updates, removes, or shuts down a node.
- Modifies the domain properties.
- Moves a folder in the domain.
- Assigns permissions on domain objects to users or groups.

The Service Manager also writes user activity log events each time a user performs one of the following security actions:

- Adds, updates, or removes a user, group, role, or operating system profile.
- Adds or removes an LDAP security domain.
- Assigns roles or privileges to a user or group.

CHAPTER 31

Monitoring

This chapter includes the following topics:

- Monitoring Overview, 382
- Monitoring Setup, 386
- Monitor Data Integration Services , 388
- Monitor Jobs, 389
- Monitor Applications, 390
- Monitor Deployed Mapping Jobs, 391
- Monitor SQL Data Services, 392
- Monitor Web Services, 395
- Monitor Logical Data Objects, 397
- Monitoring a Folder of Objects, 398
- Monitoring an Object, 399

Monitoring Overview

Monitoring is a domain function that the Service Manager performs. The Service Manager stores the monitoring configuration in the Model repository. The Service Manager also persists, updates, retrieves, and publishes run-time statistics for integration objects in the Model repository. Integration objects include jobs, applications, SQL data services, web services, and logical data objects.

Use the **Monitoring** tab in the Administrator tool to monitor integration objects that run on a Data Integration Service. The **Monitoring** tab shows properties, run-time statistics, and run-time reports about the integration objects. For example, the **Monitoring** tab can show the general properties and the status of a profiling job. It can also show the user who initiated the job and how long it took the job to complete.

You can also access monitoring from the following locations:

Informatica Monitoring tool

You can access monitoring from the Informatica Monitoring tool. The Monitoring tool is a direct link to the **Monitoring** tab of the Administrator tool. The Monitoring tool is useful if you do not need access to any other features in the Administrator tool. You must have at least one monitoring privilege to access the Monitoring tool. You can access the Monitoring tool using the following URL:

```
http://<Administrator tool host> <Administrator tool port>/monitoring
```

Analyst tool

You can access monitoring from the Analyst tool. When you access monitoring from the Analyst tool, the monitoring results appear in the **Job Status** tab. The **Job Status** tab shows the status of Analyst tool jobs, such as profile jobs, scorecard jobs, and jobs that load mapping specification results to the target.

Developer tool

You can access monitoring from the Developer tool. When you access monitoring from the Developer tool, the monitoring results appear in the Informatica Monitoring tool. The Informatica Monitoring tool shows the status of Developer tool jobs, such as mapping jobs, web services, and SQL data services.

Navigator in the Monitoring Tab

Select an object in the Navigator of the **Monitoring** tab to monitor the object.

You can select the following types of objects in the Navigator in the **Monitoring** tab:

Data Integration Service

View general properties about the Data Integration Service, and view statistics about objects that run on the Data Integration Service.

Folder

View a list of objects contained in the folder. The folder is a logical grouping of objects. When you select a folder, a list of objects appears in the contents panel. The contents panel shows multiple columns that show properties about each object. You can configure the columns that appear in the contents panel.

The following table shows the folders that appear in the Navigator:

Folder	Location
Jobs	Appears under the Data Integration Service.
Deployed Mapping Jobs	Appears under the corresponding application.
Logical Data Objects	Appears under the corresponding application.
SQL Data Services	Appears under the corresponding application.
Web Services	Appears under the corresponding application.

Integration objects

View information about the selected integration object. Integration objects include instances of applications, deployed mapping jobs, SQL data services, web services, and logical data objects.

Views in the Monitoring Tab

When you select an integration object in the Navigator or an object link in the contents panel of the **Monitoring** tab, multiple views of information appear in the contents panel. The views show information about the selected object, such as properties, run-time statistics, and run-time reports.

Depending on the type of object you select in the Navigator, the contents panel may display the following views:

Properties view

Shows general properties and run-time statistics about the selected object. General properties may include the name and description of the object. Statistics vary based on the selected object type.

Reports view

Shows reports for the selected object. The reports contain key metrics for the object. For example, you can view reports to determine the longest running jobs on a Data Integration Service during a particular time period.

Connections view

Shows connections defined for the selected object. You can view statistics about each connection, such as the number of closed, aborted, and total connections.

Requests view

Shows requests from an SQL data service or a Web Services data service and the details of each request. For a SQL data service, you can run SQL requests against a SQL connection to a virtual table. You can run SQL requests as long as the SQL connection is open. For a web service, you can use a web service client to run a SOAP request. Each SOAP request is associated with a web service operation.

Virtual Tables view

Shows virtual tables defined in an SQL data service. You can also view properties and cache refresh details for each virtual table.

Operations view

Shows the operations defined for the web service.

Statistics in the Monitoring Tab

The **Statistics** section in the **Properties** view shows aggregated statistics about the selected object. For example, when you select a Data Integration Service in the Navigator of the **Monitoring** tab, the **Statistics** section shows the total number of running, failed, canceled, and completed jobs that run on the selected Data Integration Service.

You can view statistics about the following integration objects:

Applications

Includes deployed mapping jobs, logical data objects, SQL data services, and web services.

Connections

Includes SQL connections to virtual databases.

Jobs

Includes jobs for profiles, previews, undeployed mappings, reference tables, and scorecards.

Requests

Includes SQL data service requests and web service requests.

The following table describes the statistics for each object type:

Object Type	Statistics
Connection Objects	- Aborted. Number of aborted connections. - Closed. Number of closed connections. Closed connections are database connections on which SQL data service requests have previously run, but that are

Object Type	Statistics
	now closed. You cannot run requests against closed connections. - Total. Total number of connections.
Jobs	- Aborted. Number of aborted jobs. - Canceled. Number of canceled jobs. - Completed. Number of completed jobs. - Failed. Number of failed jobs. - Total. Total number of jobs.
Request Objects	- Aborted. Number of aborted requests. - Completed. Number of completed requests. - Failed. Number of failed requests. - Total. Total number of requests.

Related Topics:

- "Properties View for a Data Integration Service" on page 388
- " Properties View for a Web Service" on page 396
- "Properties View for an Application" on page 390
- "Properties View for an SQL Data Service" on page 393

Reports in the Monitoring Tab

You can view monitoring reports in the **Reports** view of the **Monitoring** tab. The **Reports** view appears when you select the appropriate object in the Navigator. You can view reports to monitor objects deployed to a Data Integration Service, such as jobs, web services, and SQL data services.

The reports that appear in the **Reports view** are based on the selected object type and the reports configured to appear in the view. You must configure the monitoring preferences to enable reports to appear in the **Reports** view. By default, no reports appear in the **Reports** view.

You can view the following monitoring reports:

Longest Duration Jobs

Shows jobs that ran the longest during the specified time period. The report shows the job ID, type, name, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Mapping Jobs

Shows mapping jobs that ran the longest during the specified time period. The report shows the job ID, name, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Profile Jobs

Shows profile jobs that ran the longest during the specified time period. The report shows the job ID, name, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Reference Table Jobs

Shows reference table process jobs that ran the longest during the specified time period. Reference table jobs are jobs where you export or import reference table data. The report shows the job ID, name, and duration.

You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Scorecard Jobs

Shows scorecard jobs that ran the longest during the specified time period. The report shows the job ID, name, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Most Active SQL Connections

Shows SQL connections that received the most connection requests. The report shows the connection ID and the total number of connection requests. You can view this report in the **Reports** view when you monitor a Data Integration Service, an application, or an SQL data service in the **Monitoring** tab.

Most Active Users for Jobs

Shows users that ran the most number of jobs during the specified time period. The report shows the user name and the total number of jobs that the user ran. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Most Active WebService Client IP

Shows IP addresses that received the most number of web service requests during the specified time period. The report shows the IP address and the total number of requests. You can view this report in the **Reports** view when you monitor a Data Integration Service, an application, or a web service in the **Monitoring** tab.

Related Topics:

- "Reports View for a Data Integration Service" on page 389
- "Reports View for a Web Service" on page 396
- "Reports View for an Application" on page 391
- "Reports View for an SQL Data Service" on page 395

Monitoring Setup

You configure the domain to set up monitoring. When you set up monitoring, the Data Integration Service stores persisted statistics and monitoring reports in a Model repository. Persisted statistics are historical information about integration objects that previously ran. The monitoring reports show key metrics about an integration object.

Complete the following tasks to enable and view statistics and monitoring reports:

1. Configure the global settings for the Data Integration Service.
2. Configure preferences for statistics and reports.

Step 1. Configure Global Settings

Configure global settings for the domain to specify the Model repository that stores the run-time statistics about objects deployed to Data Integration Services. The global settings apply to all Data Integration Services defined in the domain.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the domain.
3. In the contents panel, click **Actions** > **Global Settings**.

4. Edit the following options:

Option	Description
Model Repository Service	Name of the Model Repository Service that stores the historical information.
Username	User name for the Model Repository Service.
Password	Password for the Model Repository Service.
Number of Days to Preserve Historical Data	Number of days that the Data Integration Service stores historical run-time statisics. Set to '0' if you do not want the Data Integration Service to preserve historical run-time statistics.
Purge Statistics Every	Frequency, in days, at which the Data Integration Service purges statistics. Default is 1.
Days At	Time of day when the Data Integration Service purges old statistics. Default is 1:00 a.m.
Maximum Number of Sortable Records	Maximum number of records that can be sorted. Default is 3,000.
Maximum Delay for Update Notifications	Maximum time period, in seconds, that the Data Integration Service buffers the statistics before persisting the statistics in the Model repository and displaying them in the **Monitoring** tab. Default is 10.
Show Milliseconds	Include milliseconds for date and time fields in the **Monitoring** tab.

5. Click **OK**.
6. Click **Save** to save the global settings.

Restart all Data Integration Services in the domain to apply the settings.

Step 2. Configure Monitoring Preferences

You must configure the time ranges for statistics and reports for the domain. These settings apply to all Data Integration Services. You also can configure the reports that appear in the **Monitoring** tab.

You must specify a Model Repository Service in the global settings, and the Model Repository Service must be available before you can configure the preferences.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the domain.
3. In the contents panel, click **Actions** > **Preferences**.
4. Click the **Statistics** tab.
5. Configure the time ranges that you want to use for statistics, and then select the frequency at which the statistics assigned to each time range should be updated.
6. Select a default time range to appear for all statistics.
7. Click the **Reports** tab.

8. Enable the time ranges that you want to use for reports, and then select the frequency at which the reports assigned to each time range should be updated.
9. Select a default time range to appear for all reports, and then click **OK**.
10. Click **Select Reports**.
11. Add the reports that you want to run to the **Selected Reports** box.
12. Organize the reports in the order in which you want to view them on the **Monitoring** tab.
13. Click **OK** to close the **Select Reports** window.
14. Click **OK** to close the **Preferences** window.
15. Click **Save** to save the preferences.

Monitor Data Integration Services

You can monitor Data Integration Services on the **Monitoring** tab.

When you select a Data Integration Service in the Navigator of the **Monitoring** tab, the contents panel shows the following views:

- **Properties** view
- **Reports** view

Properties View for a Data Integration Service

The **Properties** view shows the general properties and run-time statistics for objects that ran on the selected Data Integration Service.

When you select a Data Integration Service in the Navigator, you can view the general properties and run-time statistics.

General Properties for a Data Integration Service

You can view general properties, such as the service name, object type, and description. The Persist Statistics Enabled property indicates whether the Data Integration Service stores persisted statistics in the Model repository. This option is true when you configure the global settings for the domain.

You can also view information about objects that run on the Data Integration Service. To view information about an object, select the object in the Navigator or contents panel. Depending on the object type, details about the object appear in the contents panel or details panel.

Statistics for a Data Integration Service

You can view run-time statistics about objects that run on the Data Integration Service. Select the object type and time period to display the statistics. You can view statistics about jobs, applications, connections, and requests. For example, you can view the number of failed, canceled, and completed profiling jobs in the last four hours.

Related Topics:

- “Statistics in the Monitoring Tab” on page 384

Reports View for a Data Integration Service

The **Reports** view shows monitoring reports about objects that run on the selected Data Integration Service.

When you monitor a Data Integration Service in the **Monitoring** tab, the **Reports** view shows reports about jobs, web services, and SQL data services. For example, you can view the Most Active Users for Jobs report to determine users that ran the most jobs during a specific time period.

Related Topics:

- “Reports in the Monitoring Tab” on page 385

Monitor Jobs

You can monitor Data Integration Service jobs on the **Monitoring** tab. A job is a preview, scorecard, profile, mapping, or reference table process that runs on a Data Integration Service. Reference table jobs are jobs where you export or import reference table data.

When you select **Jobs** in the Navigator of the **Monitoring** tab, a list of jobs appears in the contents panel. By default, you can view jobs that you created. If you have the appropriate monitoring privilege, you can view jobs of other users. You can view properties about each job in the contents panel. You can also view logs, view the context of jobs, and cancel jobs.

When you select a job in the contents panel, job properties for the selected job appear in the details panel. Depending on the type of job, the details panel may show general properties and mapping properties.

General Properties for a Job

The details panel shows the general properties about the selected job, such as the name, job type, user who started the job, and end time of the job.

Mapping Properties for a Job

The **Mapping** section appears in the details panel when you select a profile or scorecard job in the contents panel. These jobs have an associated mapping. You can view mapping properties such as the request ID, the mapping name, and the log file name.

Viewing Logs for a Job

You can download the logs for a job to view the job details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service and select **Jobs**.
3. In the contents panel, select a job.
4. Click **Actions** > **View Logs for Selected Object**.

   A dialog box appears with the option to open or save the log file.

Viewing the Context of a Job

View the context of a job to view all jobs that started around the same time as the selected job. You might view the context of a job to troubleshoot why a job failed. For example, you search for your job by name. The filtered list of jobs only shows your job. You notice that your job failed. When you view the context of your job, an unfiltered list of jobs appear in a separate working view, showing you all jobs that started around the same time as your job. You notice that other jobs have also failed around the same time as your job. You determine that the Data Integration Service was unavailable.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service and select **Jobs**.
3. In the contents panel, select a job.
4. Click **Actions** > **View Context**.

Canceling a Job

You can cancel a running job. You may want to cancel a job that hangs or that is taking an excessive amount of time to complete.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service and select **Jobs**.
3. In the contents panel, select a job.
4. Click **Actions** > **Cancel Selected Object**.

Monitor Applications

You can monitor applications on the **Monitoring** tab.

When you select an application in the Navigator of the **Monitoring** tab, the contents panel shows the following views:

- **Properties** view
- **Reports** view

You can expand an application in the Navigator to monitor the objects in the application, such as deployed mapping jobs, SQL data services, logical data objects, and web services.

Properties View for an Application

The **Properties** view shows general properties and run-time statistics about each application and the objects in an application. Applications can include SQL data services, deployed mapping jobs, logical data objects, and web services.

When you select an application in the contents panel of the **Properties** view, you can view the general properties and run-time statistics.

General Properties for an Application

You can view general properties, such as the name and description of the application. You can also view additional information about the objects in an application. To view information about an object, select the folder in the Navigator and the object in the contents panel. The object appears under the application in the Navigator. Details about the object appear in the details panel.

Statistics for an Application

You can view the following run-time statistics about an application and about the jobs, connections, and requests associated with the application. For example, you can view the number of enabled and disabled applications, number of aborted connections, and number of completed, failed, and canceled jobs.

Related Topics:

- "Statistics in the Monitoring Tab" on page 384

Reports View for an Application

The **Reports** view shows monitoring reports about the selected application.

When you monitor an application in the **Monitoring** tab, the **Reports** view shows reports about objects contained in the application. For example, you can view the Most Active WebService Client IP report to determine the IP addresses that received the most number of web service requests during a specific time period.

Related Topics:

- "Reports in the Monitoring Tab" on page 385

Monitor Deployed Mapping Jobs

You can monitor deployed mapping jobs on the **Monitoring** tab.

You can view information about deployed mapping jobs in an application. When you select **Deployed Mapping Jobs** under an application in the Navigator of the **Monitoring** tab, a list of deployed mapping jobs appears in the contents panel. The contents panel shows properties about each deployed mapping job, such as Job ID, name of mapping, and state of the job.

Select a deployed mapping job in the contents panel to view logs for the job, reissue the job, and cancel the job.

When you select the link for a deployed mapping job in the contents panel, the contents panel shows the **Mapping Properties** view. The view shows mapping properties such as the request ID, the mapping name, and the log file name.

Viewing Logs for a Deployed Mapping Job

You can download the logs for a deployed mapping job to view the job details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Deployed Mapping Jobs**.

   A list of mapping jobs appear in the contents panel.
4. In the contents panel, select a mapping job.
5. Click **Actions** > **View Logs for Selected Object**.

   A dialog box appears with the option to open or save the log file.

Reissuing a Deployed Mapping Job

You can reissue a deployed mapping job when the mapping jobs fails. When you reissue a deployed mapping job, the Data Integration Service runs the job again.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Deployed Mapping Jobs**.

   The contents panel displays a list of deployed mapping jobs.
4. In the contents panel, select a deployed mapping job.
5. Click **Actions** > **Reissue Selected Object**.

Canceling a Deployed Mapping Job

You can cancel a deployed mapping job. You may want to cancel a deployed mapping job that hangs or that is taking an excessive amount of time to complete.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Deployed Mapping Jobs**.

   The contents panel displays a list of deployed mapping jobs.
4. In the contents panel, select a deployed mapping job.
5. Click **Actions** > **Cancel Selected Job**.

Monitor SQL Data Services

You can monitor SQL data services on the **Monitoring** tab. An SQL data service is a virtual database that you can query. It contains a schema and other objects that represent underlying physical data.

You can view information about the SQL data services included in an application. When you select **SQL Data Services** under an application in the Navigator of the **Monitoring** tab, a list of SQL data services appears in the contents panel. The contents panel shows properties about each SQL data service, such as the name, description, and state.

When you select the link for a SQL data service in the contents panel, the contents panel shows the following views:

- **Properties** view
- **Connections** view
- **Requests** view
- **Virtual Tables** view
- **Reports** view

Properties View for an SQL Data Service

The **Properties** view shows general properties and run-time statistics for an SQL data service.

When you select an SQL data service in the contents panel of the **Properties** view, you can view the general properties and run-time statistics.

General Properties for an SQL Data Service

You can view general properties, such as the SQL data service name and the description.

Statistics for an SQL Data Service

You can view run-time statistics about connections and requests for the SQL data service. Sample statistics include the number of connections to the SQL data service, the number of requests, and the number of aborted connections.

Related Topics:

- "Statistics in the Monitoring Tab" on page 384

Connections View for an SQL Data Service

The **Connections** view displays properties about connections from third-party clients. The view shows properties such as the connection ID, state of the connection, connect time, elapsed time, and disconnect time.

When you select a connection in the contents panel, you can abort the connection or access the **Properties** view and **Requests** view in the details panel.

Properties View

The **Properties** view in the details panel shows the user who is using the connection, the state of the connection, and the connect time.

Requests View

The **Requests** view in the details panel shows information about the requests for the SQL connection. Each connection can have more than one request. The view shows request properties such as request ID, user name, state of the request, start time, elapsed time, and end time.

Aborting a Connection

You can abort a connection to prevent it from sending more requests to the SQL data service.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.

   The contents panel displays a list of SQL data services.
4. In the contents panel, select an SQL data service.

   The contents panel displays mutiple views for the SQL data service.
5. In the contents panel, click the **Connections** view.

   The contents panel lists connections to the SQL data service.
6. Select a connection.
7. Click **Actions** > **Abort Selected Connection**.

Requests View for an SQL Data Service

The **Requests** view displays properties for requests for each SQL connection.

The **Requests** view shows properties about the requests for the SQL connection. Each connection can have more than one request. The view shows request properties such as request ID, connection ID, user name, state of the request, start time, elapsed time, and end time.

Select a request in the contents panel to view additional information about the request in the details panel.

Canceling an SQL Data Service Connection Request

You can cancel an SQL Data Service connection request. You might want to cancel a connection request that hangs or that is taking an excessive amount of time to complete.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.

   The contents panel displays a list of SQL data services.
4. In the contents panel, select an SQL data service.
5. In the contents panel, click the **Requests** view.

   A list of connection requests for the SQL data service appear.
6. In the contents panel, select a request row.
7. Click **Actions** > **Cancel Selected Request**.

Viewing Logs for an SQL Data Service Request

You can download the logs for an SQL data service request to view the request details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.

   The contents panel displays a list of SQL data services.
4. In the contents panel, select an SQL data service.
5. In the contents panel, click the **Requests** view.

   A list of requests for the SQL data service appear.
6. In the contents panel, select a request row.
7. Click **Actions** > **View Logs for Selected Object**.

Virtual Tables View for an SQL Data Service

The **Virtual Tables** view displays properties about the virtual tables in the SQL data service.

The view shows properties about the virtual tables, such as the name and description. When you select a virtual table in the contents panel, you can view the **Properties** view and **Cache Refresh Runs** view in the details panel.

Properties View

The **Properties** view displays general information and run-time statistics about the selected virtual table. General properties include the virtual table name and the schema name. Monitoring statistics include the number of request, the number of rows cached, and the last cache refresh time.

Cache Refresh Runs View

The **Cache Refresh Runs** view displays cache information for the selected virtual table. The view includes the cache run ID, the request count, row count, and the cache hit rate. The cache hit rate is the total number of requests on the cache divided by the total number of requests for the data object.

Viewing Logs for an SQL Data Service Table Cache

You can download the logs for an SQL data service table cache to view the table cache details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.

   The contents panel displays a list of SQL data services.
4. In the contents panel, select an SQL data service.
5. In the contents panel, click the **Virtual Tables** view.

   A list of virtual tables for the SQL data service appear.
6. In the contents panel, select a table row.

   Details about the selected table appear in the details panel.
7. In the details panel, select the **Cache Refresh Runs** view.
8. In the details panel, click **View Logs for Selected Object**.

Reports View for an SQL Data Service

The **Reports** view shows monitoring reports about the selected SQL data service.

When you monitor an SQL data service in the **Monitoring** tab, the **Reports** view shows reports about the SQL data service. For example, you can view the Most Active SQL Connections report to determine the SQL connections that received the most connection requests during a specific time period.

Related Topics:

- “Reports in the Monitoring Tab” on page 385

Monitor Web Services

You can monitor web services on the **Monitoring** tab. Web services are business functions that operate over the Web. They describe a collection of operations that are network accessible through standardized XML messaging.

You can view information about web services included in an application. When you select **Web Services** under an application in the Navigator of the **Monitoring** tab, a list of web services appears in the contents panel. The contents panel shows properties about each web service, such as the name, description, and state of each web service.

When you select the link for a web service in the contents panel, the contents panel shows the following views:

- **Properties** view
- **Reports** view
- **Operations** view

- **Requests** view

Properties View for a Web Service

The **Properties** view shows general properties and run-time statistics for a web service.

When you select a web service in the contents panel of the **Properties** view, you can view the general properties and monitoring statistics.

General Properties for a Web Service

You can view general properties about the web service, such as the name and type of object.

Statistics for a Web Service

You can view run-time statistics about web service requests during a specific time period. The **Statistics** section shows the number of completed, failed, and total web service requests.

Related Topics:

- "Statistics in the Monitoring Tab" on page 384

Reports View for a Web Service

The **Reports** view shows monitoring reports about the selected web service.

When you monitor a web service in the **Monitoring** tab, the **Reports** view shows reports about the web service. For example, you can view the Most Active WebService Client IP report to determine the IP addresses that received the most number of web service requests during a specific time period.

Related Topics:

- "Reports in the Monitoring Tab" on page 385

Operations View for a Web Service

The **Operations** view shows the name and description of each operation included in the web service. The view also displays properties, requests, and reports about each operation.

When you select a web service operation in the contents panel, the details panel shows the **Properties** view, **Requests** view, and **Reports** view.

Properties View for a Web Service Operation

The **Properties** view shows general properties and statistics about the selected web service operation. General properties include the operation name and type of object. The view also shows statistics about the web service operation during a particular time period. Statistics include the number of completed, failed, and total web service requests.

Requests View for a Web Service Operation

The **Requests** view shows properties about each web service operation, such as request ID, user name, state, start time, elapsed time, and end time. You can filter the list of requests. You can also view logs for the selected web service request.

Reports View for a Web Service Operation

The **Reports** view shows reports about web service operations.

Requests View for a Web Service

The **Requests** view shows properties about each web service request, such as request ID, user name, state, start time, elapsed time, and end time. You can filter the list of requests.

When you select a web service request in the contents panel, you can view logs about the request in the details panel. The details panel shows general properties and statistics about the selected web service request. Statistics include the number of completed, failed, and total web service requests.

Monitor Logical Data Objects

You can monitor logical data objects on the **Monitoring** tab.

You can view information about logical data objects included in an application. When you select **Logical Data Objects** under an application in the Navigator of the **Monitoring** tab, a list of logical data objects appears in the contents panel. The contents panel shows properties about each logical data object.

Select a logical data object in the contents panel to download the logs for a data object.

When you select the link for a logical data object in the contents panel, the details panel shows the following views:

- **Properties** view
- **Cache Refresh Runs** view

Properties View for a Logical Data Object

The **Properties** view shows general properties and run-time statistics about the selected object.

You can view properties such as the data object name, logical data object model, folder path, cache state, and last cache refresh information.

Cache Refresh Runs View for a Logical Data Object

The **Cache Refresh Runs** view shows cache refresh details about the selected logical data object.

The **Cache Refresh Runs** view shows cache refresh details such as the cache run ID, request count, and row count.

Viewing Logs for Data Object Cache Refresh Runs

You can download the logs for data object cache refresh runs to view the cache refresh run details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Logical Data Objects**.

   The contents panel displays a list of logical data objects.
4. In the contents panel, select a logical data object.

   Details about the selected data object appear in the details panel.
5. In the details panel, select the **Cache Refresh Runs** view.
6. In the details panel, click **View Logs for Selected Object**.

Monitoring a Folder of Objects

You can view properties and statistics about all objects in a folder in the Navigator of the **Monitoring** tab. You can select one of the following folders: Jobs, Deployed Mapping Jobs, Logical Data Objects, SQL Data Services, and Web Services.

You can apply a filter to limit the number of objects that appear in the contents panel. You can create custom filters based on a time range. Custom filters allow you to select particular dates and times for job start times, end times, and elapsed times. Custom filters also allow you to filter results based on multiple filter criteria.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the folder.

   The contents panel shows a list of objects contained in the folder.
3. Right-click the header of the table to add or remove columns.
4. Select **New Job Notification**, **New Operation Notification**, or **New Request Notification** to dynamically display new jobs, operations, or requests in the **Monitoring** tab.
5. Enter filter criteria to reduce the number of objects that appear in the contents panel.
6. Select the object in the contents panel to view details about the object in the details panel.

   The details panel shows more information about the object selected in the contents panel.
7. To view jobs that started around the same time as the selected job, click **Actions** > **View Context**.

   The selected job and other jobs that started around the same time appear in the **Working View** tab.
8. Click the **Close** button to close the **Working View** tab.

Configuring the Date and Time Custom Filter

You can apply a custom filter on a Start Time or End Time column in the contents panel of the **Monitoring** tab to filter results.

1. Select Custom as the filter option for the Start Time or End Time column.

   The **Custom Filter: Date and Time** dialog box appears.
2. Enter the date range using the specified date and time formats.
3. Click **OK**.

Configuring the Elapsed Time Custom Filter

You can apply a custom filter on an Elapsed Time column in the contents panel of the **Monitoring** tab to filter results.

1. Select Custom as the filter option for the Elapsed Time column.

   The **Custom Filter: Elapsed Time** dialog box appears.
2. Enter the time range.
3. Click **OK**.

Configuring the Multi-Select Custom Filter

You can apply a custom filter on columns in the contents panel of the Monitoring tab to filter results based on multiple selections.

1. Select Custom as the filter option for the column.

   The **Custom Filter: Multi-Select** dialog box appears.
2. Select one or more filters.
3. Click **OK**.

Monitoring an Object

You can monitor an object on the **Monitoring** tab. You can view information about the object, such as properties, run-time statistics, and run-time reports.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the object.

   The contents panel shows multiple views that display different information about the object. The views that appear are based on the type of object selected in the Navigator.
3. Select a view to show information about the object.
4. To add or remove reports from the **Reports** view, select **Actions** > **Reports**.

CHAPTER 32

Domain Reports

This chapter includes the following topics:

- Domain Reports Overview, 400
- License Management Report, 400
- Web Services Report, 407

Domain Reports Overview

You can run the following domain reports from the Reports tab in the Administrator tool:

- License Management Report. Monitors the number of software options purchased for a license and the number of times a license exceeds usage limits. The License Management Report displays the license usage information such as CPU and repository usage and the node configuration details.
- Web Services Report. Monitors activities of the web services running on a Web Services Hub. The Web Services Report displays run-time information such as the number of successful or failed requests and average service time. You can also view historical statistics for a specific period of time.

Note: If the master gateway node runs on a UNIX machine and the UNIX machine does not have a graphics display server, you must install X Virtual Frame Buffer on the UNIX machine to view the report charts in the License Report or the Web Services Report. If you have multiple gateway nodes running on UNIX machines, install X Virtual Frame Buffer on each UNIX machine.

License Management Report

You can monitor the list of software options purchased for a license and the number of times a license exceeds usage limits. The License Management Report displays the general properties, CPU and repository usage, user details, hardware and node configuration details, and the options purchased for each license.

You can save the License Management Report as a PDF on your local machine. You can also email a PDF version of the report to someone.

Run the License Management Report to monitor the following license usage information:

- Licensing details. Shows general properties for every license assigned in the domain.
- CPU usage. Shows the number of logical CPUs used to run application services in the domain. A logical CPU is a CPU thread. For example, if a CPU is dual-threaded, then it has two logical CPUs.

- Repository usage. Shows the number of PowerCenter Repository Services in the domain.
- User information. Shows information about users in the domain.
- Hardware configuration. Shows details about the machines used in the domain.

  Node configuration. Shows details about each node in the domain.
- Licensed options. Shows a list of PowerCenter and other Informatica options purchased for each license.

Licensing

The Licensing section of the License Management Report shows information about each license in the domain.

The following table describes the licensing information in the License Management Report:

Property	Description
Name	Name of the license.
Edition	PowerCenter edition.
Version	Version of Informatica platform.
Expiration Date	Date when the license expires.
Serial Number	Serial number of the license. The serial number identifies the customer or project. If the customer has multiple PowerCenter installations, there is a separate serial number for each project. The original and incremental keys for a license have the same serial number.
Deployment Level	Level of deployment. Values are Development and Production.
Operating System / BitMode	Operating system and bitmode for the license. Indicates whether the license is installed on a 32-bit or 64-bit operating system.
CPU	Maximum number of authorized CPUs.
Repository	Maximum number of authorized PowerCenter repositories.
AT Named Users	Maximum number of users who are assigned the License Access for Informatica Analyst privilege.
Product Bitmode	Bitmode of the server binaries that are installed. Values are 32-bit or 64-bit.

Related Topics:

- “License Properties” on page 364

CPU Summary

The CPU Summary section of the License Management Report shows the maximum number of logical CPUs used to run application services in the domain. Use the CPU summary information to determine if the CPU usage exceeded the license limits.

The following table describes the CPU summary information in the License Management Report:

Property	Description
Domain	Name of the domain on which the report runs.
Current Usage	Maximum number of CPUs used concurrently on the day the report runs.
Peak Usage	Maximum number of CPUs used concurrently during the last 12 months.
Peak Usage Date	Date when the maximum number of CPUs were used concurrently during the last 12 months.
Days Exceeded License Limit	Number of days that the CPU usage exceeded the license limits.

CPU Detail

The CPU Detail section of the License Management Report provides CPU usage information for each host in the domain. The CPU Detail section shows the maximum number of logical CPUs used each day in a selected time period.

The report counts the number of logical CPUs on each host that runs application services in the domain. The report groups logical CPU totals by node.

The following table describes the CPU detail information in the License Management Report:

Property	Description
Host Name	Host name of the machine.
Current Usage	Maximum number of CPUs used concurrently on the day the report runs.
Peak Usage	Maximum number of CPUs the host used concurrently during the last 12 months.
Peak Usage Date	Date in the last 12 months when the host concurrently used the maximum number of CPUs.
Assigned Licenses	Name of all licenses assigned to services that run on the node.

Repository Summary

The Repository Summary section of the License Management Report provides repository usage information for the domain. Use the repository summary information to determine if the repository usage exceeded the license limits.

The following table describes the repository summary information in the License Management Report:

Property	Description
Current Usage	Maximum number of repositories used concurrently in the domain on the day the report runs.
Peak Usage	Maximum number of repositories used concurrently in the domain during the last 12 months.

Property	Description
Peak Usage Date	Date in the last 12 months when the maximum number of repositories were used concurrently.
Days Exceeded License Limit	Number of days that the repository usage exceeded the license limits.

User Summary

The User Summary section of the License Management Report provides information about Analyst tool users in the domain.

The following table describes the user summary information in the License Management Report:

Property	Description
User Type	Type of user in the domain.
Current Named Users	Maximum number of users who are assigned the License Access for Informatica Analyst privilege on the day the report runs.
Peaked Name Users	Maximum number of users who are assigned the License Access for Informatica Analyst privilege during the last 12 months.
Peak Named Users Date	Date during the last 12 months when the maximum number of concurrent users were assigned the License Access for Informatica Analyst privilege.

User Detail

The User Detail section of the License Management Report provides information about each Analyst tool user in the domain.

The following table describes the user detail information in the License Management Report:

Property	Description
User Type	Type of user in the domain.
User Name	User name.
Days Logged In	Number of days the user logged in to the Analyst tool and performed profiling during the last 12 months.
Peak Unique IP Addresses in a Day	Maximum number of machines that the user was logged in to and performed profiling on during a single day of the last 12 months.
Average Unique IP Addresses	Daily average number of machines that the user was logged in to and running profiling on during the last 12 months.
Peak IP Address Date	Date when the user logged in to and performed profiling on the maximum number of machines during a single day of the last 12 months.

Property	Description
Peak Daily Sessions	Maximum number of times in a single day of the last 12 months that the user logged in to any Analyst tool and performed profiling.
Average Daily Sessions	Average number of times per day in the last 12 months that the user logged in to any Analyst tool and performed profiling.
Peak Session Date	Date in the last 12 months when the user had the most daily sessions in the Analyst tool.

Hardware Configuration

The Hardware Configuration section of the License Management Report provides details about machines used in the domain.

The following table describes the hardware configuration information in the License Management Report:

Property	Description
Host Name	Host name of the machine.
Logical CPUs	Number of logical CPUs used to run application services in the domain.
Cores	Number of cores used to run application services in the domain.
Sockets	Number of sockets on the machine.
CPU Model	Model of the CPU.
Hyperthreading Enabled	Indicates whether hyperthreading is enabled.
Virtual Machine	Indicates whether the machine is a virtual machine.

Node Configuration

The Node Configuration section of the License Management Report provides details about each node in the domain.

The following table describes the node configuration information in the License Management Report:

Property	Description
Node Name	Name of the node or nodes assigned to a machine for a license.
Host Name	Host name of the machine.
IP Address	IP address of the node.
Operating System	Operating system of the machine on which the node runs.
Status	Status of the node.

Property	Description
Gateway	Indicates whether the node is a gateway node.
Service Type	Type of the application service configured to run on the node.
Service Name	Name of the application service configured to run on the node.
Service Status	Status of the application service.
Assigned License	License assigned to the application service.

Licensed Options

The Licensed Options section of the License Management Report provides details about each option for every license assigned to the domain.

The following table describes the licensed option information in the License Management Report:

Property	Description
License Name	Name of the license.
Description	Name of the license option.
Status	Status of the license option.
Issued On	Date when the license option was issued.
Expires On	Date when the license option expires.

Running the License Management Report

Run the License Management Report from the **Reports** tab in the Administrator tool.

1. Click the **Reports** tab in the Administrator tool.
2. Click the **License Management Report** view.

   The License Management Report appears.
3. Click **Save** to save the License Management Report as a PDF.

   If a License Management Report contains multibyte characters, you must configure the Service Manager to use a Unicode font.
4. Click **Email** to send a copy of the License Management Report in an email.

   The **Send License Management Report** page appears.

Configuring a Unicode Font for the Report

Before you can save a License Management Report that contains multibyte characters, you must configure the Service Manager to use a Unicode font when generating the PDF file.

1. Install a Unicode font on the master gateway node.

2. Use a text editor to create a file named AcUtil.properties.
3. Add the following properties to the file:

```
PDF.Font.Default=Unicode_font_name
PDF.Font.MultibyteList=Unicode_font_name
```

Unicode_font_name is the name of the Unicode font installed on the master gateway node.

For example:

```
PDF.Font.Default=Arial Unicode MS
PDF.Font.MultibyteList=Arial Unicode MS
```

4. Save the AcUtil.properties file to the following location:

```
InformaticaInstallationDir\services\AdministratorConsole\administrator
```

5. Use a text editor to open the licenseUtility.css file in the following location:

```
InformaticaInstallationDir\services\AdministratorConsole\administrator\css
```

6. Append the Unicode font name to the value of each font-family property.

For example:

```
font-family: Arial Unicode MS, Verdana, Arial, Helvetica, sans-serif;
```

7. Restart Informatica services on each node in the domain.

Sending the License Management Report in an Email

You must configure the SMTP settings for the domain before you can send the License Management Report in an email.

The domain administrator can send the License Management Report in an email from Send License Management Report page in the Administrator tool.

1. Enter the following information:

Property	Description
To Email	Email address to which you send the License Management Report.
Subject	Subject of the email.
Customer Name	Name of the organization that purchased the license.
Request ID	Request ID that identifies the project for which the license was purchased.
Contact Name	Name of the contact person in the organization.
Contact Phone Number	Phone number of the contact person.
Contact Email	Email address of the contact person at the customer site.

2. Click OK.

The Administrator tool sends the License Management Report in an email.

Web Services Report

To analyze the performance of web services running on a Web Services Hub, you can run a report for the Web Services Hub or for a web service running on the Web Services Hub.

The Web Services Report provides run-time and historical information on the web service requests handled by the Web Services Hub. The report displays aggregated information for all web services in the Web Services Hub and information for each web service running on the Web Services Hub. The Web Services Report also provides historical information.

Understanding the Web Services Report

You can run the Web Services Report for a time interval that you choose. The Web Services Hub collects information on web services activities and caches 24 hours of information for use in the Web Services Report. It also writes the information to a history file.

Time Interval

By default, the Web Services Report displays activity information for a five-minute interval. You can select one of the following time intervals to display activity information for a web service or Web Services Hub:

- 5 seconds
- 1 minute
- 5 minutes
- 1 hour
- 24 hours

The Web Services Report displays activity information for the interval ending at the time you run the report. For example, if you run the Web Services Report at 8:05 a.m. for an interval of one hour, the Web Services Report displays the Web Services Hub activity from 7:05 a.m. and 8:05 a.m.

Caching

The Web Services Hub caches 24 hours of activity data. The cache is reinitialized every time the Web Services Hub is restarted. The Web Services Report displays statistics from the cache for the time interval that you run the report.

History File

The Web Services Hub writes the cached activity data to a history file. The Web Services Hub stores data in the history file for the number of days that you set in the MaxStatsHistory property of the Web Services Hub. For example, if the value of the MaxStatsHistory property is 5, the Web Services Hub keeps five days of data in the history file.

Contents of the Web Services Report

The Web Services Report displays information in different views and panels of the Informatica tool. The Web Services Hub report includes the following information:

- General Properties and Web Services Hub Summary. To view the general properties and summary information for the Web Services Hub, select the Properties view in the content panel. The Properties view displays the information.

- Web Services Historical Statistics. To view historical statistics for the web services in the Web Services Hub, select the Properties view in the content panel. The detail panel displays a table of historical statistic for the date that you specify.
- Web Services Run-Time Statistics. To view run-time statistics for each web service in the Web Services Hub, select the Web Services view in the content panel. The Web Services view lists the statistics for each web service.
- Web Service Properties. To view the properties of a web service, select the web service in the Web Services view of the content panel. In the details panel, the Properties view displays the properties for the web service.
- Web Service Top IP Addresses. To view the top IP addresses for a web service, select a web service in the Web Services view of the content panel and select the Top IP Addresses view in the details panel. The detail panel displays the most active IP addresses for the web service.
- Web Service Historical Statistics. To view a table of historical statistics for a web service, select a web service in the Web Services view of the content panel and select the Table view in the details panel. The detail panel displays a table of historical statistics for the web service.

General Properties and Web Services Hub Summary

To view the general properties and summary information for the Web Services Hub, select the Properties view in the content panel.

The following table describes the general properties:

Property	Description
Name	Name of the Web Services Hub.
Description	Short description of the Web Services Hub.
Service type	Type of Service. For a Web Services Hub, the service type is ServiceWSHubService.

The following table describes the Web Services Hub Summary properties:

Property	Description
# of Successful Message	Number of requests that the Web Services Hub processed successfully.
# of Fault Responses	Number of fault responses generated by web services in the Web Services Hub. The fault responses could be due to any error.
Total Messages	Total number of requests that the Web Services Hub received.
Last Server Restart Tme	Date and time when the Web Services Hub was last started.
Avg. # of Service Partitions	Average number of partitions allocated for all web services in the Web Services Hub.
% of Partitions in Use	Percentage of web service partitions that are in use for all web services in the Web Services Hub.
Avg. # of Run Instances	Average number of instances running for all web services in the Web Services Hub.

Web Services Historical Statistics

To view historical statistics for the web services in the Web Services Hub, select the Properties view in the content panel. The detail panel displays data from the Web Services Hub history file for the date that you specify.

The following table describes the historical statistics:

Property	Description
Time	Time of the event.
Web Service	Name of the web service for which the information is displayed. When you click the name of a web service, the Web Services Report displays the Service Statistics window.
Successful Requests	Number of requests successfully processed by the web service.
Fault Responses	Number of fault responses sent by the web service.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Max Service Time	The largest amount of time taken by the web service to process a request.
Min Service Time	The smallest amount of time taken by the web service to process a request.
Avg. DTM Time	Average number of seconds it takes the PowerCenter Integration Service to process the requests from the Web Services Hub.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Percent Partitions in Use	Percentage of partitions in use by the web service.
Avg Run Instances	Average number of instances running for the web service.

Web Services Run-time Statistics

To view run-time statistics for each web service in the Web Services Hub, select the Web Services view in the content panel. The Web Services view lists the statistics for each web service.

The report provides the following information for each web service for the selected time interval:

Property	Description
Service name	Name of the web service for which the information is displayed.
Successful Requests	Number of requests received by the web service that the Web Services Hub processed successfully.
Fault Responses	Number of fault responses generated by the web services in the Web Services Hub.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Avg. Run Instances	Average number of instances of the web service running during the interval.

Web Service Properties

To view the properties of a web service, select the web service in the Web Services view of the content panel. In the details panel, the Properties view displays the properties for the web service.

The report provides the following information for the selected web service:

Property	Description
# of Successful Requests	Number of requests received by the web service that the Web Services Hub processed successfully.
# of Fault Responses	Number of fault responses generated by the web services in the Web Services Hub.
Total Messages	Total number of requests that the Web Services Hub received.
Last Server Restart Time	Date and time when the Web Services Hub was last started
Last Service Time	Number of seconds it took to process the most recent service request
Average Service Time	Average time it takes to process a service request received by the web service.
Avg.# of Service Partitions	Average number of session partitions allocated for the web service.
Avg. # of Run Instances	Average number of instances of the web service running during the interval.

Web Service Top IP Addresses

To view the top IP addresses for a web service, select a web service in the Web Services view of the content panel and select the Top IP Addresses view in the details panel. The Top IP Addresses displays the most active IP addresses for the web service, listed in the order of longest to shortest service times.

The report provides the following information for each of the most active IP addresses:

Property	Description
Top 10 Client IP Addresses	The list of client IP addresses and the longest time taken by the web service to process a request from the client. The client IP addresses are listed in the order of longest to shortest service times. Use the *Click here* link to display the list of IP addresses and service times.

Web Service Historical Statistics Table

To view a table of historical statistics for a web service, select a web service in the Web Services view of the content panel and select the Table view in the details panel. The details panel displays a table of historical statistics for the web service.

The table provides the following information for the selected web service:

Property	Description
Time	Time of the event.
Web Service	Name of the web service for which the information is displayed.

Property	Description
Successful Requests	Number of requests successfully processed by the web service.
Fault Responses	Number of requests received for the web service that could not be processed and generated fault responses.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Min. Service Time	The smallest amount of time taken by the web service to process a request.
Max. Service Time	The largest amount of time taken by the web service to process a request.
Avg. DTM Time	Average time it takes the PowerCenter Integration Service to process the requests from the Web Services Hub.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Percent Partitions in Use	Percentage of partitions in use by the web service.
Avg. Run Instances	Average number of instances running for the web service.

Running the Web Services Report

Run the Web Services Report from the Reports tab in the Administrator tool.

Before you run the Web Services Report for a Web Services Hub, verify that the Web Services Hub is enabled. You cannot run the Web Services Report for a disabled Web Services Hub.

1. In the Administrator tool, click the Reports tab.
2. Click Web Services.
3. In the Navigator, select the Web Services Hub for which to run the report.

   In the content panel, the Properties view displays the properties of the Web Services Hub. The details view displays historical statistics for the services in the Web Services Hub.
4. To specify a date for historical statistics, click the date filter icon in the details panel, and select the date.
5. To view information about each service, select the Web Services view in the content panel.

   The Web Services view displays summary statistics for each service for the Web Services Hub.
6. To view additional information about a service, select the service from the list.

   In the details panel, the Properties view displays the properties for the service.
7. To view top IP addresses for the service, select the Top IP Addresses view in the details panel.
8. To view table attributes for the service, select the Table view in the detail panel.

Running the Web Services Report for a Secure Web Services Hub

To run a Web Services Hub on HTTPS, you must have an SSL certificate file for authentication of message transfers. When you create a Web Services Hub to run on HTTPS, you must specify the location of the keystore file that contains the certificate for the Web Services Hub. To run the Web Services Report in the Administrator tool for a secure Web Services Hub, you must import the SSL certificate into the Java certificate file. The Java certificate file is named *cacerts* and is located in the /lib/security directory of the Java directory. The Administrator tool uses the cacerts certificate file to determine whether to trust an SSL certificate.

In a domain that contains multiple nodes, the node where you generate the SSL certificate affects how you access the Web Services Report for a secure Web Services Hub.

Use the following rules and guidelines to run the Web Services Report for a secure Web Services Hub in a domain with multiple nodes:

- For each secure Web Services Hub running in a domain, generate an SSL certificate and import it to a Java certificate file.
- The Administrator tool searches for SSL certificates in the certificate file of a gateway node. The SSL certificate for a Web Services Hub running on worker node must be generated on a gateway node and imported into the certificate file of the same gateway node.
- To view the Web Services Report for a secure Web Services Hub, log in to the Administrator tool from the gateway node that has the certificate file containing the SSL certificate of the Web Services Hub for which you want to view reports.
- If a secure Web Services Hub runs on a worker node, the SSL certificate must be generated and imported into the certificate file of the gateway node. If a secure Web Services Hub runs on a gateway and a worker node, the SSL certificate of both nodes must be generated and imported into the certificate file of the gateway node. To view reports for the secure Web Services Hub, log in to the Administrator tool from the gateway node.
- If the domain has two gateway nodes and a secure Web Services Hub runs on each gateway node, access to the Web Services Reports depends on where the SSL certificate is located.

  For example, gateway node GWN01 runs Web Services Hub WSH01 and gateway node GWN02 runs Web Services Hub WSH02. You can view the reports for the Web Services Hubs based on the location of the SSL certificates:

  - If the SSL certificate for WSH01 is in the certificate file of GWN01 but not GWN02, you can view the reports for WSH01 if you log in to the Administrator tool through GWN01. You cannot view the reports for WSH01 if you log in to the Administrator tool through GWN02. If GWN01 fails, you cannot view reports for WSH01.
  - If the SSL certificate for WSH01 is in the certificate files of GWN01 and GWN02, you can view the reports for WSH01 if you log in to the Administrator tool through GWN01 or GWN02. If GWN01 fails, you can view the reports for WSH01 if you log in to the Administrator tool through GWN02.
- To ensure successful failover when a gateway node fails, generate and import the SSL certificates of all Web Services Hubs in the domain into the certificates files of all gateway nodes in the domain.

CHAPTER 33

Node Diagnostics

This chapter includes the following topics:

- Node Diagnostics Overview, 413
- Customer Support Portal Login, 414
- Generating Node Diagnostics, 415
- Downloading Node Diagnostics, 415
- Uploading Node Diagnostics, 416
- Analyzing Node Diagnostics, 417

Node Diagnostics Overview

The Configuration Support Manager is a web-based application that you can use to track Informatica updates and diagnose issues in your environment.

You can discover comprehensive information about your technical environment and diagnose issues before they become critical.

Generate node diagnostics from the Administrator tool and upload them to the Configuration Support Manager in the Informatica Customer Portal. Then, check the node diagnostics against business rules and recommendations in the Configuration Support Manager.

Complete the following tasks to generate and upload node diagnostics:

1. Log in to the Informatica Customer Portal.
2. Generate node diagnostics. The Service Manager analyzes the services of the node and generates node diagnostics including information such as operating system details, CPU details, database details, and patches.
3. Optionally, download node diagnostics to your local drive.
4. Upload node diagnostics to the Configuration Support Manager, a diagnostic web application outside the firewall. The Configuration Support Manager is a part of the Informatica Customer Portal. The Service Manager connects to the Configuration Support Manager through the HTTPS protocol and uploads the node diagnostics.
5. Review the node diagnostics in the Configuration Support Manager to find troubleshooting information for your environment.

Customer Support Portal Login

You must log in to the customer portal to upload node diagnostics to the Configuration Support Manager. The login credentials are not specific to a user. The same credentials are applicable for all users who have access to the Administrator tool. Register at http://communities.informatica.com if you do not have the customer portal login details. You need to enter the customer portal login details and, then save these details. Alternatively, you can enter the customer portal details each time you upload node diagnostics to the Configuration Support Manager. You can generate node diagnostics without entering the login details.

To maintain login security, you must log out of the Configuration Support Manager and the Node Diagnostics Upload page of the Administrator tool.

- To log out of the Configuration Support Manager, click the logout link.
- To log out of the Upload page, click **Close Window**.

Note: If you close these windows through the web browser close button, you remain logged in to the Configuration Support Manager. Other users can access the Configuration Support Manager without valid credentials.

Logging In to the Customer Support Portal

Before you generate and upload node diagnostics, you must log in to the customer support portal.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.

   A list of all the nodes in the domain appears.
4. Click **Edit Customer Portal Login Credentials**.

   The **Edit Customer Portal Login Credentials** dialog box appears.

   Note: You can also edit portal credentials from the **Actions** menu on the **Diagnostics** tab.
5. Enter the following customer portal login details:

Field	Description
Email Address	Email address with which you registered your customer portal account.
Password	Password for your customer portal account.
Project ID	Unique ID assigned to your support project.

6. Click **OK**.

Generating Node Diagnostics

When you generate node diagnostics, the Administrator tool generates node diagnostics in an XML file.

The XML file contains details about services, logs, environment variables, operating system parameters, system information, and database clients. Node diagnostics of worker nodes do not include domain metadata information but contain only node metadata information.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.

   A list of all nodes in the domain appears.
4. Select the node.
5. Click **Generate Diagnostics File**.
6. Click **Yes** to confirm that you want to generate node diagnostics.

   Note: You can also generate diagnostics from the **Actions** menu on the **Diagnostics** tab.

   The csmagent<host name>.xml file, which contains the node diagnostics, is generated at `INFA_HOME/server/csm/output`. The node diagnostics and the time stamp of the generated file appear.
7. To run diagnostics for your environment, upload the csmagent<host name>.xml file to the Configuration Support Manager.

   Alternatively, you can download the XML file to your local drive.

After you generate node diagnostics for the first time, you can regenerate or upload them.

Downloading Node Diagnostics

After you generate node diagnostics, you can download it to your local drive.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.

   A list of all nodes in the domain appears.
4. Click the diagnostics file name of the node.

   The file opens in another browser window.
5. Click **File** > **Save As**. Then, specify a location to save the file.
6. Click **Save**.

   The XML file is saved to your local drive.

Uploading Node Diagnostics

You can upload node diagnostics to the Configuration Support Manager through the Administrator tool. You must enter the customer portal login details before you upload node diagnostics.

When you upload node diagnostics, you can update or create a configuration in the Configuration Support Manager. Create a configuration the first time you upload the node diagnostics. Update a configuration to view the latest diagnostics of the configuration. To compare current and previous node configurations of an existing configuration, upload the current node diagnostics as a new configuration.

Note: If you do not have access to the Internet, you can download the file and upload it at a later time. You can also send the file to the Informatica Global Customer Support in an email to troubleshoot or to upload.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.

   A list of all nodes in the domain appears.
4. Select the node.
5. Generate node diagnostics.
6. Click **Upload Diagnostics File to CSM**.

   You can upload the node diagnostics as a new configuration or as an update to an existing configuration.
7. To upload a new configuration, go to step 10.

   To update a configuration, select **Update an existing configuration**.
8. Select the configuration you want to update from the list of configurations.
9. Go to step 12.
10. Select **Upload as a new configuration**.
11. Enter the following configuration details:

Field	Description
Name	Configuration name.
Description	Configuration description.
Type	Type of the node, which is one of the following types: - Production - Development - Test/QA

12. Click **Upload Now**.

    After you upload the node diagnostics, go to the Configuration Support Manager to analyze the node diagnostics.
13. Click **Close Window**.

    Note: If you close the window by using the close button in the browser, the user authentication session does not end and you cannot upload node diagnostics to the Configuration Support Manager with another set of customer portal login credentials.

Analyzing Node Diagnostics

Use the Configuration Support Manager to analyze node diagnostics.

Use the Configuration Support Manager to complete the following tasks:

- Diagnose issues before they become critical.
- Identify bug fixes.
- Identify recommendations that can reduce risk of unplanned outage.
- View details of your technical environment.
- Manage your configurations efficiently.
- Subscribe to proactive alerts through email and RSS.
- Run advanced diagnostics with compare configuration.

Identify Bug Fixes

You can use the Configuration Support Manager to resolve issues encountered during operations. To expedite resolution of support issues, you can generate and upload node diagnostics to the Configuration Support Manager. You can analyze node diagnostics in the Configuration Support Manager and find a solution to your issue.

For example, when you run a Sorter session that processes a large volume of data, you notice that there is some data loss. You generate node diagnostics and upload them to the Configuration Support Manager. When you review the diagnostics for bug fix alerts, you see that a bug fix, EBF178626, is available for this. You apply EBF178626, and run the session again. All data is successfully loaded.

Identify Recommendations

You can use the Configuration Support Manager to avoid issues in your environment. You can troubleshoot issues that arise after you make changes to the node properties by comparing different node diagnostics in the Configuration Support Manager. You can also use the Configuration Support Manager to identify recommendations or updates that may help you improve the performance of the node.

For example, you upgrade the node memory to handle a higher volume of data. You generate node diagnostics and upload them to the Configuration Support Manager. When you review the diagnostics for operating system warnings, you find the recommendation to increase the total swap memory of the node to twice that of the node memory for optimal performance. You increase swap space as suggested in the Configuration Support Manager and avoid performance degradation.

Tip: Regularly upload node diagnostics to the Configuration Support Manager and review node diagnostics to maintain your environment efficiently.

CHAPTER 34

Understanding Globalization

This chapter includes the following topics:

- Globalization Overview, 418
- Locales, 420
- Data Movement Modes, 421
- Code Page Overview, 423
- Code Page Compatibility, 424
- Code Page Validation, 431
- Relaxed Code Page Validation, 432
- PowerCenter Code Page Conversion, 433
- Case Study: Processing ISO 8859-1 Data, 434
- Case Study: Processing Unicode UTF-8 Data, 436

Globalization Overview

Informatica can process data in different languages. Some languages require single-byte data, while other languages require multibyte data. To process data correctly in Informatica, you must set up the following items:

- Locale. Informatica requires that the locale settings on machines that access Informatica applications are compatible with code pages in the domain. You may need to change the locale settings. The locale specifies the language, territory, encoding of character set, and collation order.
- Data movement mode. The PowerCenter Integration Service can process single-byte or multibyte data and write it to targets. Use the ASCII data movement mode to process single-byte data. Use the Unicode data movement mode for multibyte data.
- Code pages. Code pages contain the encoding to specify characters in a set of one or more languages. You select a code page based on the type of character data you want to process. To ensure accurate data movement, you must ensure compatibility among code pages for Informatica and environment components. You use code pages to distinguish between US-ASCII (7-bit ASCII), ISO 8859-1 (8-bit ASCII), and multibyte characters.

To ensure data passes accurately through your environment, the following components must work together:

- Domain configuration database code page
- Administrator tool locale settings and code page
- PowerCenter Integration Service data movement mode
- Code page for each PowerCenter Integration Service process

- PowerCenter Client code page
- PowerCenter repository code page
- Source and target database code pages
- Metadata Manager repository code page

You can configure the PowerCenter Integration Service for relaxed code page validation. Relaxed validation removes restrictions on source and target code pages.

Unicode

The Unicode Standard is the work of the Unicode Consortium, an international body that promotes the interchange of data in all languages. The Unicode Standard is designed to support any language, no matter how many bytes each character in that language may require. Currently, it supports all common languages and provides limited support for other less common languages. The Unicode Consortium is continually enhancing the Unicode Standard with new character encodings. For more information about the Unicode Standard, see http://www.unicode.org.

The Unicode Standard includes multiple character sets. Informatica uses the following Unicode standards:

- UCS-2 (Universal Character Set, double-byte). A character set in which each character uses two bytes.
- UTF-8 (Unicode Transformation Format). An encoding format in which each character can use between one to four bytes.
- UTF-16 (Unicode Transformation Format). An encoding format in which each character uses two or four bytes.
- UTF-32 (Unicode Transformation Format). An encoding format in which each character uses four bytes.
- GB18030. A Unicode encoding format defined by the Chinese government in which each character can use between one to four bytes.

Informatica is a Unicode application. The PowerCenter Client, PowerCenter Integration Service, and Data Integration Service use UCS-2 internally. The PowerCenter Client converts user input from any language to UCS-2 and converts it from UCS-2 before writing to the PowerCenter repository. The PowerCenter Integration Service and Data Integration Service converts source data to UCS-2 before processing and converts it from UCS-2 after processing. The PowerCenter repository, Model repository, PowerCenter Integration Service, and Data Integration Service support UTF-8. You can use Informatica to process data in any language.

Working with a Unicode PowerCenter Repository

The PowerCenter repository code page is the code page of the data in the PowerCenter repository. You choose the PowerCenter repository code page when you create or upgrade a PowerCenter repository. When the PowerCenter repository database code page is UTF-8, you can create a PowerCenter repository using the UTF-8 code page.

The domain configuration database uses the UTF-8 code page. If you need to store metadata in multiple languages, such as Chinese, Japanese, and Arabic, you must use the UTF-8 code page for all services in that domain.

The Service Manager synchronizes the list of users in the domain with the list of users and groups in each application service. If a user in the domain has characters that the code page of the application services does not recognize, characters do not convert correctly and inconsistencies occur.

Use the following guidelines when you use UTF-8 as the PowerCenter repository code page:

- The PowerCenter repository database code page must be UTF-8.
- The PowerCenter repository code page must be a superset of the PowerCenter Client and PowerCenter Integration Service process code pages.

- You can input any character in the UCS-2 character set. For example, you can store German, Chinese, and English metadata in a UTF-8 enabled PowerCenter repository.
- Install languages and fonts on the PowerCenter Client machine. If you are using a UTF-8 PowerCenter repository, you may want to enable the PowerCenter Client machines to display multiple languages. By default, the PowerCenter Clients display text in the language set in the system locale. Use the Regional Options tool in the Control Panel to add language groups to the PowerCenter Client machines.
- You can use the Windows Input Method Editor (IME) to enter multibyte characters from any language without having to run the version of Windows specific for that language.
- Choose a code page for a PowerCenter Integration Service process that can process all PowerCenter repository metadata correctly. The code page of the PowerCenter Integration Service process must be a subset of the PowerCenter repository code page. If the PowerCenter Integration Service has multiple service processes, ensure that the code pages for all PowerCenter Integration Service processes are subsets of the PowerCenter repository code page. If you are running the PowerCenter Integration Service process on Windows, the code page for the PowerCenter Integration Service process must be the same as the code page for the system or user locale. If you are running the PowerCenter Integration Service process on UNIX, use the UTF-8 code page for the PowerCenter Integration Service process.

Locales

Every machine has a locale. A locale is a set of preferences related to the user environment, including the input language, keyboard layout, how data is sorted, and the format for currency and dates. Informatica uses locale settings on each machine.

You can set the following locale settings on Windows:

- System locale. Determines the language, code pages, and associated bitmap font files that are used as defaults for the system.
- User locale. Determines the default formats to display date, time, currency, and number formats.
- Input locale. Describes the input method, such as the keyboard, of the system language.

For more information about configuring the locale settings on Windows, consult the Windows documentation.

System Locale

The system locale is also referred to as the system default locale. It determines which ANSI and OEM code pages, as well as bitmap font files, are used as defaults for the system. The system locale contains the language setting, which determines the language in which text appears in the user interface, including in dialog boxes and error messages. A message catalog file defines the language in which messages display. By default, the machine uses the language specified for the system locale for all processes, unless you override the language for a specific process.

The system locale is already set on your system and you may not need to change settings to run Informatica. If you do need to configure the system locale, you configure the locale on a Windows machine in the Regional Options dialog box. On UNIX, you specify the locale in the LANG environment variable.

User Locale

The user locale displays date, time, currency, and number formats for each user. You can specify different user locales on a single machine. Create a user locale if you are working with data on a machine that is in a different language than the operating system. For example, you might be an English user working in Hong Kong on a

Chinese operating system. You can set English as the user locale to use English standards in your work in Hong Kong. When you create a new user account, the machine uses a default user locale. You can change this default setting once the account is created.

Input Locale

An input locale specifies the keyboard layout of a particular language. You can set an input locale on a Windows machine to type characters of a specific language.

You can use the Windows Input Method Editor (IME) to enter multibyte characters from any language without having to run the version of Windows specific for that language. For example, if you are working on an English operating system and need to enter text in Chinese, you can use IME to set the input locale to Chinese without having to install the Chinese version of Windows. You might want to use an input method editor to enter multibyte characters into a PowerCenter repository that uses UTF-8.

Data Movement Modes

The data movement mode is a PowerCenter Integration Service option you choose based on the type of data you want to move, single-byte or multibyte data. The data movement mode you select depends the following factors:

- Requirements to store single-byte or multibyte metadata in the PowerCenter repository
- Requirements to access source data containing single-byte or multibyte character data
- Future needs for single-byte and multibyte data

The data movement mode affects how the PowerCenter Integration Service enforces session code page relationships and code page validation. It can also affect performance. Applications can process single-byte characters faster than multibyte characters.

Character Data Movement Modes

The PowerCenter Integration Service runs in the following modes:

- ASCII (American Standard Code for Information Interchange). The US-ASCII code page contains a set of 7-bit ASCII characters and is a subset of other character sets. When the PowerCenter Integration Service runs in ASCII data movement mode, each character requires one byte.
- Unicode. The universal character-encoding standard that supports all languages. When the PowerCenter Integration Service runs in Unicode data movement mode, it allots up to two bytes for each character. Run the PowerCenter Integration Service in Unicode mode when the source contains multibyte data.

  Tip: You can also use ASCII or Unicode data movement mode if the source has 8-bit ASCII data. The PowerCenter Integration Service allots an extra byte when processing data in Unicode data movement mode. To increase performance, use the ASCII data movement mode. For example, if the source contains characters from the ISO 8859-1 code page, use the ASCII data movement.

The data movement you choose affects the requirements for code pages. Ensure the code pages are compatible.

ASCII Data Movement Mode

In ASCII mode, the PowerCenter Integration Service processes single-byte characters and does not perform code page conversions. When you run the PowerCenter Integration Service in ASCII mode, it does not enforce session code page relationships.

Unicode Data Movement Mode

In Unicode mode, the PowerCenter Integration Service recognizes multibyte character data and allocates up to two bytes for every character. The PowerCenter Integration Service performs code page conversions from sources to targets. When you set the PowerCenter Integration Service to Unicode data movement mode, it uses a Unicode character set to process characters in a specified code page, such as Shift-JIS or UTF-8.

When you run the PowerCenter Integration Service in Unicode mode, it enforces session code page relationships.

Changing Data Movement Modes

You can change the data movement mode in the PowerCenter Integration Service properties in the Administrator tool. After you change the data movement mode, the PowerCenter Integration Service runs in the new data movement mode the next time you start the PowerCenter Integration Service. When the data movement mode changes, the PowerCenter Integration Service handles character data differently. To avoid creating data inconsistencies in your target tables, the PowerCenter Integration Service performs additional checks for sessions that reuse session caches and files.

The following table describes how the PowerCenter Integration Service handles session files and caches after you change the data movement mode:

Session File or Cache	Time of Creation or Use	PowerCenter Integration Service Behavior After Data Movement Mode Change
Session Log File (*.log)	Each session.	No change in behavior. Creates a new session log for each session using the code page of the PowerCenter Integration Service process.
Workflow Log	Each workflow.	No change in behavior. Creates a new workflow log file for each workflow using the code page of the PowerCenter Integration Service process.
Reject File (*.bad)	Each session.	No change in behavior. Appends rejected data to the existing reject file using the code page of the PowerCenter Integration Service process.
Output File (*.out)	Sessions writing to flat file.	No change in behavior. Creates a new output file for each session using the target code page.
Indicator File (*.in)	Sessions writing to flat file.	No change in behavior. Creates a new indicator file for each session.
Incremental Aggregation Files (*.idx, *.dat)	Sessions with Incremental Aggregation enabled.	When files are removed or deleted, the PowerCenter Integration Service creates new files. When files are not moved or deleted, the PowerCenter Integration Service fails the session with the following error message: `SM_7038 Aggregate Error: ServerMode: [server data movement mode] and CachedMode: [data movement mode that created the files] mismatch.` Move or delete files created using a different code page.
Unnamed Persistent Lookup Files (*.idx, *.dat)	Sessions with a Lookup transformation configured for	Rebuilds the persistent lookup cache.

Session File or Cache	Time of Creation or Use	PowerCenter Integration Service Behavior After Data Movement Mode Change
	an unnamed persistent lookup cache.	
Named Persistent Lookup Files (*.idx, *.dat)	Sessions with a Lookup transformation configured for a named persistent lookup cache.	When files are removed or deleted, the PowerCenter Integration Service creates new files. When files are not moved or deleted, the PowerCenter Integration Service fails the session. Move or delete files created using a different code page.

Code Page Overview

A code page contains the encoding to specify characters in a set of one or more languages. An encoding is the assignment of a number to a character in the character set. You use code pages to identify data that might be in different languages. For example, if you create a mapping to process Japanese data, you must select a Japanese code page for the source data.

When you choose a code page, the program or application for which you set the code page refers to a specific set of data that describes the characters the application recognizes. This influences the way that application stores, receives, and sends character data.

Most machines use one of the following code pages:

- US-ASCII (7-bit ASCII)
- MS Latin1 (MS 1252) for Windows operating systems
- Latin1 (ISO 8859-1) for UNIX operating systems
- IBM EBCDIC US English (IBM037) for mainframe systems

The US-ASCII code page contains all 7-bit ASCII characters and is the most basic of all code pages with support for United States English. The US-ASCII code page is not compatible with any other code page. When you install either the PowerCenter Client, PowerCenter Integration Service, or PowerCenter repository on a US-ASCII system, you must install all components on US-ASCII systems and run the PowerCenter Integration Service in ASCII mode.

MS Latin1 and Latin1 both support English and most Western European languages and are compatible with each other. When you install the PowerCenter Client, PowerCenter Integration Service, or PowerCenter repository on a system using one of these code pages, you can install the rest of the components on any machine using the MS Latin1 or Latin1 code pages.

You can use the IBM EBCDIC code page for the PowerCenter Integration Service process when you install it on a mainframe system. You cannot install the PowerCenter Client or PowerCenter repository on mainframe systems, so you cannot use the IBM EBCDIC code page for PowerCenter Client or PowerCenter repository installations.

UNIX Code Pages

In the United States, most UNIX operating systems have more than one code page installed and use the ASCII code page by default. If you want to run PowerCenter in an ASCII-only environment, you can use the ASCII code page and run the PowerCenter Integration Service in ASCII mode.

UNIX systems allow you to change the code page by changing the LANG, LC_CTYPE or LC_ALL environment variable. For example, you want to change the code page an HP-UX machine uses. Use the following command in the C shell to view your environment:

```
locale
```

This results in the following output, in which “C” implies “ASCII”:

```
LANG="C"
LC_CTYPE="C"
LC_NUMERIC="C"
LC_TIME="C"
LC_ALL="C"
```

To change the language to English and require the system to use the Latin1 code page, you can use the following command:

```
setenv LANG en_US.iso88591
```

When you check the locale again, it has been changed to use Latin1 (ISO 8859-1):

```
LANG="en_US.iso88591"
LC_CTYPE="en_US.iso88591"
LC_NUMERIC="en_US.iso88591"
LC_TIME="en_US.iso88591"
LC_ALL="en_US.iso88591"
```

For more information about changing the locale or code page of a UNIX system, see the UNIX documentation.

Windows Code Pages

The Windows operating system is based on Unicode, but does not display the code page used by the operating system in the environment settings. However, you can make an educated guess based on the country in which you purchased the system and the language the system uses.

If you purchase Windows in the United States and use English as an input and display language, your operating system code page is MS Latin1 (MS1252) by default. However, if you install additional display or input languages from the Windows installation CD and use those languages, the operating system might use a different code page.

For more information about the default code page for your Windows system, contact Microsoft.

Choosing a Code Page

Choose code pages based on the character data you use in mappings. Character data can be represented by character modes based on the character size. Character size is the storage space a character requires in the database. Different character sizes can be defined as follows:

- Single-byte. A character represented as a unique number between 0 and 255. One byte is eight bits. ASCII characters are single-byte characters.
- Double-byte. A character two bytes or 16 bits in size represented as a unique number 256 or greater. Many Asian languages, such as Chinese, have double-byte characters.
- Multibyte. A character two or more bytes in size is represented as a unique number 256 or greater. Many Asian languages, such as Chinese, have multibyte characters.

Code Page Compatibility

Compatibility between code pages is essential for accurate data movement when the PowerCenter Integration Service runs in the Unicode data movement mode.

A code page can be compatible with another code page, or it can be a subset or a superset of another:

- Compatible. Two code pages are compatible when the characters encoded in the two code pages are virtually identical. For example, JapanEUC and JIPSE code pages contain identical characters and are compatible with each other. The PowerCenter repository and PowerCenter Integration Service process can each use one of these code pages and can pass data back and forth without data loss.
- Superset. A code page is a superset of another code page when it contains all the characters encoded in the other code page and additional characters not encoded in the other code page. For example, MS Latin1 is a superset of US-ASCII because it contains all characters in the US-ASCII code page.

  Note: Informatica considers a code page to be a superset of itself and all other compatible code pages.
- Subset. A code page is a subset of another code page when all characters in the code page are also encoded in the other code page. For example, US-ASCII is a subset of MS Latin1 because all characters in the US-ASCII code page are also encoded in the MS Latin1 code page.

For accurate data movement, the target code page must be a superset of the source code page. If the target code page is not a superset of the source code page, the PowerCenter Integration Service may not process all characters, resulting in incorrect or missing data. For example, Latin1 is a superset of US-ASCII. If you select Latin1 as the source code page and US-ASCII as the target code page, you might lose character data if the source contains characters that are not included in US-ASCII.

When you install or upgrade a PowerCenter Integration Service to run in Unicode mode, you must ensure code page compatibility among the domain configuration database, the Administrator tool, PowerCenter Clients, PowerCenter Integration Service process nodes, the PowerCenter repository, the Metadata Manager repository, and the machines hosting *pmrep* and *pmcmd*. In Unicode mode, the PowerCenter Integration Service enforces code page compatibility between the PowerCenter Client and the PowerCenter repository, and between the PowerCenter Integration Service process and the PowerCenter repository. In addition, when you run the PowerCenter Integration Service in Unicode mode, code pages associated with sessions must have the appropriate relationships:

- For each source in the session, the source code page must be a subset of the target code page. The PowerCenter Integration Service does not require code page compatibility between the source and the PowerCenter Integration Service process or between the PowerCenter Integration Service process and the target.
- If the session contains a Lookup or Stored Procedure transformation, the database or file code page must be a subset of the target that receives data from the Lookup or Stored Procedure transformation and a superset of the source that provides data to the Lookup or Stored Procedure transformation.
- If the session contains an External Procedure or Custom transformation, the procedure must pass data in a code page that is a subset of the target code page for targets that receive data from the External Procedure or Custom transformation.

Informatica uses code pages for the following components:

- Domain configuration database. The domain configuration database must be compatible with the code pages of the PowerCenter repository and Metadata Manager repository.
- Administrator tool. You can enter data in any language in the Administrator tool.
- PowerCenter Client. You can enter metadata in any language in the PowerCenter Client.
- PowerCenter Integration Service process. The PowerCenter Integration Service can move data in ASCII mode and Unicode mode. The default data movement mode is ASCII, which passes 7-bit ASCII or 8-bit ASCII character data. To pass multibyte character data from sources to targets, use the Unicode data movement mode. When you run the PowerCenter Integration Service in Unicode mode, it uses up to three bytes for each character to move data and performs additional checks at the session level to ensure data integrity.
- PowerCenter repository. The PowerCenter repository can store data in any language. You can use the UTF-8 code page for the PowerCenter repository to store multibyte data in the PowerCenter repository. The code page for the PowerCenter repository is the same as the database code page.

- Metadata Manager repository. The Metadata Manager repository can store data in any language. You can use the UTF-8 code page for the Metadata Manager repository to store multibyte data in the repository. The code page for the repository is the same as the database code page.
- Sources and targets. The sources and targets store data in one or more languages. You use code pages to specify the type of characters in the sources and targets.
- PowerCenter command line programs. You must also ensure that the code page for *pmrep* is a subset of the PowerCenter repository code page and the code page for *pmcmd* is a subset of the PowerCenter Integration Service process code page.

Most database servers use two code pages, a client code page to receive data from client applications and a server code page to store the data. When the database server is running, it converts data between the two code pages if they are different. In this type of database configuration, the PowerCenter Integration Service process interacts with the database client code page. Thus, code pages used by the PowerCenter Integration Service process, such as the PowerCenter repository, source, or target code pages, must be identical to the database client code page. The database client code page is usually identical to the operating system code page on which the PowerCenter Integration Service process runs. The database client code page is a subset of the database server code page.

For more information about specific database client and server code pages, see your database documentation.

Note: The Reporting Service does not require that you specify a code page for the data that is stored in the Data Analyzer repository. The Administrator tool writes domain, user, and group information to the Reporting Service. However, DataDirect drivers perform the required data conversions.

Domain Configuration Database Code Page

The domain configuration database must be compatible with the code pages of the PowerCenter repository, Metadata Manager repository, and Model repository.

The Service Manager synchronizes the list of users in the domain with the list of users and groups in each application service. If a user name in the domain has characters that the code page of the application service does not recognize, characters do not convert correctly and inconsistencies occur.

Administrator Tool Code Page

The Administrator tool can run on any node in a Informatica domain. The Administrator tool code page is the code page of the operating system of the node. Each node in the domain must use the same code page.

The Administrator tool code page must be:

- A subset of the PowerCenter repository code page
- A subset of the Metadata Manager repository code page
- A subset of the Model Repository code page

PowerCenter Client Code Page

The PowerCenter Client code page is the code page of the operating system of the PowerCenter Client. To communicate with the PowerCenter repository, the PowerCenter Client code page must be a subset of the PowerCenter repository code page.

PowerCenter Integration Service Process Code Page

The code page of a PowerCenter Integration Service process is the code page of the node that runs the PowerCenter Integration Service process. Define the code page for each PowerCenter Integration Service process in the Administrator tool on the Processes tab.

However, on UNIX, you can change the code page of the PowerCenter Integration Service process by changing the LANG, LC_CTYPE or LC_ALL environment variable for the user that starts the process.

The code page of the PowerCenter Integration Service process must be:

- A subset of the PowerCenter repository code page
- A superset of the machine hosting *pmcmd* or a superset of the code page specified in the INFA_CODEPAGENAME environment variable

The code pages of all PowerCenter Integration Service processes must be compatible with each other. For example, you can use MS Windows Latin1 for a node on Windows and ISO-8859-1 for a node on UNIX.

PowerCenter Integration Services configured for Unicode mode validate code pages when you start a session to ensure accurate data movement. It uses session code pages to convert character data. When the PowerCenter Integration Service runs in ASCII mode, it does not validate session code pages. It reads all character data as ASCII characters and does not perform code page conversions.

Each code page has associated sort orders. When you configure a session, you can select one of the sort orders associated with the code page of the PowerCenter Integration Service process. When you run the PowerCenter Integration Service in Unicode mode, it uses the selected session sort order to sort character data. When you run the PowerCenter Integration Service in ASCII mode, it sorts all character data using a binary sort order.

If you run the PowerCenter Integration Service in the United States on Windows, consider using MS Windows Latin1 (ANSI) as the code page of the PowerCenter Integration Service process.

If you run the PowerCenter Integration Service in the United States on UNIX, consider using ISO 8859-1 as the code page for the PowerCenter Integration Service process.

If you use *pmcmd* to communicate with the PowerCenter Integration Service, the code page of the operating system hosting *pmcmd* must be identical to the code page of the PowerCenter Integration Service process.

The PowerCenter Integration Service generates the names of session log files, reject files, caches and cache files, and performance detail files based on the code page of the PowerCenter Integration Service process.

PowerCenter Repository Code Page

The PowerCenter repository code page is the code page of the data in the repository. The PowerCenter Repository Service uses the PowerCenter repository code page to save metadata in and retrieve metadata from the PowerCenter repository database. Choose the PowerCenter repository code page when you create or upgrade a PowerCenter repository. When the PowerCenter repository database code page is UTF-8, you can create a PowerCenter repository using UTF-8 as its code page.

The PowerCenter repository code page must be:

- Compatible with the domain configuration database code page
- A superset of the the Administrator tool code page
- A superset of the PowerCenter Client code page
- A superset of the code page for the PowerCenter Integration Service process
- A superset of the machine hosting *pmrep* or a superset of the code page specified in the INFA_CODEPAGENAME environment variable

A global PowerCenter repository code page must be a subset of the local PowerCenter repository code page if you want to create shortcuts in the local PowerCenter repository that reference an object in a global PowerCenter repository.

If you copy objects from one PowerCenter repository to another PowerCenter repository, the code page for the target PowerCenter repository must be a superset of the code page for the source PowerCenter repository.

Metadata Manager Repository Code Page

The Metadata Manager repository code page is the code page of the data in the repository. The Metadata Manager Service uses the Metadata Manager repository code page to save metadata to and retrieve metadata from the repository database. The Administrator tool writes user and group information to the Metadata Manager Service. The Administrator tool also writes domain information in the repository database. The PowerCenter Integration Service process writes metadata to the repository database. Choose the repository code page when you create or upgrade a Metadata Manager repository. When the repository database code page is UTF-8, you can create a repository using UTF-8 as its code page.

The Metadata Manager repository code page must be:

- Compatible with the domain configuration database code page
- A superset of the Administrator tool code page
- A subset of the PowerCenter repository code page
- A superset of the code page for the PowerCenter Integration Service process

PowerCenter Source Code Page

The source code page depends on the type of source:

- Flat files and VSAM files. The code page of the data in the file. When you configure the flat file or COBOL source definition, choose a code page that matches the code page of the data in the file.
- XML files. The PowerCenter Integration Service converts XML to Unicode when it parses an XML source. When you create an XML source definition, the PowerCenter Designer assigns a default code page. You cannot change the code page.
- Relational databases. The code page of the database client. When you configure the relational connection in the PowerCenter Workflow Manager, choose a code page that is compatible with the code page of the database client. If you set a database environment variable to specify the language for the database, ensure the code page for the connection is compatible with the language set for the variable. For example, if you set the NLS_LANG environment variable for an Oracle database, ensure that the code page of the Oracle connection is identical to the value set in the NLS_LANG variable. If you do not use compatible code pages, sessions may hang, data may become inconsistent, or you might receive a database error, such as:

  ```
  ORA-00911: Invalid character specified.
  ```

Regardless of the type of source, the source code page must be a subset of the code page of transformations and targets that receive data from the source. The source code page does not need to be a subset of transformations or targets that do not receive data from the source.

Note: Select IBM EBCDIC as the source database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.

PowerCenter Target Code Page

The target code page depends on the type of target:

- Flat files. When you configure the flat file target definition, choose a code page that matches the code page of the data in the flat file.

- XML files. Configure the XML target code page after you create the XML target definition. The XML Wizard assigns a default code page to the XML target. The PowerCenter Designer does not apply the code page that appears in the XML schema.
- Relational databases. When you configure the relational connection in the PowerCenter Workflow Manager, choose a code page that is compatible with the code page of the database client. If you set a database environment variable to specify the language for the database, ensure the code page for the connection is compatible with the language set for the variable. For example, if you set the NLS_LANG environment variable for an Oracle database, ensure that the code page of the Oracle connection is compatible with the value set in the NLS_LANG variable. If you do not use compatible code pages, sessions may hang or you might receive a database error, such as:

```
ORA-00911: Invalid character specified.
```

The target code page must be a superset of the code page of transformations and sources that provide data to the target. The target code page does not need to be a superset of transformations or sources that do not provide data to the target.

The PowerCenter Integration Service creates session indicator files, session output files, and external loader control and data files using the target flat file code page.

Note: Select IBM EBCDIC as the target database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.

Command Line Program Code Pages

The *pmcmd* and *pmrep* command line programs require code page compatibility. *pmcmd* and *pmrep* use code pages when sending commands in Unicode. Other command line programs do not require code pages.

The code page compatibility for *pmcmd* and *pmrep* depends on whether you configured the code page environment variable INFA_CODEPAGENAME for *pmcmd* or *pmrep*. You can set this variable for either command line program or for both.

If you did not set this variable for a command line program, ensure the following requirements are met:

- If you did not set the variable for *pmcmd*, then the code page of the machine hosting *pmcmd* must be a subset of the code page for the PowerCenter Integration Service process.
- If you did not set the variable for *pmrep*, then the code page of the machine hosting *pmrep* must be a subset of the PowerCenter repository code page.

If you set the code page environment variable INFA_CODEPAGENAME for *pmcmd* or *pmrep*, ensure the following requirements are met:

- If you set INFA_CODEPAGENAME for *pmcmd,* the code page defined for the variable must be a subset of the code page for the PowerCenter Integration Service process.
- If you set INFA_CODEPAGENAME for *pmrep*, the code page defined for the variable must be a subset of the PowerCenter repository code page.
- If you run *pmcmd and pmrep* from the same machine and you set the INFA_CODEPAGENAME variable, the code page defined for the variable must be subsets of the code pages for the PowerCenter Integration Service process and the PowerCenter repository.

If the code pages are not compatible, the PowerCenter Integration Service process may not fetch the workflow, session, or task from the PowerCenter repository.

Code Page Compatibility Summary

The following table summarizes code page compatibility between sources, targets, repositories, the Administrator tool, PowerCenter Client, and PowerCenter Integration Service process:

Component Code Page	Code Page Compatibility
Source (including relational, flat file, and XML file)	Subset of target. Subset of lookup data. Subset of stored procedures. Subset of External Procedure or Custom transformation procedure code page.
Target (including relational, XML files, and flat files)	Superset of source. Superset of lookup data. Superset of stored procedures. Superset of External Procedure or Custom transformation procedure code page. PowerCenter Integration Service process creates external loader data and control files using the target flat file code page.
Lookup and stored procedure database	Subset of target. Superset of source.
External Procedure and Custom transformation procedures	Subset of target. Superset of source.
Domain Configuration Database	Compatible with the PowerCenter repository. Compatible with the Metadata Manager repository.
PowerCenter Integration Service process	Compatible with its operating system. Subset of the PowerCenter repository. Subset of the Metadata Manager repository. Superset of the machine hosting *pmcmd*. Identical to other nodes running the PowerCenter Integration Service processes.
PowerCenter repository	Compatible with the domain configuration database. Superset of PowerCenter Client. Superset of the nodes running the PowerCenter Integration Service process. Superset of the Metadata Manager repository. A global PowerCenter repository code page must be a subset of a local PowerCenter repository.
PowerCenter Client	Subset of the PowerCenter repository.
Machine running *pmcmd*	Subset of the PowerCenter Integration Service process.
Machine running *pmrep*	Subset of the PowerCenter repository.
Administrator Tool	Subset of the PowerCenter repository. Subset of the Metadata Manager repository.
Metadata Manager repository	Compatible with the domain configuration database. Subset of the PowerCenter repository. Superset of the Administrator tool. Superset of the PowerCenter Integration Service process.

Code Page Validation

The machines hosting the PowerCenter Client, PowerCenter Integration Service process, and PowerCenter repository database must use appropriate code pages. This eliminates the risk of data or repository inconsistencies. When the PowerCenter Integration Service runs in Unicode data movement mode, it enforces session code page relationships. When the PowerCenter Integration Service runs in ASCII mode, it does not enforce session code page relationships.

To ensure compatibility, the PowerCenter Client and PowerCenter Integration Service perform the following code page validations:

- PowerCenter restricts the use of EBCDIC-based code pages for repositories. Since you cannot install the PowerCenter Client or PowerCenter repository on mainframe systems, you cannot select EBCDIC-based code pages, like IBM EBCDIC, as the PowerCenter repository code page.
- PowerCenter Client can connect to the PowerCenter repository when its code page is a subset of the PowerCenter repository code page. If the PowerCenter Client code page is not a subset of the PowerCenter repository code page, the PowerCenter Client fails to connect to the PowerCenter repository code page with the following error:

  ```
  REP_61082 <PowerCenter Client>'s code page <PowerCenter Client code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
  ```

- After you set the PowerCenter repository code page, you cannot change it. After you create or upgrade a PowerCenter repository, you cannot change the PowerCenter repository code page. This prevents data loss and inconsistencies in the PowerCenter repository.
- The PowerCenter Integration Service process can start if its code page is a subset of the PowerCenter repository code page. The code page of the PowerCenter Integration Service process must be a subset of the PowerCenter repository code page to prevent data loss or inconsistencies. If it is not a subset of the PowerCenter repository code page, the PowerCenter Integration Service writes the following message to the log files:

  ```
  REP_61082 <PowerCenter Integration Service>'s code page <PowerCenter Integration Service code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
  ```

- When in Unicode data movement mode, the PowerCenter Integration Service starts workflows with the appropriate source and target code page relationships for each session. When the PowerCenter Integration Service runs in Unicode mode, the code page for every source in a session must be a subset of the target code page. This prevents data loss during a session.

  If the source and target code pages do not have the appropriate relationships with each other, the PowerCenter Integration Service fails the session and writes the following message to the session log:

  ```
  TM_6227 Error: Code page incompatible in session <session name>. <Additional details>.
  ```

- The PowerCenter Workflow Manager validates source, target, lookup, and stored procedure code page relationships for each session. The PowerCenter Workflow Manager checks code page relationships when you save a session, regardless of the PowerCenter Integration Service data movement mode. If you configure a session with invalid source, target, lookup, or stored procedure code page relationships, the PowerCenter Workflow Manager issues a warning similar to the following when you save the session:

  ```
  CMN_1933 Code page <code page name> for data from file or connection associated with transformation <name of source, target, or transformation> needs to be one-way compatible with code page <code page name> for transformation <source or target or transformation name>.
  ```

  If you want to run the session in ASCII mode, you can save the session as configured. If you want to run the session in Unicode mode, edit the session to use appropriate code pages.

Relaxed Code Page Validation

Your environment may require you to process data from different sources using character sets from different languages. For example, you may need to process data from English and Japanese sources using the same PowerCenter repository, or you may want to extract source data encoded in a Unicode encoding such as UTF-8. You can configure the PowerCenter Integration Service for relaxed code page validation. Relaxed code page validation enables you to process data using sources and targets with incompatible code pages.

Although relaxed code page validation removes source and target code page restrictions, it still enforces code page compatibility between the PowerCenter Integration Service and PowerCenter repository.

Note: Relaxed code page validation does not safeguard against possible data inconsistencies when you move data between incompatible code pages. You must verify that the characters the PowerCenter Integration Service reads from the source are included in the target code page.

Informatica removes the following restrictions when you relax code page validation:

- Source and target code pages. You can use any code page supported by Informatica for your source and target data.
- Session sort order. You can use any sort order supported by Informatica when you configure a session.

When you run a session with relaxed code page validation, the PowerCenter Integration Service writes the following message to the session log:

```
TM_6185 WARNING! Data code page validation is disabled in this session.
```

When you relax code page validation, the PowerCenter Integration Service writes descriptions of the database connection code pages to the session log.

The following text shows sample code page messages in the session log:

```
TM_6187 Repository code page: [MS Windows Latin 1 (ANSI), superset of Latin 1]
WRT_8222 Target file [$PMTargetFileDir\passthru.out] code page: [MS Windows Traditional Chinese,
superset of Big 5]
WRT_8221 Target database connection [Japanese Oracle] code page: [MS Windows Japanese, superset of
Shift-JIS]
TM_6189 Source database connection [Japanese Oracle] code page: [MS Windows Japanese, superset of Shift-
JIS]
CMN_1716 Lookup [LKP_sjis_lookup] uses database connection [Japanese Oracle] in code page [MS Windows
Japanese, superset of Shift-JIS]
CMN_1717 Stored procedure [J_SP_INCREMENT] uses database connection [Japanese Oracle] in code page [MS
Windows Japanese, superset of Shift-JIS]
```

If the PowerCenter Integration Service cannot correctly convert data, it writes an error message to the session log.

Configuring the PowerCenter Integration Service

To configure the PowerCenter Integration Service for code page relaxation, complete the following tasks in the Administrator tool:

- Disable code page validation. Disable the ValidateDataCodePages option in the PowerCenter Integration Service properties.
- Configure the PowerCenter Integration Service for Unicode data movement mode. Select Unicode for the Data Movement Mode option in the PowerCenter Integration Service properties.
- Configure the PowerCenter Integration Service to write to the logs using the UTF-8 character set. If you configure sessions or workflows to write to log files, enable the LogsInUTF8 option in the PowerCenter Integration Service properties. The PowerCenter Integration Service writes all logs in UTF-8 when you enable the LogsInUTF8 option. The PowerCenter Integration Service writes to the Log Manager in UTF-8 by default.

Selecting Compatible Source and Target Code Pages

Although PowerCenter allows you to use any supported code page, there are risks associated with using incompatible code pages for sources and targets. If your target code page is not a superset of your source code page, you risk inconsistencies in the target data because the source data may contain characters not encoded in the target code page.

When the PowerCenter Integration Service reads characters that are not included in the target code page, you risk transformation errors, inconsistent data, or failed sessions.

Note: If you relax code page validation, it is your responsibility to ensure that data converts from the source to target properly.

Troubleshooting for Code Page Relaxation

The PowerCenter Integration Service failed a session and wrote the following message to the session log:

```
TM_6188 The specified sort order is incompatible with the PowerCenter Integration Service code page.
```

If you want to validate code pages, select a sort order compatible with the PowerCenter Integration Service code page. If you want to relax code page validation, configure the PowerCenter Integration Service to relax code page validation in Unicode data movement mode.

I tried to view the session or workflow log, but it contains garbage characters.

The PowerCenter Integration Service is not configured to write session or workflow logs using the UTF-8 character set.

Enable the LogsInUTF8 option in the PowerCenter Integration Service properties.

PowerCenter Code Page Conversion

When in data movement mode is set to Unicode, the PowerCenter Client accepts input in any language and converts it to UCS-2. The PowerCenter Integration Service converts source data to UCS-2 before processing and converts the processed data from UCS-2 to the target code page before loading.

When you run a session, the PowerCenter Integration Service converts source, target, and lookup queries from the PowerCenter repository code page to the source, target, or lookup code page. The PowerCenter Integration Service also converts the name and call text of stored procedures from the PowerCenter repository code page to the stored procedure database code page.

At run time, the PowerCenter Integration Service verifies that it can convert the following queries and procedure text from the PowerCenter repository code page without data loss:

- Source query. Must convert to source database code page.
- Lookup query. Must convert to lookup database code page.
- Target SQL query. Must convert to target database code page.
- Name and call text of stored procedures. Must convert to stored procedure database code page.

Choosing Characters for PowerCenter Repository Metadata

You can use any character in the PowerCenter repository code page when inputting PowerCenter repository metadata. If the PowerCenter repository uses UTF-8, you can input any Unicode character. For example, you can store German, Japanese, and English metadata in a UTF-8 enabled PowerCenter repository. However, you must ensure that the PowerCenter Integration Service can successfully perform SQL transactions with source, target, lookup, and stored procedure databases. You must also ensure that the PowerCenter Integration Service can read from source and lookup files and write to target and lookup files. Therefore, when you run a session, you must ensure that the PowerCenter repository metadata characters are encoded in the source, target, lookup, and stored procedure code pages.

Example

The PowerCenter Integration Service, PowerCenter repository, and PowerCenter Client use the ISO 8859-1 Latin1 code page, and the source database contains Japanese data encoded using the Shift-JIS code page. Each code page contains characters not encoded in the other. Using characters other than 7-bit ASCII for the PowerCenter repository and source database metadata can cause the sessions to fail or load no rows to the target in the following situations:

- You create a mapping that contains a string literal with characters specific to the German language range of ISO 8859-1 in a query. The source database may reject the query or return inconsistent results.
- You use the PowerCenter Client to generate SQL queries containing characters specific to the German language range of ISO 8859-1. The source database cannot convert the German-specific characters from the ISO 8859-1 code page into the Shift-JIS code page.
- The source database has a table name that contains Japanese characters. The PowerCenter Designer cannot convert the Japanese characters from the source database code page to the PowerCenter Client code page. Instead, the PowerCenter Designer imports the Japanese characters as question marks (?), changing the name of the table. The PowerCenter Repository Service saves the source table name in the PowerCenter repository as question marks. If the PowerCenter Integration Service sends a query to the source database using the changed table name, the source database cannot find the correct table, and returns no rows or an error to the PowerCenter Integration Service, causing the session to fail.

Because the US-ASCII code page is a subset of both the ISO 8859-1 and Shift-JIS code pages, you can avoid these data inconsistencies if you use 7-bit ASCII characters for all of your metadata.

Case Study: Processing ISO 8859-1 Data

This case study describes how you might set up an environment to process ISO 8859-1 multibyte data. You might want to configure your environment this way if you need to process data from different Western European languages with character sets contained in the ISO 8859-1 code page. This example describes an environment that processes English and German language data.

For this case study, the ISO 8859-1 environment consists of the following elements:

- The PowerCenter Integration Service on a UNIX system
- PowerCenter Client on a Windows system, purchased in the United States
- The PowerCenter repository stored on an Oracle database on UNIX
- A source database containing English language data
- Another source database containing German and English language data
- A target database containing German and English language data

- A lookup database containing English language data

  The data environment must process English and German character data.

Configuring the ISO 8859-1 Environment

Use the following guidelines when you configure an environment similar to this case study for ISO 8859-1 data processing:

1. Verify code page compatibility between the PowerCenter repository database client and the database server.
2. Verify code page compatibility between the PowerCenter Client and the PowerCenter repository, and between the PowerCenter Integration Service process and the PowerCenter repository.
3. Set the PowerCenter Integration Service data movement mode to ASCII.
4. Verify session code page compatibility.
5. Verify lookup and stored procedure database code page compatibility.
6. Verify External Procedure or Custom transformation procedure code page compatibility.
7. Configure session sort order.

Step 1. Verify PowerCenter Repository Database Client and Server Compatibility

The database client and server hosting the PowerCenter repository must be able to communicate without data loss.

The PowerCenter repository resides in an Oracle database. Use NLS_LANG to set the locale (language, territory, and character set) you want the database client and server to use with your login:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

By default, Oracle configures NLS_LANG for the U.S. English language, the U.S. territory, and the 7-bit ASCII character set:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Change the default configuration to write ISO 8859-1 data to the PowerCenter repository using the Oracle WE8ISO8859P1 code page. For example:

```
NLS_LANG = AMERICAN_AMERICA.WE8ISO8859P1
```

For more information about verifying and changing the PowerCenter repository database code page, see your database documentation.

Step 2. Verify PowerCenter Code Page Compatibility

The PowerCenter Integration Service and PowerCenter Client code pages must be subsets of the PowerCenter repository code page. Because the PowerCenter Client and PowerCenter Integration Service each use the system code pages of the machines they are installed on, you must verify that the system code pages are subsets of the PowerCenter repository code page.

In this case, the PowerCenter Client on Windows systems were purchased in the United States. Thus the system code pages for the PowerCenter Client machines are set to MS Windows Latin1 by default. To verify system input and display languages, open the Regional Options dialog box from the Windows Control Panel. For systems purchased in the United States, the Regional Settings and Input Locale must be configured for English (United States).

The PowerCenter Integration Service is installed on a UNIX machine. The default code page for UNIX operating systems is ASCII. In this environment, change the UNIX system code page to ISO 8859-1 Western European so that it is a subset of the PowerCenter repository code page.

Step 3. Configure the PowerCenter Integration Service for ASCII Data Movement Mode

Configure the PowerCenter Integration Service to process ISO 8859-1 data. In the Administrator tool, set the Data Movement Mode to ASCII for the PowerCenter Integration Service.

Step 4. Verify Session Code Page Compatibility

When you run a workflow in ASCII data movement mode, the PowerCenter Integration Service enforces source and target code page relationships. To guarantee accurate data conversion, the source code page must be a subset of the target code page.

In this case, the environment contains source databases containing German and English data. When you configure a source database connection in the PowerCenter Workflow Manager, the code page for the connection must be identical to the source database code page and must be a subset of the target code page. Since both the MS Windows Latin1 and the ISO 8859-1 Western European code pages contain German characters, you would most likely use one of these code pages for source database connections.

Because the target code page must be a superset of the source code page, use either MS Windows Latin1, ISO 8859-1 Western European, or UTF-8 for target database connection or flat file code pages. To ensure data consistency, the configured target code page must match the target database or flat file system code page.

If you configure the PowerCenter Integration Service for relaxed code page validation, the PowerCenter Integration Service removes restrictions on source and target code page compatibility. You can select any supported code page for source and target data. However, you must ensure that the targets only receive character data encoded in the target code page.

Step 5. Verify Lookup and Stored Procedure Database Code Page Compatibility

Lookup and stored procedure database code pages must be supersets of the source code pages and subsets of the target code pages. In this case, all lookup and stored procedure database connections must use a code page compatible with the ISO 8859-1 Western European or MS Windows Latin1 code pages.

Step 6. Verify External Procedure or Custom Transformation Procedure Compatibility

External Procedure and Custom transformation procedures must be able to process character data from the source code pages, and they must pass characters that are compatible in the target code pages. In this case, all data processed by the External Procedure or Custom transformations must be in the ISO 8859-1 Western European or MS Windows Latin1 code pages.

Step 7. Configure Session Sort Order

When you run the PowerCenter Integration Service in ASCII mode, it uses a binary sort order for all sessions. In the session properties, the PowerCenter Workflow Manager lists all sort orders associated with the PowerCenter Integration Service code page. You can select a sort order for the session.

Case Study: Processing Unicode UTF-8 Data

This case study describes how you might set up an environment that processes Unicode UTF-8 multibyte data. You might want to configure your environment this way if you need to process data from Western European,

Middle Eastern, Asian, or any other language with characters encoded in the UTF-8 character set. This example describes an environment that processes German and Japanese language data.

For this case study, the UTF-8 environment consists of the following elements:

- The PowerCenter Integration Service on a UNIX machine
- The PowerCenter Clients on Windows systems
- The PowerCenter repository stored on an Oracle database on UNIX
- A source database contains German language data
- A source database contains German and Japanese language data
- A target database contains German and Japanese language data
- A lookup database contains German language data

  The data environment must process German and Japanese character data.

Configuring the UTF-8 Environment

Use the following guidelines when you configure an environment similar to this case study for UTF-8 data processing:

1. Verify code page compatibility between the PowerCenter repository database client and the database server.
2. Verify code page compatibility between the PowerCenter Client and the PowerCenter repository, and between the PowerCenter Integration Service and the PowerCenter repository.
3. Configure the PowerCenter Integration Service for Unicode data movement mode.
4. Verify session code page compatibility.
5. Verify lookup and stored procedure database code page compatibility.
6. Verify External Procedure or Custom transformation procedure code page compatibility.
7. Configure session sort order.

Step 1. Verify PowerCenter Repository Database Client and Server Code Page Compatibility

The database client and server hosting the PowerCenter repository must be able to communicate without data loss.

The PowerCenter repository resides in an Oracle database. With Oracle, you can use NLS_LANG to set the locale (language, territory, and character set) you want the database client and server to use with your login:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

By default, Oracle configures NLS_LANG for U.S. English language, the U.S. territory, and the 7-bit ASCII character set:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Change the default configuration to write UTF-8 data to the PowerCenter repository using the Oracle UTF8 character set. For example:

```
NLS_LANG = AMERICAN_AMERICA.UTF8
```

For more information about verifying and changing the PowerCenter repository database code page, see your database documentation.

Step 2. Verify PowerCenter Code Page Compatibility

The PowerCenter Integration Service and PowerCenter Client code pages must be subsets of the PowerCenter repository code page. Because the PowerCenter Client and PowerCenter Integration Service each use the system code pages of the machines they are installed on, you must verify that the system code pages are subsets of the PowerCenter repository code page.

In this case, the PowerCenter Client on Windows systems were purchased in Switzerland. Thus, the system code pages for the PowerCenter Client machines are set to MS Windows Latin1 by default. To verify system input and display languages, open the Regional Options dialog box from the Windows Control Panel.

The PowerCenter Integration Service is installed on a UNIX machine. The default code page for UNIX operating systems is ASCII. In this environment, the UNIX system character set must be changed to UTF-8.

Step 3. Configure the PowerCenter Integration Service for Unicode Data Movement Mode

You must configure the PowerCenter Integration Service to process UTF-8 data. In the Administrator tool, set the Data Movement Mode to Unicode for the PowerCenter Integration Service. The PowerCenter Integration Service allots an extra byte for each character when processing multibyte data.

Step 4. Verify Session Code Page Compatibility

When you run a PowerCenter workflow in Unicode data movement mode, the PowerCenter Integration Service enforces source and target code page relationships. To guarantee accurate data conversion, the source code page must be a subset of the target code page.

In this case, the environment contains a source database containing German and Japanese data. When you configure a source database connection in the PowerCenter Workflow Manager, the code page for the connection must be identical to the source database code page. You can use any code page for the source database.

Because the target code page must be a superset of the source code pages, you must use UTF-8 for the target database connections or flat files. To ensure data consistency, the configured target code page must match the target database or flat file system code page.

If you configure the PowerCenter Integration Service for relaxed code page validation, the PowerCenter Integration Service removes restrictions on source and target code page compatibility. You can select any supported code page for source and target data. However, you must ensure that the targets only receive character data encoded in the target code page.

Step 5. Verify Lookup and Stored Procedure Database Code Page Compatibility

Lookup and stored procedure database code pages must be supersets of the source code pages and subsets of the target code pages. In this case, all lookup and stored procedure database connections must use a code page compatible with UTF-8.

Step 6. Verify External Procedure or Custom Transformation Procedure Compatibility

External Procedure and Custom transformation procedures must be able to process character data from the source code pages, and they must pass characters that are compatible in the target code pages.

In this case, the External Procedure or Custom transformations must be able to process the German and Japanese data from the sources. However, the PowerCenter Integration Service passes data to procedures in UCS-2. Therefore, all data processed by the External Procedure or Custom transformations must be in the UCS-2 character set.

Step 7. Configure Session Sort Order

When you run the PowerCenter Integration Service in Unicode mode, it sorts session data using the sort order configured for the session. By default, sessions are configured for a binary sort order.

To sort German and Japanese data when the PowerCenter Integration Service uses UTF-8, you most likely want to use the default binary sort order.

APPENDIX A

Code Pages

This appendix includes the following topics:

- Supported Code Pages for Application Services, 440
- Supported Code Pages for Sources and Targets, 442

Supported Code Pages for Application Services

Informatica supports code pages for internationalization. Informatica uses International Components for Unicode (ICU) for its globalization support. For a list of code page aliases in ICU, see http://demo.icu-project.org/icu-bin/convexp.

The following table lists the name, description, and ID for supported code pages for the PowerCenter Repository Service, the Metadata Manager Service, and for each PowerCenter Integration Service process. When you assign an application service code page in the Administrator tool, you select the code page description.

Name	Description	ID
IBM037	IBM EBCDIC US English	2028
IBM1047	IBM EBCDIC US English IBM1047	1047
IBM273	IBM EBCDIC German	2030
IBM280	IBM EBCDIC Italian	2035
IBM285	IBM EBCDIC UK English	2038
IBM297	IBM EBCDIC French	2040
IBM500	IBM EBCDIC International Latin-1	2044
IBM930	IBM EBCDIC Japanese	930
IBM935	IBM EBCDIC Simplified Chinese	935
IBM937	IBM EBCDIC Traditional Chinese	937
IBM939	IBM EBCDIC Japanese CP939	939

Name	Description	ID
ISO-8859-10	ISO 8859-10 Latin 6 (Nordic)	13
ISO-8859-15	ISO 8859-15 Latin 9 (Western European)	201
ISO-8859-2	ISO 8859-2 Eastern European	5
ISO-8859-3	ISO 8859-3 Southeast European	6
ISO-8859-4	ISO 8859-4 Baltic	7
ISO-8859-5	ISO 8859-5 Cyrillic	8
ISO-8859-6	ISO 8859-6 Arabic	9
ISO-8859-7	ISO 8859-7 Greek	10
ISO-8859-8	ISO 8859-8 Hebrew	11
ISO-8859-9	ISO 8859-9 Latin 5 (Turkish)	12
JapanEUC	Japanese Extended UNIX Code (including JIS X 0212)	18
Latin1	ISO 8859-1 Western European	4
MS1250	MS Windows Latin 2 (Central Europe)	2250
MS1251	MS Windows Cyrillic (Slavic)	2251
MS1252	MS Windows Latin 1 (ANSI), superset of Latin1	2252
MS1253	MS Windows Greek	2253
MS1254	MS Windows Latin 5 (Turkish), superset of ISO 8859-9	2254
MS1255	MS Windows Hebrew	2255
MS1256	MS Windows Arabic	2256
MS1257	MS Windows Baltic Rim	2257
MS1258	MS Windows Vietnamese	2258
MS1361	MS Windows Korean (Johab)	1361
MS874	MS-DOS Thai, superset of TIS 620	874
MS932	MS Windows Japanese, Shift-JIS	2024
MS936	MS Windows Simplified Chinese, superset of GB 2312-80, EUC encoding	936
MS949	MS Windows Korean, superset of KS C 5601-1992	949
MS950	MS Windows Traditional Chinese, superset of Big 5	950

Name	Description	ID
US-ASCII	7-bit ASCII	1
UTF-8	UTF-8 encoding of Unicode	106

Supported Code Pages for Sources and Targets

Informatica supports code pages for internationalization. Informatica uses International Components for Unicode (ICU) for its globalization support. For a list of code page aliases in ICU, see http://demo.icu-project.org/icu-bin/convexp.

The following table lists the name, description, and ID for supported code pages for sources and targets. When you assign a source or target code page in the PowerCenter Client, you select the code page description. When you assign a code page using the *pmrep* CreateConnection command or define a code page in a parameter file, you enter the code page name.

Name	Description	ID
Adobe-Standard-Encoding	Adobe Standard Encoding	10073
BOCU-1	Binary Ordered Compression for Unicode (BOCU-1)	10010
CESU-8	ICompatibility Encoding Scheme for UTF-16 (CESU-8)	10011
cp1006	ISO Urdu	10075
cp1098	PC Farsi	10076
cp1124	ISO Cyrillic Ukraine	10077
cp1125	PC Cyrillic Ukraine	10078
cp1131	PC Cyrillic Belarus	10080
cp1381	PC Chinese GB (S-Ch Data mixed)	10082
cp850	PC Latin1	10036
cp851	PC DOS Greek (without euro)	10037
cp856	PC Hebrew (old)	10040
cp857	PC Latin5 (without euro update)	10041
cp858	PC Latin1 (with euro update)	10042
cp860	PC Portugal	10043
cp861	PC Iceland	10044

Name	Description	ID
cp862	PC Hebrew (without euro update)	10045
cp863	PC Canadian French	10046
cp864	PC Arabic (without euro update)	10047
cp865	PC Nordic	10048
cp866	PC Russian (without euro update)	10049
cp868	PC Urdu	10051
cp869	PC Greek (without euro update)	10052
cp922	IPC Estonian (without euro update)	10056
cp949c	PC Korea - KS	10028
ebcdic-xml-us	EBCDIC US (with euro) - Extension for XML4C(Xerces)	10180
EUC-KR	EUC Korean	10029
GB_2312-80	Simplified Chinese (GB2312-80)	10025
gb18030	GB 18030 MBCS codepage	1392
GB2312	Chinese EUC	10024
HKSCS	Hong Kong Supplementary Character Set	9200
hp-roman8	HP Latin1	10072
HZ-GB-2312	Simplified Chinese (HZ GB2312)	10092
IBM037	IBM EBCDIC US English	2028
IBM-1025	EBCDIC Cyrillic	10127
IBM1026	EBCDIC Turkey	10128
IBM1047	IBM EBCDIC US English IBM1047	1047
IBM-1047-s390	EBCDIC IBM-1047 for S/390 (lf and nl swapped)	10167
IBM-1097	EBCDIC Farsi	10129
IBM-1112	EBCDIC Baltic	10130
IBM-1122	EBCDIC Estonia	10131
IBM-1123	EBCDIC Cyrillic Ukraine	10132
IBM-1129	ISO Vietnamese	10079

Name	Description	ID
IBM-1130	EBCDIC Vietnamese	10133
IBM-1132	EBCDIC Lao	10134
IBM-1133	ISO Lao	10081
IBM-1137	EBCDIC Devanagari	10163
IBM-1140	EBCDIC US (with euro update)	10135
IBM-1140-s390	EBCDIC IBM-1140 for S/390 (lf and nl swapped)	10168
IBM-1141	EBCDIC Germany, Austria (with euro update)	10136
IBM-1142	EBCDIC Denmark, Norway (with euro update)	10137
IBM-1142-s390	EBCDIC IBM-1142 for S/390 (lf and nl swapped)	10169
IBM-1143	EBCDIC Finland, Sweden (with euro update)	10138
IBM-1143-s390	EBCDIC IBM-1143 for S/390 (lf and nl swapped)	10170
IBM-1144	EBCDIC Italy (with euro update)	10139
IBM-1144-s390	EBCDIC IBM-1144 for S/390 (lf and nl swapped)	10171
IBM-1145	EBCDIC Spain, Latin America (with euro update)	10140
IBM-1145-s390	EBCDIC IBM-1145 for S/390 (lf and nl swapped)	10172
IBM-1146	EBCDIC UK, Ireland (with euro update)	10141
IBM-1146-s390	EBCDIC IBM-1146 for S/390 (lf and nl swapped)	10173
IBM-1147	EBCDIC French (with euro update)	10142
IBM-1147-s390	EBCDIC IBM-1147 for S/390 (lf and nl swapped)	10174
IBM-1147-s390	EBCDIC IBM-1147 for S/390 (lf and nl swapped)	10174
IBM-1148	EBCDIC International Latin1 (with euro update)	10143
IBM-1148-s390	EBCDIC IBM-1148 for S/390 (lf and nl swapped)	10175
IBM-1149	EBCDIC Iceland (with euro update)	10144
IBM-1149-s390	IEBCDIC IBM-1149 for S/390 (lf and nl swapped)	10176
IBM-1153	EBCDIC Latin2 (with euro update)	10145
IBM-1153-s390	EBCDIC IBM-1153 for S/390 (lf and nl swapped)	10177
IBM-1154	EBCDIC Cyrillic Multilingual (with euro update)	10146

Name	Description	ID
IBM-1155	EBCDIC Turkey (with euro update)	10147
IBM-1156	EBCDIC Baltic Multilingual (with euro update)	10148
IBM-1157	EBCDIC Estonia (with euro update)	10149
IBM-1158	EBCDIC Cyrillic Ukraine (with euro update)	10150
IBM1159	IBM EBCDIC Taiwan, Traditional Chinese	11001
IBM-1160	EBCDIC Thai (with euro update)	10151
IBM-1162	Thai (with euro update)	10033
IBM-1164	EBCDIC Vietnamese (with euro update)	10152
IBM-1250	MS Windows Latin2 (without euro update)	10058
IBM-1251	MS Windows Cyrillic (without euro update)	10059
IBM-1255	MS Windows Hebrew (without euro update)	10060
IBM-1256	MS Windows Arabic (without euro update)	10062
IBM-1257	MS Windows Baltic (without euro update)	10064
IBM-1258	MS Windows Vietnamese (without euro update)	10066
IBM-12712	EBCDIC Hebrew (updated with euro and new sheqel, control characters)	10161
IBM-12712-s390	EBCDIC IBM-12712 for S/390 (lf and nl swapped)	10178
IBM-1277	Adobe Latin1 Encoding	10074
IBM13121	IBM EBCDIC Korean Extended CP13121	11002
IBM13124	IBM EBCDIC Simplified Chinese CP13124	11003
IBM-1363	PC Korean KSC MBCS Extended (with \ <-> Won mapping)	10032
IBM-1364	EBCDIC Korean Extended (SBCS IBM-13121 combined with DBCS IBM-4930)	10153
IBM-1371	EBCDIC Taiwan Extended (SBCS IBM-1159 combined with DBCS IBM-9027)	10154
IBM-1373	Taiwan Big-5 (with euro update)	10019
IBM-1375	MS Taiwan Big-5 with HKSCS extensions	10022
IBM-1386	PC Chinese GBK (IBM-1386)	10023
IBM-1388	EBCDIC Chinese GB (S-Ch DBCS-Host Data)	10155

Name	Description	ID
IBM-1390	EBCDIC Japanese Katakana (with euro)	10156
IBM-1399	EBCDIC Japanese Latin-Kanji (with euro)	10157
IBM-16684	EBCDIC Japanese Extended (DBCS IBM-1390 combined with DBCS IBM-1399)	10158
IBM-16804	EBCDIC Arabic (with euro update)	10162
IBM-16804-s390	EBCDIC IBM-16804 for S/390 (lf and nl swapped)	10179
IBM-25546	ISO-2022 encoding for Korean (extension 1)	10089
IBM273	IBM EBCDIC German	2030
IBM277	EBCDIC Denmark, Norway	10115
IBM278	EBCDIC Finland, Sweden	10116
IBM280	IBM EBCDIC Italian	2035
IBM284	EBCDIC Spain, Latin America	10117
IBM285	IBM EBCDIC UK English	2038
IBM290	EBCDIC Japanese Katakana SBCS	10118
IBM297	IBM EBCDIC French	2040
IBM-33722	Japanese EUC (with \ <-> Yen mapping)	10017
IBM367	IBM367	10012
IBM-37-s390	EBCDIC IBM-37 for S/390 (lf and nl swapped)	10166
IBM420	EBCDIC Arabic	10119
IBM424	EBCDIC Hebrew (updated with new sheqel, control characters)	10120
IBM437	PC United States	10035
IBM-4899	EBCDIC Hebrew (with euro)	10159
IBM-4909	ISO Greek (with euro update)	10057
IBM4933	IBM Simplified Chinese CP4933	11004
IBM-4971	EBCDIC Greek (with euro update)	10160
IBM500	IBM EBCDIC International Latin-1	2044
IBM-5050	Japanese EUC (Packed Format)	10018
IBM-5123	EBCDIC Japanese Latin (with euro update)	10164

Name	Description	ID
IBM-5351	MS Windows Hebrew (older version)	10061
IBM-5352	MS Windows Arabic (older version)	10063
IBM-5353	MS Windows Baltic (older version)	10065
IBM-803	EBCDIC Hebrew	10121
IBM833	IBM EBCDIC Korean CP833	833
IBM834	IBM EBCDIC Korean CP834	834
IBM835	IBM Taiwan, Traditional Chinese CP835	11005
IBM836	IBM EBCDIC Simplified Chinese Extended	11006
IBM837	IBM Simplified Chinese CP837	11007
IBM-838	EBCDIC Thai	10122
IBM-8482	EBCDIC Japanese Katakana SBCS (with euro update)	10165
IBM852	PC Latin2 (without euro update)	10038
IBM855	PC Cyrillic (without euro update)	10039
IBM-867	PC Hebrew (with euro update)	10050
IBM870	EBCDIC Latin2	10123
IBM871	EBCDIC Iceland	10124
IBM-874	PC Thai (without euro update)	10034
IBM-875	EBCDIC Greek	10125
IBM-901	PC Baltic (with euro update)	10054
IBM-902	PC Estonian (with euro update)	10055
IBM918	EBCDIC Urdu	10126
IBM930	IBM EBCDIC Japanese	930
IBM933	IBM EBCDIC Korean CP933	933
IBM935	IBM EBCDIC Simplified Chinese	935
IBM937	IBM EBCDIC Traditional Chinese	937
IBM939	IBM EBCDIC Japanese CP939	939
IBM-942	PC Japanese SJIS-78 syntax (IBM-942)	10015

Name	Description	ID
IBM-943	PC Japanese SJIS-90 (IBM-943)	10016
IBM-949	PC Korea - KS (default)	10027
IBM-950	Taiwan Big-5 (without euro update)	10020
IBM-964	EUC Taiwan	10026
IBM-971	EUC Korean (DBCS-only)	10030
IMAP-mailbox-name	IMAP Mailbox Name	10008
is-960	Israeli Standard 960 (7-bit Hebrew encoding)	11000
ISO-2022-CN	ISO-2022 encoding for Chinese	10090
ISO-2022-CN-EXT	ISO-2022 encoding for Chinese (extension 1)	10091
ISO-2022-JP	ISO-2022 encoding for Japanese	10083
ISO-2022-JP-2	ISO-2022 encoding for Japanese (extension 2)	10085
ISO-2022-KR	ISO-2022 encoding for Korean	10088
ISO-8859-10	ISO 8859-10 Latin 6 (Nordic)	13
ISO-8859-13	ISO 8859-13 PC Baltic (without euro update)	10014
ISO-8859-15	ISO 8859-15 Latin 9 (Western European)	201
ISO-8859-2	ISO 8859-2 Eastern European	5
ISO-8859-3	ISO 8859-3 Southeast European	6
ISO-8859-4	ISO 8859-4 Baltic	7
ISO-8859-5	ISO 8859-5 Cyrillic	8
ISO-8859-6	ISO 8859-6 Arabic	9
ISO-8859-7	ISO 8859-7 Greek	10
ISO-8859-8	ISO 8859-8 Hebrew	11
ISO-8859-9	ISO 8859-9 Latin 5 (Turkish)	12
JapanEUC	Japanese Extended UNIX Code (including JIS X 0212)	18
JEF	Japanese EBCDIC Fujitsu	9000
JEF-K	Japanese EBCDIC-Kana Fujitsu	9005
JIPSE	NEC ACOS JIPSE Japanese	9002

Name	Description	ID
JIPSE-K	NEC ACOS JIPSE-Kana Japanese	9007
JIS_Encoding	ISO-2022 encoding for Japanese (extension 1)	10084
JIS_X0201	ISO-2022 encoding for Japanese (JIS_X0201)	10093
JIS7	ISO-2022 encoding for Japanese (extension 3)	10086
JIS8	ISO-2022 encoding for Japanese (extension 4)	10087
JP-EBCDIC	EBCDIC Japanese	9010
JP-EBCDIK	EBCDIK Japanese	9011
KEIS	HITACHI KEIS Japanese	9001
KEIS-K	HITACHI KEIS-Kana Japanese	9006
KOI8-R	IRussian Internet	10053
KSC_5601	PC Korean KSC MBCS Extended (KSC_5601)	10031
Latin1	ISO 8859-1 Western European	4
LMBCS-1	Lotus MBCS encoding for PC Latin1	10103
LMBCS-11	Lotus MBCS encoding for MS-DOS Thai	10110
LMBCS-16	Lotus MBCS encoding for Windows Japanese	10111
LMBCS-17	Lotus MBCS encoding for Windows Korean	10112
LMBCS-18	Lotus MBCS encoding for Windows Chinese (Traditional)	10113
LMBCS-19	Lotus MBCS encoding for Windows Chinese (Simplified)	10114
LMBCS-2	Lotus MBCS encoding for PC DOS Greek	10104
LMBCS-3	Lotus MBCS encoding for Windows Hebrew	10105
LMBCS-4	Lotus MBCS encoding for Windows Arabic	10106
LMBCS-5	Lotus MBCS encoding for Windows Cyrillic	10107
LMBCS-6	Lotus MBCS encoding for PC Latin2	10108
LMBCS-8	Lotus MBCS encoding for Windows Turkish	10109
macintosh	Apple Latin 1	10067
MELCOM	MITSUBISHI MELCOM Japanese	9004
MELCOM-K	MITSUBISHI MELCOM-Kana Japanese	9009

Name	Description	ID
MS1250	MS Windows Latin 2 (Central Europe)	2250
MS1251	MS Windows Cyrillic (Slavic)	2251
MS1252	MS Windows Latin 1 (ANSI), superset of Latin1	2252
MS1253	MS Windows Greek	2253
MS1254	MS Windows Latin 5 (Turkish), superset of ISO 8859-9	2254
MS1255	MS Windows Hebrew	2255
MS1256	MS Windows Arabic	2256
MS1257	MS Windows Baltic Rim	2257
MS1258	MS Windows Vietnamese	2258
MS1361	MS Windows Korean (Johab)	1361
MS874	MS-DOS Thai, superset of TIS 620	874
MS932	MS Windows Japanese, Shift-JIS	2024
MS936	MS Windows Simplified Chinese, superset of GB 2312-80, EUC encoding	936
MS949	MS Windows Korean, superset of KS C 5601-1992	949
MS950	MS Windows Traditional Chinese, superset of Big 5	950
SCSU	Standard Compression Scheme for Unicode (SCSU)	10009
UNISYS	UNISYS Japanese	9003
UNISYS-K	UNISYS-Kana Japanese	9008
US-ASCII	7-bit ASCII	1
UTF-16_OppositeEndian	UTF-16 encoding of Unicode (Opposite Platform Endian)	10004
UTF-16_PlatformEndian	UTF-16 encoding of Unicode (Platform Endian)	10003
UTF-16BE	UTF-16 encoding of Unicode (Big Endian)	1200
UTF-16LE	UTF-16 encoding of Unicode (Lower Endian)	1201
UTF-32_OppositeEndian	UTF-32 encoding of Unicode (Opposite Platform Endian)	10006
UTF-32_PlatformEndian	UTF-32 encoding of Unicode (Platform Endian)	10005
UTF-32BE	UTF-32 encoding of Unicode (Big Endian)	10001
UTF-32LE	UTF-32 encoding of Unicode (Lower Endian)	10002

Name	Description	ID
UTF-7	UTF-7 encoding of Unicode	10007
UTF-8	UTF-8 encoding of Unicode	106
windows-57002	Indian Script Code for Information Interchange - Devanagari	10094
windows-57003	Indian Script Code for Information Interchange - Bengali	10095
windows-57004	Indian Script Code for Information Interchange - Tamil	10099
windows-57005	Indian Script Code for Information Interchange - Telugu	10100
windows-57007	Indian Script Code for Information Interchange - Oriya	10098
windows-57008	Indian Script Code for Information Interchange - Kannada	10101
windows-57009	Indian Script Code for Information Interchange - Malayalam	10102
windows-57010	Indian Script Code for Information Interchange - Gujarati	10097
windows-57011	Indian Script Code for Information Interchange - Gurumukhi	10096
x-mac-centraleurroman	Apple Central Europe	10070
x-mac-cyrillic	Apple Cyrillic	10069
x-mac-greek	Apple Greek	10068
x-mac-turkish	Apple Turkish	10071

Note: Select IBM EBCDIC as your source database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.

APPENDIX B

Command Line Privileges and Permissions

This appendix includes the following topics:

- infacmd as Commands, 452
- infacmd dis Commands, 453
- infacmd ipc Commands, 454
- infacmd isp Commands, 454
- infacmd mrs Commands, 464
- infacmd ms Commands, 465
- infacmd oie Commands, 465
- infacmd ps Commands, 465
- infacmd pwx Commands, 466
- infacmd rtm Commands, 467
- infacmd sql Commands, 467
- pmcmd Commands, 468
- pmrep Commands, 470

infacmd as Commands

To run *infacmd as* commands, users must have one of the listed sets of domain privileges, Analyst Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd as* commands:

infacmd as Command	Privilege Group	Privilege Name	Permission On...
CreateAuditTables	Domain Administration	Manage Service	Domain or node where Analyst Service runs
CreateService	Domain Administration	Manage Service	Domain or node where Analyst Service runs

infacmd as Command	Privilege Group	Privilege Name	Permission On...
DeleteAuditTables	Domain Administration	Manage Service	Domain or node where Analyst Service runs
ListServiceOptions	n/a	n/a	Analyst Service
ListServiceProcessOptions	n/a	n/a	Analyst Service
UpdateServiceOptions	Domain Administration	Manage Service	Domain or node where Analyst Service runs
UpdateServiceProcessOptions	Domain Administration	Manage Service	Domain or node where Analyst Service runs

infacmd dis Commands

To run *infacmd dis* commands, users must have one of the listed sets of domain privileges, Data Integration Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd dis* commands:

infacmd dis Command	Privilege Group	Privilege Name	Permission On...
BackupApplication	Application Administration	Manage Applications	n/a
CancelDataObjectCacheRefresh	n/a	n/a	n/a
CreateService	Domain Administration	Manage Services	Domain or node where Data Integration Service runs
DeployApplication	Application Administration	Manage Applications	n/a
ListApplicationObjects	n/a	n/a	n/a
ListApplications	n/a	n/a	n/a
ListDataObjectOptions	n/a	n/a	n/a
ListServiceOptions	n/a	Manage Service	Domain or node where Data Integration Service runs
ListServiceProcessOptions	n/a	Manage Service	Domain or node where Data Integration Service runs
PurgeDataObjectCache	n/a	n/a	n/a
RefreshDataObjectCache	n/a	n/a	n/a
RenameApplication	Application Administration	Manage Applications	n/a

infacmd dis Command	Privilege Group	Privilege Name	Permission On...
RestoreApplication	Application Administration	Manage Applications	n/a
StartApplication	Application Administration	Manage Applications	n/a
StopApplication	Application Administration	Manage Applications	n/a
UndeployApplication	Application Administration	Manage Applications	n/a
UpdateApplication	Application Administration	Manage Applications	n/a
UpdateApplicationOptions	Application Administration	Manage Applications	n/a
UpdateDataObjectOptions	Application Administration	Manage Applications	n/a
UpdateServiceOptions	Domain Administration	Manage Services	Domain or node where Data Integration Service runs
UpdateServiceProcessOptions	Domain Administration	Manage Services	Domain or node where Data Integration Service runs

infacmd ipc Commands

To run *infacmd ipc* commands, users must have one of the listed Model repository object permissions.

The following table lists the required privileges and permissions for *infacmd ipc* commands:

infacmd ipc Command	Privilege Group	Privilege Name	Permission On...
ExportToPC	n/a	n/a	Read on the folder that creates reference tables to be exported

infacmd isp Commands

To run the following *infacmd isp* commands, users must have one of the listed sets of domain privileges, service privileges, domain object permissions, and connection permissions.

The following table lists the required privileges and permissions for *infacmd isp* commands:

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
AddAlertUser (for your user account)	n/a	n/a	n/a
AddAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	n/a
AddConnectionPermissions	n/a	n/a	Grant on connection
AddDomainLink*	n/a	n/a	n/a
AddDomainNode	Domain Administration	Manage Nodes and Grids	Domain and node
AssignGroupPermission (on application services or license objects)	Domain Administration	Manage Services	Application service or license object
AssignGroupPermission (on domain)*	n/a	n/a	n/a
AssignGroupPermission (on folders)	Domain Administration	Manage Domain Folders	Folder
AssignGroupPermission (on nodes and grids)	Domain Administration	Manage Nodes and Grids	Node or grid
AssignGroupPermission (on operating system profiles)*	n/a	n/a	n/a
AddGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AddLicense	Domain Administration	Manage Services	Domain or parent folder
AddNodeResource	Domain Administration	Manage Nodes and Grids	Node
AddRolePrivilege	Security Administration	Manage Users, Groups, and Roles	n/a
AddServiceLevel*	n/a	n/a	n/a
AssignUserPermission (on application services or license objects)	Domain Administration	Manage Services	Application service or license object
AssignUserPermission (on domain)*	n/a	n/a	n/a
AssignUserPermission (on folders)	Domain Administration	Manage Domain Folders	Folder

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
AssignUserPermission (on nodes or grids)	Domain Administration	Manage Nodes and Grids	Node or grid
AssignUserPermission (on operating system profiles)*	n/a	n/a	n/a
AssignUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignUserToGroup	Security Administration	Manage Users, Groups, and Roles	n/a
AssignedToLicense	Domain Administration	Manage Services	License object and application service
AssignISTOMMService	Domain Administration	Manage Services	Metadata Manager Service
AssignLicense	Domain Administration	Manage Services	License object and application service
AssignRoleToGroup	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignRoleToUser	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignRSToWSHubService	Domain Administration	Manage Services	PowerCenter Repository Service and Web Services Hub
BackupReportingServiceContents	Domain Administration	Manage Services	Reporting Service
ConvertLogFile	n/a	n/a	Domain or application service
CreateFolder	Domain Administration	Manage Domain Folders	Domain or parent folder
CreateConnection	n/a	n/a	n/a
CreateGrid	Domain Administration	Manage Nodes and Grids	Domain or parent folder and nodes assigned to grid
CreateGroup	Security Administration	Manage Users, Groups, and Roles	n/a

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
CreateIntegrationService	Domain Administration	Manage Services	Domain or parent folder, node or grid where PowerCenter Integration Service runs, license object, and associated PowerCenter Repository Service
CreateMMService	Domain Administration	Manage Services	Domain or parent folder, node where Metadata Manager Service runs, license object, and associated PowerCenter Integration Service and PowerCenter Repository Service
CreateOSProfile*	n/a	n/a	n/a
CreateReportingService	Domain Administration	Manage Services	Domain or parent folder, node where Reporting Service runs, license object, and the application service selected for reporting
CreateReportingServiceContents	Domain Administration	Manage Services	Reporting Service
CreateRepositoryService	Domain Administration	Manage Services	Domain or parent folder, node where PowerCenter Repository Service runs, and license object
CreateRole	Security Administration	Manage Users, Groups, and Roles	n/a
CreateSAPBWService	Domain Administration	Manage Services	Domain or parent folder, node or grid where SAP BW Service runs, license object, and associated PowerCenter Integration Service
CreateUser	Security Administration	Manage Users, Groups, and Roles	n/a
CreateWSHubService	Domain Administration	Manage Services	Domain or parent folder, node or grid where Web Services Hub runs, license object, and associated PowerCenter Repository Service
DeleteSchemaReportingServiceContents	Domain Administration	Manage Services	Reporting Service
DisableNodeResource	Domain Administration	Manage Nodes and Grids	Node

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
DisableService (for Metadata Manager Service)	Domain Administration	Manage Service Execution	Metadata Manager Service and associated PowerCenter Integration Service and PowerCenter Repository Service
DisableService (for all other application services)	Domain Administration	Manage Service Execution	Application service
DisableServiceProcess	Domain Administration	Manage Service Execution	Application service
DisableUser	Security Administration	Manage Users, Groups, and Roles	n/a
EditUser	Security Administration	Manage Users, Groups, and Roles	n/a
EnableNodeResource	Domain Administration	Manage Nodes and Grids	Node
EnableService (for Metadata Manager Service)	Domain Administration	Manage Service Execution	Metadata Manager Service, and associated PowerCenter Integration Service and PowerCenter Repository Service
EnableService (for all other application services)	Domain Administration	Manage Service Execution	Application service
EnableServiceProcess	Domain Administration	Manage Service Execution	Application service
EnableUser	Security Administration	Manage Users, Groups, and Roles	n/a
ExportDomainObjects (for users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	n/a
ExportDomainObjects (for connections)	Domain Administration	Manage Connections	Read on connections
ExportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	n/a
GetFolderInfo	n/a	n/a	Folder
GetLastError	n/a	n/a	Application service
GetLog	n/a	n/a	Domain or application service
GetNodeName	n/a	n/a	Node
GetServiceOption	n/a	n/a	Application service
GetServiceProcessOption	n/a	n/a	Application service

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
GetServiceProcessStatus	n/a	n/a	Application service
GetServiceStatus	n/a	n/a	Application service
GetSessionLog	Run-time Objects	Monitor	Read on repository folder
GetWorkflowLog	Run-time Objects	Monitor	Read on repository folder
Help	n/a	n/a	n/a
ImportDomainObjects (for users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	n/a
ImportDomainObjects (for connections)	Domain Administration	Manage Connections	Write on connections
ImportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	n/a
ListAlertUsers	n/a	n/a	Domain
ListAllGroups	n/a	n/a	n/a
ListAllRoles	n/a	n/a	n/a
ListAllUsers	n/a	n/a	n/a
ListConnectionOptions	n/a	n/a	Read on connection
ListConnections	n/a	n/a	n/a
ListConnectionPermissions	n/a	n/a	n/a
ListConnectionPermissions by Group	n/a	n/a	n/a
ListConnectionPermissions by User	n/a	n/a	n/a
ListDomainLinks	n/a	n/a	Domain
ListDomainOptions	n/a	n/a	Domain
ListFolders	n/a	n/a	Folders
ListGridNodes	n/a	n/a	n/a
ListGroupsForUser	n/a	n/a	Domain
ListGroupPermissions	n/a	n/a	n/a
ListGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
			Repository Service, or Reporting Service
ListLDAPConnectivity	Security Administration	Manage Users, Groups, and Roles	n/a
ListLicenses	n/a	n/a	License objects
ListNodeOptions	n/a	n/a	Node
ListNodes	n/a	n/a	n/a
ListNodeResources	n/a	n/a	Node
ListPlugins	n/a	n/a	n/a
ListRepositoryLDAPConfiguration	n/a	n/a	Domain
ListRolePrivileges	n/a	n/a	n/a
ListSecurityDomains	Security Administration	Manage Users, Groups, and Roles	n/a
ListServiceLevels	n/a	n/a	Domain
ListServiceNodes	n/a	n/a	Application service
ListServicePrivileges	n/a	n/a	n/a
ListServices	n/a	n/a	n/a
ListSMTPOptions	n/a	n/a	Domain
ListUserPermissions	n/a	n/a	n/a
ListUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
MigrateReportingServiceContents	Domain Administration and Security Administration	Manage Services and Manage Users, Groups, and Roles	Domain
MoveFolder	Domain Administration	Manage Domain Folders	Original and destination folders
MoveObject (for application services or license objects)	Domain Administration	Manage Services	Original and destination folders
MoveObject (for nodes or grids)	Domain Administration	Manage Nodes and Grids	Original and destination folders
Ping	n/a	n/a	n/a

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
PurgeLog*	n/a	n/a	n/a
RemoveAlertUser (for your user account)	n/a	n/a	n/a
RemoveAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	n/a
RemoveConnection	n/a	n/a	Write on connection
RemoveConnectionPermissions	n/a	n/a	Grant on connection
RemoveDomainLink*	n/a	n/a	n/a
RemoveFolder	Domain Administration	Manage Domain Folders	Domain or parent folder and folder being removed
RemoveGrid	Domain Administration	Manage Nodes and Grids	Domain or parent folder and grid
RemoveGroup	Security Administration	Manage Users, Groups, and Roles	n/a
RemoveGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
RemoveLicense	Domain Administration	Manage Services	Domain or parent folder and license object
RemoveNode	Domain Administration	Manage Nodes and Grids	Domain or parent folder and node
RemoveNodeResource	Domain Administration	Manage Nodes and Grids	Node
RemoveOSProfile*	n/a	n/a	n/a
RemoveRole	Security Administration	Manage Users, Groups, and Roles	n/a
RemoveRolePrivilege	Security Administration	Manage Users, Groups, and Roles	n/a
RemoveService	Domain Administration	Manage Services	Domain or parent folder and application service
RemoveServiceLevel*	n/a	n/a	n/a
RemoveUser	Security Administration	Manage Users, Groups, and Roles	n/a

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
RemoveUserFromGroup	Security Administration	Manage Users, Groups, and Roles	n/a
RemoveUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
ResetPassword (for your user account)	n/a	n/a	n/a
ResetPassword (for other users)	Security Administration	Manage Users, Groups, and Roles	n/a
RestoreReportingServiceContents	Domain Administration	Manage Services	Reporting Service
RunCPUProfile	Domain Administration	Manage Nodes and Grids	Node
SetConnectionPermission	n/a	n/a	Grant on connection
SetLDAPConnectivity	Security Administration	Manage Users, Groups, and Roles	n/a
SetRepositoryLDAPConfiguration	n/a	n/a	Domain
ShowLicense	n/a	n/a	License object
ShutdownNode	Domain Administration	Manage Nodes and Grids	Node
SwitchToGatewayNode*	n/a	n/a	n/a
SwitchToWorkerNode*	n/a	n/a	n/a
UnAssignISMMService	Domain Administration	Manage Services	PowerCenter Integration Service and Metadata Manager Service
UnassignLicense	Domain Administration	Manage Services	License object and application service
UnAssignRoleFromGroup	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
UnAssignRoleFromUser	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
UnassignRSWSHubService	Domain Administration	Manage Services	PowerCenter Repository Service and Web Services Hub
UnassociateDomainNode	Domain Administration	Manage Nodes and Grids	Node
UpdateConnection	n/a	n/a	Write on connection
UpdateDomainOptions*	n/a	n/a	n/a
UpdateDomainPassword*	n/a	n/a	n/a
UpdateFolder	Domain Administration	Manage Domain Folders	Folder
UpdateGatewayInfo*	n/a	n/a	n/a
UpdateGrid	Domain Administration	Manage Nodes and Grids	Grid and nodes
UpdateIntegrationService	Domain Administration	Manage Services	PowerCenter Integration Service
UpdateLicense	Domain Administration	Manage Services	License object
UpdateMMService	Domain Administration	Manage Services	Metadata Manager Service
UpdateNodeOptions	Domain Administration	Manage Nodes and Grids	Node
UpdateOSProfile	Security Administration	Manage Users, Groups, and Roles	Operating system profile
UpdateReportingService	Domain Administration	Manage Services	Reporting Service
UpdateRepositoryService	Domain Administration	Manage Services	PowerCenter Repository Service
UpdateSAPBWService	Domain Administration	Manage Services	SAP BW Service
UpdateServiceLevel*	n/a	n/a	n/a
UpdateServiceProcess	Domain Administration	Manage Services	PowerCenter Integration Service Each node added to the PowerCenter Integration Service
UpdateSMTPOptions*	n/a	n/a	n/a
UpdateWSHubService	Domain Administration	Manage Services	Web Services Hub
UpgradeReportingServiceContents	Domain Administration	Manage Services	Reporting Service
*Users assigned the Administrator role for the domain can run these commands.			

infacmd mrs Commands

To run *infacmd mrs* commands, users must have one of the listed sets of domain privileges, Model Repository Service privileges, and Model repository object permissions.

The following table lists the required privileges and permissions for *infacmd mrs* commands:

infacmd mrs Command	Privilege Group	Privilege Name	Permission On...
BackupContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
CreateContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
CreateService	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
DeleteContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListBackupFiles	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListProjects	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListServiceOptions	n/a	n/a	The Model Repository Service
ListServiceProcessOptions	n/a	n/a	The Model Repository Service
RestoreContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
UpgradeContents	Domain Administration	Manage Service	The Model Repository Service
UpdateServiceOptions	Domain Administration	Manage Service	The Model Repository Service
UpdateServiceProcessOptions	Domain Administration	Manage Service	The Model Repository Service

infacmd ms Commands

To run *infacmd ms* commands, users must have one of the listed sets of domain object permissions.

The following table lists the required privileges and permissions for *infacmd ms* commands:

infacmd ms Command	Privilege Group	Privilege Name	Permission On...
ListMappings	n/a	n/a	n/a
ListMappingParams	n/a	n/a	n/a
RunMapping	n/a	n/a	Execute on connection objects used by the mapping

infacmd oie Commands

To run *infacmd oie* commands, users must have one of the listed Model repository object permissions.

The following table lists the required permissions for *infacmd oie* commands:

infacmd oie Command	Privilege Group	Privilege Name	Permission On...
ExportObjects	n/a	n/a	Read on project
ImportObjects	n/a	n/a	Write on project

infacmd ps Commands

To run *infacmd ps* commands, users must have one of the listed sets of profiling privileges and domain object permissions.

The following table lists the required privileges and permissions for *infacmd ps* commands:

infacmd ps Command	Privilege Group	Privilege Name	Permission On...
CreateWH	n/a	n/a	n/a
DropWH	n/a	n/a	n/a
Execute	n/a	n/a	Read on project Execute on the source connection object

infacmd ps Command	Privilege Group	Privilege Name	Permission On...
List	n/a	n/a	Read on project
Purge			Read and write on project

infacmd pwx Commands

To run *infacmd pwx* commands, users must have one of the listed sets of PowerExchange application service permissions and privileges.

The following table lists the required privileges and permissions for *infacmd pwx* commands:

infacmd pwx Command	Privilege Group	Privilege Name	Permission On...
CloseForceListener	Management Commands	closeforce	n/a
CloseListener	Management Commands	close	n/a
CondenseLogger	Management Commands	condense	n/a
CreateListenerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
CreateLoggerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
DisplayAllLogger	Informational Commands	displayall	n/a
DisplayCheckpointsLogger	Informational Commands	displaycheckpoints	n/a
DisplayCPULogger	Informational Commands	displaycpu	n/a
DisplayEventsLogger	Informational Commands	displayevents	n/a
DisplayMemoryLogger	Informational Commands	displaymemory	n/a
DisplayRecordsLogger	Informational Commands	displayrecords	n/a
DisplayStatusLogger	Informational Commands	displaystatus	n/a
FileSwitchLogger	Management Commands	fileswitch	n/a
ListTaskListener	Informational Commands	listtask	n/a
ShutDownLogger	Management Commands	shutdown	n/a
StopTaskListener	Management Commands	stoptask	n/a

infacmd pwx Command	Privilege Group	Privilege Name	Permission On...
UpdateListenerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
UpdateLoggerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs

infacmd rtm Commands

To run *infacmd rtm* commands, users must have one of the listed sets of Model Repository Service privileges and domain object permissions.

The following table lists the required privileges and permissions for *infacmd rtm* commands:

infacmd rtm Command	Privilege Group	Privilege Name	Permission On...
Deployimport	n/a	n/a	n/a
Export	n/a	n/a	Read on the project that contains reference tables to be exported
Import	n/a	n/a	Read and Write on the project where reference tables are imported

infacmd sql Commands

To run *infacmd sql* commands, users must have one of the listed sets of domain privileges, Data Integration Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd sql* commands:

infacmd sql Command	Privilege Group	Privilege Name	Permission On...
ExecuteSQL	n/a	n/a	Based on objects that you want to access in your SQL statement
ListColumnPermissions	n/a	n/a	n/a
ListSQLDataServiceOptions	n/a	n/a	n/a
ListSQLDataServicePermissions	n/a	n/a	n/a

infacmd sql Command	Privilege Group	Privilege Name	Permission On...
ListSQLDataServices	n/a	n/a	n/a
ListStoredProcedurePermissions	n/a	n/a	n/a
ListTableOptions	n/a	n/a	n/a
ListTablePermissions	n/a	n/a	n/a
PurgeTableCache	n/a	n/a	n/a
RefreshTableCache	n/a	n/a	n/a
RenameSQLDataService	Application Administration	Manage Applications	n/a
SetColumnPermissions	n/a	n/a	Grant on the object
SetSQLDataServicePermissions	n/a	n/a	Grant on the object
SetStoredProcedurePermissions	n/a	n/a	Grant on the object
SetTablePermissions	n/a	n/a	Grant on the object
StartSQLDataService	Application Administration	Manage Applications	n/a
StopSQLDataService	Application Administration	Manage Applications	n/a
UpdateColumnOptions	Application Administration	Manage Applications	n/a
UpdateSQLDataServiceOptions	Application Administration	Manage Applications	n/a
UpdateTableOptions	Application Administration	Manage Applications	n/a

pmcmd Commands

To run the following *pmcmd* commands, users must have the listed sets of PowerCenter Repository Service privileges and PowerCenter repository object permissions.

The following table lists the required privileges and permissions for *pmcmd* commands:

pmcmd Command	Privilege Group	Privilege Name	Permission
aborttask (started by own user account)*	n/a	n/a	Read and Execute on folder
aborttask (started by other users)*	Run-time Objects	Manage Execution	Read and Execute on folder
abortworkflow (started by own user account)*	n/a	n/a	Read and Execute on folder
abortworkflow (started by other users)*	Run-time Objects	Manage Execution	Read and Execute on folder
connect	n/a	n/a	n/a
disconnect	n/a	n/a	n/a
exit	n/a	n/a	n/a
getrunningsessionsdetails*	Run-time Objects	Monitor	n/a
getservicedetails*	Run-time Objects	Monitor	Read on folder
getserviceproperties	n/a	n/a	n/a
getsessionstatistics*	Run-time Objects	Monitor	Read on folder
gettaskdetails*	Run-time Objects	Monitor	Read on folder
getworkflowdetails*	Run-time Objects	Monitor	Read on folder
help	n/a	n/a	n/a
pingservice	n/a	n/a	n/a
recoverworkflow (started by own user account)*	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile**
recoverworkflow (started by other users)*	Run-time Objects	Manage Execution	Read and Execute on folder Read and Execute on connection object Permission on operating system profile**
scheduleworkflow*	Run-time Objects	Manage Execution	Read and Execute on folder Read and Execute on connection object Permission on operating system profile**
setfolder	n/a	n/a	Read on folder

pmcmd Command	Privilege Group	Privilege Name	Permission
setnowait	n/a	n/a	n/a
setwait	n/a	n/a	n/a
showsettings	n/a	n/a	n/a
startask*	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile**
startworkflow*	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile**
stoptask (started by own user account)*	n/a	n/a	Read and Execute on folder
stoptask (started by other users)*	Run-time Objects	Manage Execution	Read and Execute on folder
stopworkflow (started by own user account)*	n/a	n/a	Read and Execute on folder
stopworkflow (started by other users)*	Run-time Objects	Manage Execution	Read and Execute on folder
unscheduleworkflow*	Run-time Objects	Manage Execution	Read and Execute on folder
unsetfolder	n/a	n/a	Read on folder
version	n/a	n/a	n/a
waittask	Run-time Objects	Monitor	Read on folder
waitworkflow	Run-time Objects	Monitor	Read on folder

*When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter Repository Service.
**If the PowerCenter Integration Service uses operating system profiles, users must have permission on the operating system profile.

pmrep Commands

Users must have the Access Repository Manager privilege to run all *pmrep* commands except for the following commands:

- Run
- Create

- Restore
- Upgrade
- Version
- Help

To run the following *pmrep* commands, users must have one of the listed sets of domain privileges, PowerCenter Repository Service privileges, domain object permissions, and PowerCenter repository object permissions.

The following table lists the required privileges and permissions for *pmrep* commands:

pmrep Command	Privilege Group	Privilege Name	Permission
AddToDeploymentGroup	Global Objects	Manage Deployment Groups	Read on original folder Read and Write on deployment group
ApplyLabel	n/a	n/a	Read on folder Read and Execute on label
AssignPermission*	n/a	n/a	n/a
BackUp	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ChangeOwner*	n/a	n/a	n/a
CheckIn (for your own checkouts)	Design Objects	Create, Edit, and Delete	Read and Write on folder
	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
CheckIn (for others' checkouts)	Design Objects	Manage Versions	Read and Write on folder
	Sources and Targets	Manage Versions	Read and Write on folder
	Run-time Objects	Manage Versions	Read and Write on folder
CleanUp	n/a	n/a	n/a
ClearDeploymentGroup	Global Objects	Manage Deployment Groups	Read and Write on deployment group
Connect	n/a	n/a	n/a
Create	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
CreateConnection	Global Objects	Create Connections	n/a
CreateDeploymentGroup	Global Objects	Manage Deployment Groups	n/a
CreateFolder	Folders	Create	n/a
CreateLabel	Global Objects	Create Labels	n/a

pmrep Command	Privilege Group	Privilege Name	Permission
Delete	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
DeleteConnection*	n/a	n/a	n/a
DeleteDeploymentGroup*	n/a	n/a	n/a
DeleteFolder*	n/a	n/a	n/a
DeleteLabel*	n/a	n/a	n/a
DeleteObject	Design Objects	Create, Edit, and Delete	Read and Write on folder
	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
DeployDeploymentGroup	Global Objects	Manage Deployment Groups	Read on original folder Read and Write on destination folder Read and Execute on deployment group
DeployFolder	Folders	Copy on original repository Create on destination repository	Read on folder
ExecuteQuery	n/a	n/a	Read and Execute on query
Exit	n/a	n/a	n/a
FindCheckout	n/a	n/a	Read on folder
GetConnectionDetails	n/a	n/a	Read on connection object
Help	n/a	n/a	n/a
KillUserConnection	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ListConnections	n/a	n/a	Read on connection object
ListObjectDependencies	n/a	n/a	Read on folder
ListObjects	n/a	n/a	Read on folder
ListTablesBySess	n/a	n/a	Read on folder
ListUserConnections	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ModifyFolder (to change owner, configure permissions, designate the folder as	n/a	n/a	n/a

pmrep Command	Privilege Group	Privilege Name	Permission
shared, or edit the folder name or description)*			
ModifyFolder (to change status)	Folders	Manage Versions	Read and Write on folder
Notify	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ObjectExport	n/a	n/a	Read on folder
ObjectImport	Design Objects	Create, Edit, and Delete	Read and Write on folder
	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
PurgeVersion (to purge objects at the repository level)	Design Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
	Sources and Targets	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
	Run-time Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
PurgeVersion (to purge objects at the folder level)	Design Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
	Sources and Targets	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
	Run-time Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
	Folders	Manage Versions	Read and Write on folder
Register	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
RegisterPlugin	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
Restore	Domain Administration	Manage Services	Permission on PowerCenter Repository Service

pmrep Command	Privilege Group	Privilege Name	Permission
RollbackDeployment	Global Objects	Manage Deployment Groups	Read and Write on destination folder
Run	n/a	n/a	n/a
ShowConnectionInfo	n/a	n/a	n/a
SwitchConnection	Run-time Objects	Create, Edit, and Delete	Read and Write on folder Read on connection object
TruncateLog	Run-time Objects	Manage Execution	Read and Execute on folder
UndoCheckout (for your own checkouts)	Design Objects	Create, Edit, and Delete	Read and Write on folder
	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UndoCheckout (for others' checkouts)	Design Objects	Manage Versions	Read and Write on folder
	Sources and Targets	Manage Versions	Read and Write on folder
	Run-time Objects	Manage Versions	Read and Write on folder
Unregister	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
UnregisterPlugin	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
UpdateConnection	n/a	n/a	Read and Write on connection object
UpdateEmailAddr	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UpdateSeqGenVals	Design Objects	Create, Edit, and Delete	Read and Write on folder
UpdateSrcPrefix	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UpdateStatistics	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
UpdateTargPrefix	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
Upgrade	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
Validate	Design Objects	Create, Edit, and Delete	Read and Write on folder
	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
Version	n/a	n/a	n/a
*The object owner or a user assigned the Administrator role for the PowerCenter Repository Service can run these commands.			

APPENDIX C

Custom Roles

This appendix includes the following topics:

- PowerCenter Repository Service Custom Roles, 475
- Metadata Manager Service Custom Roles, 476
- Reporting Service Custom Roles, 477

PowerCenter Repository Service Custom Roles

The following table lists the default privileges assigned to each PowerCenter Repository Service custom role:

Custom Role	Privilege Group	Privilege Name
PowerCenter Connection Administrator	Tools	- Access Workflow Manager
	Global Objects	- Create Connections
PowerCenter Developer	Tools	- Access Designer - Access Workflow Manager - Access Workflow Monitor
	Design Objects	- Create, Edit, and Delete - Manage Versions
	Sources and Targets	- Create, Edit, and Delete - Manage Versions
	Run-time Objects	- Create, Edit, and Delete - Execute - Manage Versions - Monitor
PowerCenterOperator	Tools	- Access Workflow Monitor
	Run-time Objects	- Execute - Manage Execution - Monitor
PowerCenter Repository Folder Administrator	Tools	- Access Repository Manager

Custom Role	Privilege Group	Privilege Name
	Folders	- Copy - Create - Manage Versions
	Global Objects	- Manage Deployment Groups - Execute Deployment Groups - Create Labels - Create Queries

Metadata Manager Service Custom Roles

The following table lists the default privileges assigned to each Metadata Manager Service custom role:

Custom Role	Privilege Group	Privilege Name
Metadata Manager Advanced User	Catalog	- Share Shortcuts - View Lineage - View Related Catalogs - View Reports - View Profile Results - View Catalog - View Relationships - Manage Relationships - View Comments - Post Comments - Delete Comments - View Links - Manage Links - View Glossary - Draft/Propose Business Terms - Manage Glossary - Manage Objects
	Load	- View Resource - Load Resource - Manage Schedules - Purge Metadata - Manage Resource
	Model	- View Model - Manage Model - Export/Import Models
	Security	- Manage Catalog Permissions
Metadata Manager Basic User	Catalog	- View Lineage - View Related Catalogs - View Catalog - View Relationships - View Comments - View Links

Custom Role	Privilege Group	Privilege Name
	Model	- View Model
Metadata Manager Intermediate User	Catalog	- View Lineage - View Related Catalogs - View Reports - View Profile Results - View Catalog - View Relationships - View Comments - Post Comments - Delete Comments - View Links - Manage Links - View Glossary
	Load	- View Resource - Load Resource
	Model	- View Model

Reporting Service Custom Roles

The following table lists the default privileges assigned to each Reporting Service custom role:

Custom Role	Privilege Group	Privilege Name
Reporting Service Advanced Consumer	Administration	- Maintain Schema - Export/Import XML Files - Manage User Access - Set Up Schedules and Tasks - Manage System Properties - Set Up Query Limits - Configure Real-time Message Streams
	Alerts	- Receive Alerts - Create Real-time Alerts - Set up Delivery Options
	Communication	- Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback

Custom Role	Privilege Group	Privilege Name
	Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
	Dashboard	- View Dashboards - Manage Personal Dashboards
	Indicators	- Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
	Manage Accounts	- Manage Personal Settings
	Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports
Reporting Service Advanced Provider	Administration	- Maintain Schema
	Alerts	- Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
	Communication	- Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
	Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
	Dashboards	- View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation - Access Advanced Dashboard Creation

Custom Role	Privilege Group	Privilege Name
	Indicators	- Interact With Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
	Manage Accounts	- Manage Personal Settings
	Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports
Reporting Service Basic Consumer	Alerts	- Receive Alerts - Set Up Delivery Options
	Communication	- Print - Email Object Links - Export - View Discussions - Add Discussions - Give Feedback
	Content Directory	- Access Content Directory
	Dashboards	- View Dashboards
	Manage Account	- Manage Personal Settings
	Reports	- View Reports - Analyze Reports
Reporting Service Basic Provider	Administration	- Maintain Schema
	Alerts	- Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
	Communication	- Print - Email Object Links - Email Object Contents - Export - Export To Excel or CSV - Export To Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback

Custom Role	Privilege Group	Privilege Name
	Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
	Dashboards	- View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation
	Indicators	- Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
	Manage Accounts	- Manage Personal Settings
	Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports
Reporting Service Intermediate Consumer	Alerts	- Receive Alerts - Set Up Delivery Options
	Communication	- Print - Email Object Links - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
	Content Directory	- Access Content Directory
	Dashboards	- View Dashboards - Manage Personal Dashboards
	Indicators	- Interact with Indicators - Get Continuous, Automatic Real-time Indicator Updates
	Manage Accounts	- Manage Personal Settings

Custom Role	Privilege Group	Privilege Name
	Reports	- View Reports - Analyze Reports - Interact with Data - View Life Cycle Metadata - Save Copy of Reports
Reporting Service Read Only Consumer	Reports	- View Reports
Reporting Service Schema Designer	Administration	- Maintain Schema - Set Up Schedules and Tasks - Configure Real-time Message Streams
	Alerts	- Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
	Communication	- Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
	Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
	Dashboards	- View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards
	Indicators	- Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
	Manage Accounts	- Manage Personal Settings
	Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

APPENDIX D

Repository Database Configuration for PowerCenter

This appendix includes the following topics:

- Repository Database Configuration Overview, 482
- Guidelines for Setting Up Database User Accounts, 482
- PowerCenter Repository Database Requirements, 483
- Data Analyzer Repository Database Requirements, 484
- Metadata Manager Repository Database Requirements, 485

Repository Database Configuration Overview

PowerCenter stores data and metadata in repositories in the domain. Before you create the PowerCenter application services, set up the databases and database user accounts for the repositories.

You can create the repositories in the following relational database systems:

- Oracle
- IBM DB2
- Microsoft SQL Server
- Sybase ASE

For more information about configuring the database, see the documentation for your database system.

Set up a database and user account for the following repositories:

- PowerCenter repository
- Data Analyzer repository
- Metadata Manager repository

Guidelines for Setting Up Database User Accounts

Use the following rules and guidelines when you set up the user accounts:

- The database must be accessible to all gateway nodes in the Informatica domain.

- The database user account must have permissions to create and drop tables, indexes, and views, and to select, insert, update, and delete data from tables.
- Use 7-bit ASCII to create the password for the account.
- To prevent database errors in one repository from affecting other repositories, create each repository in a separate database schema with a different database user account. Do not create the a repository in the same database schema as the domain configuration repository or the other repositories in the domain.

PowerCenter Repository Database Requirements

Verify that the configuration of the database meets the requirements of the PowerCenter repository.

Oracle

Use the following guidelines when you set up the repository on Oracle:

- Set the storage size for the tablespace to a small number to prevent the repository from using an excessive amount of space. Also verify that the default tablespace for the user that owns the repository tables is set to a small size.
  The following example shows how to set the recommended storage parameter for a tablespace named REPOSITORY.

  ```
  ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS UNLIMITED
  PCTINCREASE 50 );
  ```

  Verify or change these parameters before you create the repository.
- The database user account must have the CONNECT, RESOURCE, and CREATE VIEW privileges.

IBM DB2

To optimize repository performance, set up the database with the tablespace on a single node. When the tablespace is on one node, PowerCenter Client and PowerCenter Integration Service access the repository faster than if the repository tables exist on different database nodes.

Specify the single-node tablespace name when you create, copy, or restore a repository. If you do not specify the tablespace name, DB2 uses the default tablespace.

Sybase ASE

Use the following guidelines when you set up the repository on Sybase ASE:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Set the following database options to TRUE:

  - allow nulls by default

  - ddl in tran
- Verify the database user has CREATE TABLE and CREATE VIEW privileges.

- Set the database memory configuration requirements. The following table lists the memory configuration requirements and the recommended baseline values:

Database Configuration	Sybase System Procedure	Value
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	8000
Number of locks	sp_configure "number of locks"	100000

Adjust the above recommended values according to operations that are performed on the database.

Data Analyzer Repository Database Requirements

Verify that the configuration of the database meets the requirements of the Data Analyzer repository.

Oracle

Use the following guidelines when you set up the repository on Oracle:

- Set the storage size for the tablespace to a small number to prevent the repository from using an excessive amount of space. Also verify that the default tablespace for the user that owns the repository tables is set to a small size.
  The following example shows how to set the recommended storage parameter for a tablespace named REPOSITORY.

```
ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS UNLIMITED
PCTINCREASE 50 );
```

  Verify or change these parameters before you create the repository.
- The database user account must have the CONNECT, RESOURCE, and CREATE VIEW privileges.

Microsoft SQL Server

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- If you create the repository in Microsoft SQL Server 2005, Microsoft SQL Server must be installed with case-sensitive collation.
- If you create the repository in Microsoft SQL Server 2005, the repository database must have a database compatibility level of 80 or earlier. Data Analyzer uses non-ANSI SQL statements that Microsoft SQL Server supports only on a database with a compatibility level of 80 or earlier.

  To set the database compatibility level to 80, run the following query against the database:

```
sp_dbcmptlevel '<DatabaseName>', 80
```

  Or open the Microsoft SQL Server Enterprise Manager, right-click the database, and select Properties > Options. Set the compatibility level to 80 and click OK.

Sybase ASE

Use the following guidelines when you set up the repository on Sybase ASE:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
  The database for the Data Analyzer repository requires a page size of at least 8 KB. If you set up a Data Analyzer database on a Sybase ASE instance with a page size smaller than 8 KB, Data Analyzer can generate errors when you run reports. Sybase ASE relaxes the row size restriction when you increase the page size.

  Data Analyzer includes a GROUP BY clause in the SQL query for the report. When you run the report, Sybase ASE stores all GROUP BY and aggregate columns in a temporary worktable. The maximum index row size of the worktable is limited by the database page size. For example, if Sybase ASE is installed with the default page size of 2 KB, the index row size cannot exceed 600 bytes. However, the GROUP BY clause in the SQL query for most Data Analyzer reports generates an index row size larger than 600 bytes.
- Verify the database user has CREATE TABLE and CREATE VIEW privileges.
- Enable the Distributed Transaction Management (DTM) option on the database server.
- Create a DTM user account and grant the dtm_tm_role to the user. The following table lists the DTM configuration setting for the dtm_tm_role value:

DTM Configuration	Sybase System Procedure	Value
Distributed Transaction Management privilege	sp_role "grant"	dtm_tm_role, *username*

Metadata Manager Repository Database Requirements

Verify that the configuration of the database meets the requirements of the Metadata Manager repository.

Oracle

Use the following guidelines when you set up the repository on Oracle:

- Set the following parameters for the tablespace:

Property	Setting	Oracle Version	Notes
pga_aggregate_target	100 - 200 MB	All	Configure pga_aggregate_target and sort_area_size in ora.init.
sort_area_size	50 MB	Oracle 9i	Configure pga_aggregate_target and sort_area_size in ora.init.
Temp tablespace (minimum requirement)	2 GB	All	
Rollback/undo tablespace	1 - 2 GB	All	Undo is available in Oracle 10g and higher.

- If the repository must store metadata in a multibyte language, set the NLS_LENGTH_SEMANTICS parameter to CHAR on the database instance. Default is BYTE.
- The database user account must have the RESOURCE privilege.

IBM DB2

Use the following guidelines when you set up the repository on IBM DB2:

- Set up system temporary tablespaces larger than the default page size of 4 KB and update the heap sizes. Queries running against tables in tablespaces defined with a page size larger than 4 KB require system temporary tablespaces with a page size larger than 4 KB. If there are no system temporary table spaces defined with a larger page size, the queries can fail. The server displays the following error:

  ```
  SQL 1585N A system temporary table space with sufficient page size does not exist. SQLSTATE=54048
  ```

  Create system temporary tablespaces with page sizes of 8 KB, 16 KB, and 32 KB. Run the following SQL statements on each database to configure the system temporary tablespaces and update the heap sizes:

  ```
  CREATE Bufferpool RBF IMMEDIATE  SIZE 1000 PAGESIZE 32 K  EXTENDED STORAGE ;
  CREATE Bufferpool STBF IMMEDIATE  SIZE 2000 PAGESIZE 32 K  EXTENDED STORAGE ;
  CREATE REGULAR  TABLESPACE REGTS32 PAGESIZE 32 K  MANAGED BY SYSTEM  USING ('C:
  \DB2\NODE0000\reg32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE 0.33 BUFFERPOOL RBF;
  CREATE  SYSTEM TEMPORARY  TABLESPACE TEMP32 PAGESIZE 32 K  MANAGED BY SYSTEM  USING ('C:
  \DB2\NODE0000\temp32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE 0.33 BUFFERPOOL
  STBF;
  GRANT USE OF TABLESPACE REGTS32 TO USER <USERNAME>;
  UPDATE DB CFG FOR <DB NAME> USING APP_CTL_HEAP_SZ 16384
  UPDATE DB CFG FOR <DB NAME> USING APPLHEAPSZ 16384
  UPDATE DBM CFG USING QUERY_HEAP_SZ 8000
  UPDATE DB CFG FOR <DB NAME> USING LOGPRIMARY 100
  UPDATE DB CFG FOR <DB NAME> USING LOGFILSIZ 2000
  UPDATE DB CFG FOR <DB NAME> USING LOCKLIST 1000
  UPDATE DB CFG FOR <DB NAME> USING DBHEAP 2400
  "FORCE APPLICATIONS ALL"
  DB2STOP
  DB2START
  ```

- Set the locking parameters to avoid deadlocks when you load metadata into a Metadata Manager repository on IBM DB2.
  You can configure the following locking parameters:

Parameter Name	Value	IBM DB2 Description
LOCKLIST	8192	Max storage for lock list (4KB)
MAXLOCKS	10	Percent of lock lists per application
LOCKTIMEOUT	300	Lock timeout (sec)
DLCHKTIME	10000	Interval for checking deadlock (ms)

  Also, set the DB2_RR_TO_RS parameter to YES to change the read policy from Repeatable Read to Read Stability.

Note: If you use IBM DB2 as a metadata source, the source database has the same configuration requirements.

Microsoft SQL Server

If the repository must store metadata in a multibyte language, set the database collation to that multibyte language when you install Microsoft SQL Server.

Note: You cannot change the database collation after you set it.

APPENDIX E

PowerCenter Platform Connectivity

This appendix includes the following topics:

- Connectivity Overview, 487
- Domain Connectivity, 488
- PowerCenter Connectivity, 488
- Native Connectivity, 492
- ODBC Connectivity, 492
- JDBC Connectivity, 493

Connectivity Overview

The Informatica platform uses the following types of connectivity communicate between clients, services, and other components in the domain:

- **TCP/IP network protocol.** Application services and the Service Managers in a domain use TCP/IP network protocol to communicate with other nodes and services. The clients also use TCP/IP to communicate with application services. You can configure the host name and port number for TCP/IP communication on a node when you install the Informatica services. You can configure the port numbers used for services on a node when during installation or in the Administrator tool.
- **Native drivers**. The PowerCenter Integration Service and the PowerCenter Repository Service use native drivers to communicate with databases. Native drivers are packaged with the database server and client software. Install and configure native database client software on the machines where the PowerCenter Integration Service and the PowerCenter Repository Service run.
- **ODBC**. The ODBC drivers are installed with the Informatica services and the Informatica clients. The integration services use ODBC drivers to communicate with databases.
- **JDBC.** The Reporting Service uses JDBC to connect to the Data Analyzer repository and data sources. The Metadata Manager Service uses JDBC to connect to the Metadata Manager repository and metadata source repositories.

  The server installer uses JDBC to connect to the domain configuration repository during installation. The gateway nodes in the Informatica domain use JDBC to connect to the domain configuration repository.

Domain Connectivity

Services on a node in an Informatica domain use TCP/IP to connect to services on other nodes. Because services can run on multiple nodes in the domain, services rely on the Service Manager to route requests. The Service Manager on the master gateway node handles requests for services and responds with the address of the requested service.

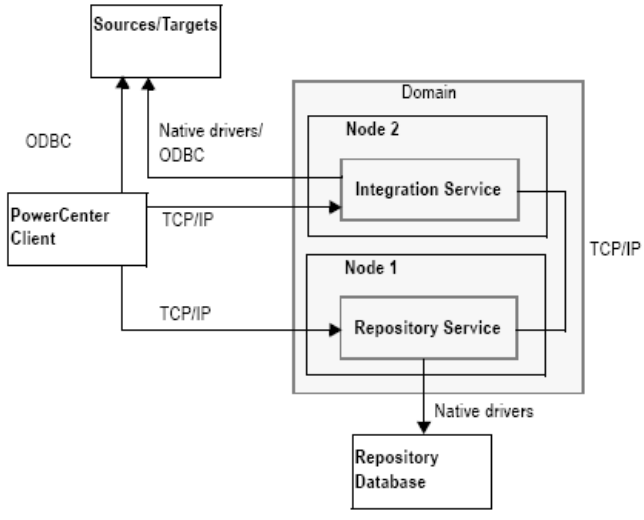
Nodes communicate through TCP/IP on the port you select for a node when you install Informatica Services. When you create a node, you select a port number for the node. The Service Manager listens for incoming TCP/IP connections on that port.

PowerCenter Connectivity

PowerCenter uses the TCP/IP network protocol, native database drivers, ODBC, and JDBC for communication between the following PowerCenter components:

- **PowerCenter Repository Service.** The PowerCenter Repository Service uses native database drivers to communicate with the PowerCenter repository. The PowerCenter Repository Service uses TCP/IP to communicate with other PowerCenter components.
- **PowerCenter Integration Service.** The PowerCenter Integration Service uses native database connectivity and ODBC to connect to source and target databases. The PowerCenter Integration Service uses TCP/IP to communicate with other PowerCenter components.
- **Reporting Service and Metadata Manager Service.** Data Analyzer and Metadata Manager use JDBC and ODBC to access data sources and repositories.
- **PowerCenter Client.** PowerCenter Client uses ODBC to connect to source and target databases. PowerCenter Client uses native protocol to communicate with the PowerCenter Repository Service and PowerCenter Integration Service.

The following figure shows an overview of PowerCenter components and connectivity:



The following table lists the drivers used by PowerCenter components:

Component	Database	Driver
PowerCenter Repository Service	PowerCenter Repository	Native
PowerCenter Integration Service	Source Target Stored Procedure Lookup	Native ODBC
Reporting Service	Data Analyzer Repository	JDBC
Reporting Service	Data Source	JDBC ODBC with JDBC-ODBC bridge
Metadata Manager Service	Metadata Manager Repository	JDBC
PowerCenter Client	PowerCenter Repository	Native
PowerCenter Client	Source Target Stored Procedure Lookup	ODBC
Custom Metadata Configurator (Metadata Manager client)	Metadata Manager Repository	JDBC

Repository Service Connectivity

The PowerCenter Repository Service manages the metadata in the PowerCenter repository database. All applications that connect to the repository must connect to the PowerCenter Repository Service. The PowerCenter Repository Service uses native drivers to communicate with the repository database.

The following table describes the connectivity required to connect the Repository Service to the repository and source and target databases:

Repository Service Connection	Connectivity Requirement
PowerCenter Client	TCP/IP
PowerCenter Integration Service	TCP/IP
PowerCenter Repository database	Native database drivers

The PowerCenter Integration Service connects to the Repository Service to retrieve metadata when it runs workflows.

Connecting from PowerCenter Client

To connect to the PowerCenter Repository Service from PowerCenter Client, add a domain and repository in the PowerCenter Client tool. When you connect to the repository from a PowerCenter Client tool, the client tool sends a connection request to the Service Manager on the gateway node. The Service Manager returns the host name and port number of the node where the PowerCenter Repository Service runs. PowerCenter Client uses TCP/IP to connect to the PowerCenter Repository Service.

Connecting to Databases

To set up a connection from the PowerCenter Repository Service to the repository database, configure the database properties in the Administrator tool. You must install and configure the native database drivers for the repository database on the machine where the PowerCenter Repository Service runs.

Integration Service Connectivity

The PowerCenter Integration Service connects to the repository to read repository objects. The PowerCenter Integration Service connects to the repository through the PowerCenter Repository Service. Use the Administrator tool to configure an associated repository for the Integration Service.

The following table describes the connectivity required to connect the PowerCenter Integration Service to the platform components, source databases, and target databases:

PowerCenter Integration Service Connection	Connectivity Requirement
PowerCenter Client	TCP/IP
Other PowerCenter Integration Service Processes	TCP/IP
Repository Service	TCP/IP
Source and target databases	Native database drivers or ODBC **Note:** The PowerCenter Integration Service on Windows and UNIX can use ODBC drivers to connect to databases. You can use native drivers to improve performance.

The PowerCenter Integration Service includes ODBC libraries that you can use to connect to other ODBC sources. The Informatica installation includes ODBC drivers.

For flat file, XML, or COBOL sources, you can either access data with network connections, such as NFS, or transfer data to the PowerCenter Integration Service node through FTP software. For information about connectivity software for other ODBC sources, refer to your database documentation.

Connecting from the PowerCenter Client

The Workflow Manager communicates with a PowerCenter Integration Service process over a TCP/IP connection. The Workflow Manager communicates with the PowerCenter Integration Service process each time you start a workflow or display workflow details.

Connecting to the PowerCenter Repository Service

When you create a PowerCenter Integration Service, you specify the PowerCenter Repository Service to associate with the PowerCenter Integration Service. When the PowerCenter Integration Service runs a workflow, it uses TCP/IP to connect to the associated PowerCenter Repository Service and retrieve metadata.

Connecting to Databases

Use the Workflow Manager to create connections to databases. You can create connections using native database drivers or ODBC. If you use native drivers, specify the database user name, password, and native connection string for each connection. The PowerCenter Integration Service uses this information to connect to the database when it runs the session.

Note: PowerCenter supports ODBC drivers, such as ISG Navigator, that do not need user names and passwords to connect. To avoid using empty strings or nulls, use the reserved words PmNullUser and PmNullPasswd for the user name and password when you configure a database connection. The PowerCenter Integration Service treats PmNullUser and PmNullPasswd as no user and no password.

PowerCenter Client Connectivity

The PowerCenter Client uses ODBC drivers and native database client connectivity software to communicate with databases. It uses TCP/IP to communicate with the Integration Service and with the repository.

The following table describes the connectivity types required to connect the PowerCenter Client to the Integration Service, repository, and source and target databases:

PowerCenter Client Connection	Connectivity Requirement
Integration Service	TCP/IP
Repository Service	TCP/IP
Databases	ODBC connection for each database

Connecting to the Repository

You can connect to the repository using the PowerCenter Client tools. All PowerCenter Client tools use TCP/IP to connect to the repository through the Repository Service each time you access the repository to perform tasks such as connecting to the repository, creating repository objects, and running object queries.

Connecting to Databases

To connect to databases from the Designer, use the Windows ODBC Data Source Administrator to create a data source for each database you want to access. Select the data source names in the Designer when you perform the following tasks:

- **Import a table or a stored procedure definition from a database.** Use the Source Analyzer or Target Designer to import the table from a database. Use the Transformation Developer, Mapplet Designer, or Mapping Designer to import a stored procedure or a table for a Lookup transformation.

  To connect to the database, you must also provide your database user name, password, and table or stored procedure owner name.
- **Preview data.** You can select the data source name when you preview data in the Source Analyzer or Target Designer. You must also provide your database user name, password, and table owner name.

Connecting to the Integration Service

The Workflow Manager and Workflow Monitor communicate directly with the Integration Service over TCP/IP each time you perform session and workflow-related tasks, such as running a workflow. When you log in to a repository through the Workflow Manager or Workflow Monitor, the client application lists the Integration Services that are configured for that repository in the Administrator tool.

Reporting Service and Metadata Manager Service Connectivity

To connect to a Data Analyzer repository, the Reporting Service requires a Java Database Connectivity (JDBC) driver. To connect to the data source, the Reporting Service can use a JDBC driver or a JDBC-ODBC bridge with an ODBC driver.

To connect to a Metadata Manager repository, the Metadata Manager Service requires a JDBC driver. The Custom Metadata Configurator uses a JDBC driver to connect to the Metadata Manager repository.

JDBC drivers are installed with the Informatica services and the Informatica clients. You can use the installed JDBC drivers to connect to the Data Analyzer or Metadata Manager repository, data source, or to a PowerCenter repository.

The Informatica installers do not install ODBC drivers or the JDBC-ODBC bridge for the Reporting Service or Metadata Manager Service.

Native Connectivity

To establish native connectivity between an application service and a database, you must install the database client software on the machine where the service runs.

The PowerCenter Integration Service and PowerCenter Repository Service use native drivers to communicate with source and target databases and repository databases.

The following table describes the syntax for the native connection string for each supported database system:

Database	Connect String Syntax	Example
IBM DB2	*dbname*	mydatabase
Informix	*dbname*@*servername*	mydatabase@informix
Microsoft SQL Server	*servername*@*dbname*	sqlserver@mydatabase
Oracle	*dbname*.world (same as TNSNAMES entry)	oracle.world
Sybase ASE	*servername*@*dbname*	sambrown@mydatabase **Note:** Sybase ASE servername is the name of the Adaptive Server from the interfaces file.
Teradata	*ODBC_data_source_name* or *ODBC_data_source_name*@*db_name* or *ODBC_data_source_name*@*db_user_name*	TeradataODBC TeradataODBC@mydatabase TeradataODBC@sambrown **Note:** Use Teradata ODBC drivers to connect to source and target databases.

ODBC Connectivity

Open Database Connectivity (ODBC) provides a common way to communicate with different database systems.

PowerCenter Client uses ODBC drivers to connect to source, target, and lookup databases and call the stored procedures in databases. The PowerCenter Integration Service can also use ODBC drivers to connect to databases.

To use ODBC connectivity, you must install the following components on the machine hosting the Informatica service or client tool:

- **Database client software.** Install the client software for the database system. This installs the client libraries needed to connect to the database.

  Note: Some ODBC drivers contain wire protocols and do not require the database client software.

- **ODBC drivers.** The DataDirect closed 32-bit ODBC drivers are installed when you install the Informaica services or the Informatica clients. The database server can also include an ODBC driver.

After you install the necessary components you must configure an ODBC data source for each database that you want to connect to. A data source contains information that you need to locate and access the database, such as database name, user name, and database password. On Windows, you use the ODBC Data Source Administrator to create a data source name. On UNIX, you add data source entries to the odbc.ini file found in the system $ODBCHOME directory.

When you create an ODBC data source, you must also specify the driver that the ODBC driver manager sends database calls to.

The following table shows the recommended ODBC drivers to use with each database:

Database	ODBC Driver	Requires Database Client Software
IBM DB2	IBM ODBC driver	Yes
Informix	DataDirect 32-bit closed ODBC driver	No
Microsoft Access	Microsoft Access driver	No
Microsoft Excel	Microsoft Excel driver	No
Microsoft SQL Server	Microsoft SQL Server ODBC driver	No
Oracle	DataDirect 32-bit closed ODBC driver	No
Sybase ASE	DataDirect 32-bit closed ODBC driver	No
Teradata	Teradata ODBC driver	Yes
HP Neoview	HP ODBC driver	No
Netezza	Netezza SQL	Yes

JDBC Connectivity

JDBC (Java Database Connectivity) is a Java API that provides connectivity to relational databases. Java-based applications can use JDBC drivers to connect to databases.

The following services and clients use JDBC to connect to databases:

- Metadata Manager Service

- Reporting Service
- Custom Metadata Configurator

JDBC drivers are installed with the Informatica services and the Informatica clients.

APPENDIX F

Connecting to Databases in PowerCenter from Windows

This appendix includes the following topics:

- Connecting to Databases from Windows Overview, 495
- Connecting to an IBM DB2 Universal Database, 495
- Connecting to Microsoft Access and Microsoft Excel, 496
- Connecting to a Microsoft SQL Server Database, 497
- Connecting to an Oracle Database, 498
- Connecting to a Sybase ASE Database, 499
- Connecting to a Teradata Database, 500
- Connecting to a Neoview Database, 501
- Connecting to a Netezza Database, 502

Connecting to Databases from Windows Overview

To use native connectivity, you must install and configure the database client software for the database you want to access. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries. To improve performance, use native connectivity.

The Informatica installation includes DataDirect ODBC drivers. If you have existing ODBC data sources created with an earlier version of the drivers, you must create new ODBC data sources using the new drivers. Configure ODBC connections using the DataDirect ODBC drivers provided by Informatica or third-party ODBC drivers that are Level 2 compliant or higher.

Connecting to an IBM DB2 Universal Database

For native connectivity, install the version of IBM DB2 Client Application Enabler (CAE) appropriate for the IBM DB2 database server version. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Configuring Native Connectivity

Use the following procedure as a guideline to configure native connectivity. For specific connectivity instructions, see the database documentation.

To connect to an IBM DB2 database:

1. Verify that the following environment variable settings have been established by DB2 Client Application Enabler:

```
DB2HOME=C:\SQLLIB (directory where the client is installed)
DB2INSTANCE = DB2
DB2CODEPAGE = 437 (Sometimes required. Use only if you encounter problems. Depends on the locale,
you may use other values.)
```

2. Verify that the PATH environment variable includes the DB2 bin directory. For example:

```
PATH=C:\WINNT\SYSTEM32;C:\SQLLIB\BIN;...
```

3. Configure the IBM DB2 client to connect to the database that you want to access.
   - Launch the Client Configuration Assistant.
   - Add the database connection and BIND the connection.
4. Verify that you can connect to the DB2 database.

   Run the following command in the DB2 Command Line Processor:

```
CONNECT TO <dbalias> USER <username> USING <password>
```

   If the connection is successful, disconnect and clean up with the TERMINATE command. If the connection fails, see the database documentation.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure ODBC. For specific connectivity instructions, see the database documentation.

To connect to an IBM DB2 database using ODBC:

1. Install the IBM DB2 Client Application Enabler (CAE) and configure native connectivity.
2. Create an ODBC data source using the driver provided by IBM. Do not use the DataDirect 32-bit closed ODBC driver for DB2 provided by Informatica.

   For specific instructions on creating an ODBC data source using the IBM DB2 ODBC driver, see the database documentation.
3. Verify that you can connect to the DB2 database using the ODBC data source. If the connection fails, see the database documentation.

Connecting to Microsoft Access and Microsoft Excel

Configure connectivity to the following Informatica components on Windows:

- **PowerCenter Integration Service.** Install Microsoft Access or Excel on the machine where the PowerCenter Integration Service processes run. Create an ODBC data source for the Microsoft Access or Excel data you want to access.
- **PowerCenter Client.** Install Microsoft Access or Excel on the machine hosting the PowerCenter Client. Create an ODBC data source for the Microsoft Access or Excel data you want to access.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the Microsoft Access or Excel documentation.

To connect to an Access or Excel database:

1. Create an ODBC data source using the driver provided by Microsoft.
2. To avoid using empty string or nulls, use the reserved words PmNullUser for the user name and PmNullPasswd for the password when you create a database connection in the Workflow Manager.

Connecting to a Microsoft SQL Server Database

For native connectivity, install SQL Client, including the Microsoft OLE DB provider for Microsoft SQL Server. Verify that the version of of SQL Client is compatible with your Microsoft SQL Server version. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Configuring Native Connectivity

Use the following procedure as a guideline to configure native connectivity. For specific connectivity instructions, see the database documentation.

To connect to a Microsoft SQL Server database:

1. Verify that the Microsoft SQL Server home directory is set.
2. Verify that the PATH environment variable includes the Microsoft SQL Server directory.

   For example:

   ```
   PATH=C:\MSSQL\BIN;C:\MSSQL\BINN;....
   ```

3. Configure the Microsoft SQL Server client to connect to the database that you want to access.

   Launch the Client Network Utility. On the General tab, verify that the Default Network Library matches the default network for the Microsoft SQL Server database.

4. Verify that you can connect to the Microsoft SQL Server database.

   To connect to the database, launch ISQL_w, and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure ODBC. For specific connectivity instructions, see the Microsoft SQL Server documentation.

To connect to a Microsoft SQL Server database using ODBC:

1. Install the Microsoft SQL Server client and configure native connectivity.
2. Create an ODBC data source using the driver provided by Microsoft.

   Do not use the DataDirect 32-bit closed ODBC driver for Microsoft SQL Server provided by Informatica.

   To ensure consistent data in Microsoft SQL Server repositories, clear the Create temporary stored procedures for prepared SQL statements option in the Create a New Data Source to SQL Server dialog box.

If you have difficulty clearing the temporary stored procedures for prepared SQL statements options, see the Informatica Knowledge Base for more information about configuring Microsoft SQL Server. Access the Knowledge Base at http://my.informatica.com.

3. Verify that you can connect to the Microsoft SQL Server database using the ODBC data source. If the connection fails, see the database documentation.

Connecting to an Oracle Database

For native connectivity, install the version of Oracle client appropriate for the Oracle database server version. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

Note: If you use the DataDirect ODBC driver provided by Informatica, you do not need the database client. The ODBC wire protocols do not require the database client software to connect to the database.

Configuring Native Connectivity

Use the following procedure as a guideline to configure native connectivity using Oracle Net Services or Net8. For specific connectivity instructions, see the database documentation.

To connect to an Oracle database:

1. Verify that the Oracle home directory is set.

   For example:

   ```
   ORACLE_HOME=C:\Oracle
   ```

2. Verify that the PATH environment variable includes the Oracle bin directory.

   For example, if you install Net8, the path might include the following entry:

   ```
   PATH=C:\ORANT\BIN;
   ```

3. Configure the Oracle client to connect to the database that you want to access.

   Launch SQL*Net Easy Configuration Utility or edit an existing tnsnames.ora file to the home directory and modify it.

   The tnsnames.ora file is stored in the $ORACLE_HOME\network\admin directory.

   Enter the correct syntax for the Oracle connect string, typically *databasename* .world. Make sure the SID entered here matches the database server instance ID defined on the Oracle server.

   Following is a sample tnsnames.ora. You need to enter the information for the database.

   ```
   mydatabase.world =
      (DESCRIPTION
      (ADDRESS_LIST =
           (ADDRESS =
              (COMMUNITY = mycompany.world
              (PROTOCOL = TCP)
              (Host = mymachine)
              (Port = 1521)
           )
      )
      (CONNECT_DATA =
         (SID = MYORA7)
         (GLOBAL_NAMES = mydatabase.world)
   ```

4. Set the NLS_LANG environment variable to the locale (language, territory, and character set) you want the database client and server to use with the login.

   The value of this variable depends on the configuration. For example, if the value is american_america.UTF8, you must set the variable as follows:

   ```
   NLS_LANG=american_america.UTF8;
   ```

   To determine the value of this variable, contact the database administrator.

5. Verify that you can connect to the Oracle database.

   To connect to the database, launch SQL*Plus and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   Use the connect string as defined in tnsnames.ora.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure ODBC. For specific connectivity instructions, see the database documentation.

To connect to an Oracle database using ODBC:

1. Create an ODBC data source using the DataDirect ODBC driver for Oracle provided by Informatica.
2. Verify that you can connect to the Oracle database using the ODBC data source.

If PowerCenter Client does not accurately display non-ASCII characters, set the NLS_LANG environment variable to the locale that you want the database client and server to use with the login.

The value of this variable depends on the configuration. For example, if the value is american_america.UTF8, you must set the variable as follows:

```
NLS_LANG=american_america.UTF8;
```

To determine the value of this variable, contact the database administrator.

Connecting to a Sybase ASE Database

For native connectivity, install the version of Open Client appropriate for your database version. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

If you want to create, restore, or upgrade a Sybase ASE repository, set *allow nulls by default* to TRUE at the database level. Setting this option changes the default null type of the column to null in compliance with the SQL standard.

Note: If you use the DataDirect ODBC driver provided by Informatica, you do not need the database client. The ODBC wire protocols do not require the database client software to connect to the database.

Configuring Native Connectivity

Use the following procedure as a guideline to configure native connectivity. For specific connectivity instructions, see the database documentation.

To connect to a Sybase ASE database:

1. Verify that the SYBASE environment variable refers to the Sybase ASE directory.

   For example:

   ```
   SYBASE=C:\SYBASE
   ```

2. Verify that the PATH environment variable includes the Sybase ASE directory.

   For example:

   ```
   PATH=C:\SYBASE\BIN;C:\SYBASE\DLL
   ```

3. Configure Sybase Open Client to connect to the database that you want to access.

   Use SQLEDIT to configure the Sybase client, or copy an existing SQL.INI file (located in the %SYBASE%\INI directory) and make any necessary changes.

   Select NLWNSCK as the Net-Library driver and include the Sybase ASE server name.

   Enter the host name and port number for the Sybase ASE server. If you do not know the host name and port number, check with the system administrator.

4. Verify that you can connect to the Sybase ASE database.

   To connect to the database, launch ISQL and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   User names and database names are case sensitive.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure ODBC. For specific connectivity instructions, see the database documentation.

To connect to a Sybase ASE database using ODBC:

1. Create an ODBC data source using the DataDirect 32-bit closed ODBC driver for Sybase provided by Informatica.
2. On the Performance tab, set Prepare Method to 2-Full. This ensures consistent data in the repository, optimizes performance, and reduces overhead on tempdb.
3. Verify that you can connect to the Sybase ASE database using the ODBC data source.

Connecting to a Teradata Database

Install and configure native client software on the machines where the Data Integration Service process runs and where you install Informatica Developer. To ensure compatibility between the Informatica products and databases, use 32-bit database client libraries only. You must configure connectivity to the following Informatica components on Windows:

- **PowerCenter Integration Service.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on the machine where the PowerCenter Integration Service process runs. You must also configure ODBC connectivity.
- **PowerCenter Client.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on each PowerCenter Client machine that accesses Teradata. Use the Workflow Manager to create a database connection object for the Teradata database.

Note: Based on a recommendation from Teradata, Informatica uses ODBC to connect to Teradata. ODBC is a native interface for Teradata. To process Teradata bigint data, use the Teradata ODBC driver version 03.06.00.02 or later.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

To connect to a Teradata database:

1. Create an ODBC data source for each Teradata database that you want to access.

   To create the ODBC data source, use the driver provided by Teradata.

   Create a System DSN if you start the Informatica service with a *Local System account* logon. Create a User DSN if you select the *This account* log in option to start the Informatica service.

2. Enter the name for the new ODBC data source and the name of the Teradata server or its IP address.

   To configure a connection to a single Teradata database, enter the DefaultDatabase name. To create a single connection to the default database, enter the user name and password. To connect to multiple databases, using the same ODBC data source, leave the DefaultDatabase field and the user name and password fields empty.

3. Configure Date Options in the Options dialog box.

   In the Teradata Options dialog box, specify AAA for DateTime Format.

4. Configure Session Mode in the Options dialog box.

   When you create a target data source, choose ANSI session mode. If you choose ANSI session mode, Teradata does not roll back the transaction when it encounters a row error. If you choose Teradata session mode, Teradata rolls back the transaction when it encounters a row error. In Teradata mode, the Integration Service cannot detect the rollback and does not report this in the session log.

5. Verify that you can connect to the Teradata database.

   To test the connection, use a Teradata client program, such as WinDDI, BTEQ, Teradata Administrator, or Teradata SQL Assistant.

Connecting to a Neoview Database

Install and configure ODBC on the machines where the PowerCenter Integration Service process runs and where you install PowerCenter Client. You must configure connectivity to the following Informatica components on Windows:

- **PowerCenter Integration Service.** Install the HP ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity.
- **PowerCenter Client.** Install the HP ODBC driver on each PowerCenter Client machine that accesses the Neoview database. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity. Use the Workflow Manager to create a database connection object for the Neoview database.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

1. Create an ODBC data source for each Neoview database that you want to access.

   To create the ODBC data source, use the driver provided by HP.

   Create a System DSN if you start the Informatica service with a Local System account logon. Create a User DSN if you select the This account log in option to start the Informatica service.

   After you create the data source, configure the properties of the data source.
2. Enter a name for the new ODBC data source.
3. Enter the IP address and port number for the HP Neoview server.

   Optionally, you can configure DSN properties such as Login Timeout, Connection Timeout, Query Timeout, and Fetch Buffer Size.
4. Enter the name of the Neoview schema where you plan to to create database objects.
5. Configure the character set.

   Set Client/Server Character Set Interaction to System_Default so that client uses the character set configured for the client locale.
6. Configure the path and file name for the ODBC log file.
7. Verify that you can connect to the Neoview database.

   You can use the Microsoft ODBC Data Source Administrator to test the connection to the database. To test the connection, select the Neoview data source and click Configure. On the Testing tab, click Test Connection and enter the connection information for the Neoview schema.

Connecting to a Netezza Database

Install and configure ODBC on the machines where the PowerCenter Integration Service process runs and where you install PowerCenter Client. You must configure connectivity to the following Informatica components on Windows:

- **PowerCenter Integration Service.** Install the Netezza ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity.
- **PowerCenter Client.** Install the Netezza ODBC driver on each PowerCenter Client machine that accesses the Netezza database. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity. Use the Workflow Manager to create a database connection object for the Netezza database.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

1. Create an ODBC data source for each Netezza database that you want to access.

   To create the ODBC data source, use the driver provided by Netezza.

   Create a System DSN if you start the Informatica service with a Local System account logon. Create a User DSN if you select the This account log in option to start the Informatica service.

   After you create the data source, configure the properties of the data source.
2. Enter a name for the new ODBC data source.
3. Enter the IP address/host name and port number for the Netezza server.
4. Enter the name of the Netezza schema where you plan to create database objects.
5. Configure the path and file name for the ODBC log file.
6. Verify that you can connect to the Netezza database.

   You can use the Microsoft ODBC Data Source Administrator to test the connection to the database. To test the connection, select the Netezza data source and click Configure. On the Testing tab, click Test Connection and enter the connection information for the Netezza schema.

APPENDIX G

Connecting to Databases in PowerCenter from UNIX

This appendix includes the following topics:

- Connecting to Databases from UNIX Overview, 504
- Connecting to Microsoft SQL Server, 505
- Connecting to an IBM DB2 Universal Database, 505
- Connecting to an Informix Database, 507
- Connecting to an Oracle Database, 509
- Connecting to a Sybase ASE Database, 512
- Connecting to a Teradata Database, 513
- Connecting to a Neoview Database, 516
- Connecting to a Netezza Database, 518
- Connecting to an ODBC Data Source, 521
- Sample odbc.ini File, 523

Connecting to Databases from UNIX Overview

To use native connectivity, you must install and configure the database client software for the database you want to access. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries. To improve performance, use native connectivity.

The Informatica installation includes DataDirect ODBC drivers. If you have existing ODBC data sources created with an earlier version of the drivers, you must create new ODBC data sources using the new drivers. Configure ODBC connections using the DataDirect ODBC drivers provided by Informatica or third-party ODBC drivers that are Level 2 compliant or higher.

Use the following guidelines when you connect to databases from Linux;

- Use native drivers to connect to IBM DB2, Oracle, or Sybase ASE databases
- Use ODBC to connect to Informix. The Informix client is not available on Linux.
- You can use ODBC to connect to other sources and targets.

Connecting to Microsoft SQL Server

Use ODBC to connect to a Microsoft SQL Server database from a UNIX machine.

Connecting to an IBM DB2 Universal Database

For native connectivity, install the version of IBM DB2 Client Application Enabler (CAE) appropriate for the IBM DB2 database server version. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Configuring Native Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

To connect to a DB2 database:

1. To configure connectivity on the machine where the PowerCenter Integration Service or Repository Service process runs, log in to the machine as a user who can start a service process.
2. Set the DB2INSTANCE, INSTHOME, DB2DIR, and PATH environment variables.

   The UNIX IBM DB2 software always has an associated user login, often db2admin, which serves as a holder for database configurations. This user holds the instance for DB2.

   DB2INSTANCE. The name of the instance holder.

   Using a Bourne shell:

   ```
   $ DB2INSTANCE=db2admin; export DB2INSTANCE
   ```

   Using a C shell:

   ```
   $ setenv DB2INSTANCE db2admin
   ```

   INSTHOME. This is db2admin home directory path.

   Using a Bourne shell:

   ```
   $ INSTHOME=~db2admin
   ```

   Using a C shell:

   ```
   $ setenv INSTHOME ~db2admin>
   ```

   DB2DIR. Set the variable to point to the IBM DB2 CAE installation directory. For example, if the client is installed in the /opt/IBMdb2/v6.1 directory:

   Using a Bourne shell:

   ```
   $ DB2DIR=/opt/IBMdb2/v6.1; export DB2DIR
   ```

   Using a C shell:

   ```
   $ setenv DB2DIR /opt/IBMdb2/v6.1
   ```

   PATH. To run the IBM DB2 command line programs, set the variable to include the DB2 bin directory.

   Using a Bourne shell:

   ```
   $ PATH=${PATH}:$DB2DIR/bin; export PATH
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:$DB2DIR/bin
   ```
3. Set the shared library variable to include the DB2 lib directory.

The IBM DB2 client software contains a number of shared library components that the PowerCenter Integration Service and Repository Service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

The shared library path must also include the Informatica installation directory *(server_dir)*.

Set the shared library environment variable based on the operating system. The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH
HP-UX	SHLIB_PATH

For example, use the following syntax for Solaris and Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib; export LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib
```

For HP-UX:

- Using a Bourne shell:

```
$ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$DB2DIR/lib; export SHLIB_PATH
```

- Using a C shell:

```
$ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$DB2DIR/lib
```

For AIX:

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$DB2DIR/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$DB2DIR/lib
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

5. If the DB2 database resides on the same machine on which PowerCenter Integration Service or Repository Service processes run, configure the DB2 instance as a remote instance.

   Run the following command to verify if there is a remote entry for the database:

   ```
   DB2 LIST DATABASE DIRECTORY
   ```

   The command lists all the databases that the DB2 client can access and their configuration properties. If this command lists an entry for “Directory entry type” of “Remote,” skip to step 6.

If the database is not configured as remote, run the following command to verify whether a TCP/IP node is cataloged for the host:

```
DB2 LIST NODE DIRECTORY
```

If the node name is empty, you can create one when you set up a remote database. Use the following command to set up a remote database and, if needed, create a node:

```
db2 CATALOG TCPIP NODE <nodename> REMOTE <hostname_or_address> SERVER <port number>
```

Run the following command to catalog the database:

```
db2 CATALOG DATABASE <dbname> as <dbalias> at NODE <nodename>
```

For more information about these commands, see the database documentation.

6. Verify that you can connect to the DB2 database. Run the DB2 Command Line Processor and run the command:

```
CONNECT TO <dbalias> USER <username> USING <password>
```

If the connection is successful, clean up with the `CONNECT RESET` or `TERMINATE` command.

Connecting to an Informix Database

For native connectivity, install ESQL for C, Informix Client SDK, or any other Informix client software. Also, install compatible versions of ESQL/runtime or iconnect. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install the ESQL/C version that is compatible with the Informix database server. To verify compatibility, contact Informix.

Note: If you use the DataDirect ODBC driver provided by Informatica, you do not need the database client. The ODBC wire protocols do not require the database client software to connect to the database.

Configuring Native Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

To connect to an Informix database:

1. To configure connectivity for the Integration Service process, log in to the machine as a user who can start the server process.
2. Set the INFORMIXDIR, INFORMIXSERVER, DBMONEY, and PATH environment variables.

   INFORMIXDIR. Set the variable to the directory where the database client is installed. For example, if the client is installed in the /databases/informix directory:

   Using a Bourne shell:

   ```
   $ INFORMIXDIR=/databases/informix; export INFORMIXDIR
   ```

   Using a C shell:

   ```
   $ setenv INFORMIXDIR /databases/informix
   ```

   INFORMIXSERVER. Set the variable to the name of the server. For example, if the name of the Informix server is INFSERVER:

   Using a Bourne shell:

   ```
   $ INFORMIXSERVER=INFSERVER; export INFORMIXSERVER
   ```

Using a C shell:

```
$ setenv INFORMIXSERVER INFSERVER
```

DBMONEY. Set the variable so Informix does not prefix the data with the dollar sign ($) for money datatypes.

Using a Bourne shell:

```
$ DBMONEY=' .'; export DBMONEY
```

Using a C shell:

```
$ setenv DBMONEY=' .'
```

PATH. To run the Informix command line programs, set the variable to include the Informix bin directory.

Using a Bourne shell:

```
$ PATH=${PATH}:$INFORMIXDIR/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:$INFORMIXDIR/bin
```

3. Set the shared library path to include the Informix lib directory.

   The Informix client software contains a number of shared library components that the Integration Service process loads dynamically. To locate the shared libraries during run time, set the shared library environment variable.

   The shared library path must also include the Informatica installation directory *(server_dir)*.

   Set the shared library environment variable based on the operating system. The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH
HP-UX	SHLIB_PATH

   For example, use the following syntax for Solaris:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$INFORMIXDIR/lib: $INFORMIXDIR/lib/esql;
     export LD_LIBRARY_PATH
     ```

   - Using a C shell:

     ```
     $ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$INFORMIXDIR/lib:$INFORMIXDIR/lib/
     esql
     ```

   For HP-UX:

   - Using a Bourne shell:

     ```
     $ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$INFORMIXDIR/lib:$INFORMIXDIR/lib/esql; export
     SHLIB_PATH
     ```

   - Using a C shell:

     ```
     $ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$INFORMIXDIR/lib:$INFORMIXDIR/lib/esql
     ```

   For AIX:

   - Using a Bourne shell:

     ```
     $ LIBPATH=${LIBPATH}:$HOME/server_dir:$INFORMIXDIR/lib:$INFORMIXDIR/lib/esql; export LIBPATH
     ```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$INFORMIXDIR/lib:$INFORMIXDIR/lib/esql
```

4. Optionally, set the $ONCONFIG environment variable to the Informix configuration file name.
5. If you plan to call Informix stored procedures in mappings, set all of the date parameters to the Informix datatype Datetime year to fraction(5).
6. Make sure the DBDATE environment variable is *not* set.

   For example, to check if DBDATE is set, you might enter the following at a UNIX prompt:

   ```
   $ env | grep -i DBDATE
   ```

   If DBDATE=MDY2/ appears, unset DBDATE by typing:

   ```
   $ unsetenv DBDATE
   ```

7. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

8. Verify that the Informix server name is defined in the $INFORMIXDIR/etc/sqlhosts file.
9. Verify that the Service (last column entry for the server named in the sqlhosts file) is defined in the services file (usually /etc/services).

   If not, define the Informix Services name in the Services file.

   Enter the Services name and port number. The default port number is 1525, which should work in most cases.

   For more information, see the Informix and UNIX documentation.

10. Verify that you can connect to the Informix database.

    If you fail to connect to the database, verify that you have correctly entered all the information.

Connecting to an Oracle Database

For native connectivity, install the version of Oracle client appropriate for the Oracle database server version. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

Configuring Native Connectivity

Use the following procedure as a guideline to connect to an Oracle database through Oracle Net Services or Net8. For specific connectivity instructions, see the database documentation.

To connect to an Oracle database:

1. To configure connectivity for the PowerCenter Integration Service or Repository Service process, log in to the machine as a user who can start the server process.
2. Set the ORACLE_HOME, NLS_LANG, TNS_ADMIN, and PATH environment variables.

ORACLE_HOME. Set the variable to the Oracle client installation directory. For example, if the client is installed in the /HOME2/oracle directory:

Using a Bourne shell:

```
$ ORACLE_HOME=/HOME2/oracle; export ORACLE_HOME
```

Using a C shell:

```
$ setenv ORACLE_HOME /HOME2/oracle
```

NLS_LANG. Set the variable to the locale (language, territory, and character set) you want the database client and server to use with the login. The value of this variable depends on the configuration. For example, if the value is american_america.UTF8, you must set the variable as follows:

Using a Bourne shell:

```
$ NLS_LANG=american_america.UTF8; export NLS_LANG
```

Using a C shell:

```
$ NLS_LANG american_america.UTF8
```

To determine the value of this variable, contact the Administrator.

TNS_ADMIN. Set the variable to the directory where the tnsnames.ora file resides. For example, if the file is in the /HOME2/oracle/network/admin directory:

Using a Bourne shell:

```
$ TNS_ADMIN=$HOME2/oracle/network/admin; export TNS_ADMIN
```

Using a C shell:

```
$ setenv TNS_ADMIN=$HOME2/oracle/network/admin
```

Setting the TNS_ADMIN is optional, and might vary depending on the configuration.

PATH. To run the Oracle command line programs, set the variable to include the Oracle bin directory.

Using a Bourne shell:

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

3. Set the shared library environment variable.

   The Oracle client software contains a number of shared library components that the PowerCenter Integration Service and Repository Service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

   The shared library path must also include the Informatica installation directory *(server_dir)* .

   Set the shared library environment variable based on the operating system. The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH
HP-UX	SHLIB_PATH

For example, use the following syntax for Solaris and Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
```

For HP-UX

- Using a Bourne shell:

```
$ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export SHLIB_PATH
```

- Using a C shell:

```
$ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ORACLE_HOME/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ORACLE_HOME/lib
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

5. Verify that the Oracle client is configured to access the database.

   Use the SQL*Net Easy Configuration Utility or copy an existing tnsnames.ora file to the home directory and modify it.

   The tnsnames.ora file is stored in the $ORACLE_HOME/network/admin directory.

   Enter the correct syntax for the Oracle connect string, typically *databasename* .world.

   Here is a sample tnsnames.ora. You need to enter the information for the database.

   ```
   mydatabase.world =
      (DESCRIPTION
      (ADDRESS_LIST =
           (ADDRESS =
              (COMMUNITY = mycompany.world
              (PROTOCOL = TCP)
              (Host = mymachine)
              (Port = 1521)
           )
      )
      (CONNECT_DATA =
         (SID = MYORA7)
         (GLOBAL_NAMES = mydatabase.world)
   ```

6. Verify that you can connect to the Oracle database.

   To connect to the Oracle database, launch SQL*Plus and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   Enter the user name and connect string as defined in tnsnames.ora.

Connecting to a Sybase ASE Database

For native connectivity, install the version of Open Client appropriate for your database version. For ODBC connectivity, use the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

If you want to create, restore, or upgrade a Sybase ASE repository, set *allow nulls by default* to TRUE at the database level. Setting this option changes the default null type of the column to null in compliance with the SQL standard.

Configuring Native Connectivity

Use the following procedure as a guideline to connect to a Sybase ASE database. For specific connectivity instructions, see the database documentation.

To connect to a Sybase ASE database:

1. To configure connectivity to the Integration Service or Repository Service, log in to the machine as a user who can start the server process.
2. Set the SYBASE and PATH environment variables.

   SYBASE. Set the variable to the Sybase Open Client installation directory. For example if the client is installed in the /usr/sybase directory:

   Using a Bourne shell:

   ```
   $ SYBASE=/usr/sybase; export SYBASE
   ```

   Using a C shell:

   ```
   $ setenv SYBASE /usr/sybase
   ```

   PATH. To run the Sybase command line programs, set the variable to include the Sybase bin directory.

   Using a Bourne shell:

   ```
   $ PATH=${PATH}:/usr/sybase/bin; export PATH
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:/usr/sybase/bin
   ```
3. Set the shared library environment variable.

   The Sybase Open Client software contains a number of shared library components that the Integration Service and the Repository Service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

   The shared library path must also include the installation directory of the Informatica services *(server_dir)* .

   Set the shared library environment variable based on the operating system. The following table describes the shared library variables for each operating system.

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH

Operating System	Variable
AIX	LIBPATH
HP-UX	SHLIB_PATH

For example, use the following syntax for Solaris and Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$SYBASE/lib; export LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$SYBASE/lib
```

For HP-UX

- Using a Bourne shell:

```
$ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$SYBASE/lib; export SHLIB_PATH
```

- Using a C shell:

```
$ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$SYBASE/lib
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$SYBASE/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$SYBASE/lib
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

5. Verify the Sybase ASE server name in the Sybase interfaces file stored in the $SYBASE directory.
6. Verify that you can connect to the Sybase ASE database.

   To connect to the Sybase ASE database, launch ISQL and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   User names and database names are case sensitive.

Connecting to a Teradata Database

Install and configure native client software on the machines where the Data Integration Service process runs and where you install Informatica Developer. To ensure compatibility between the Informatica products and databases, use 32-bit database client libraries only. You must configure connectivity to the following Informatica components on Windows:

- **PowerCenter Integration Service.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on the machine where the PowerCenter Integration Service process runs. You must also configure ODBC connectivity.

- **PowerCenter Client.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on each PowerCenter Client machine that accesses Teradata. Use the Workflow Manager to create a database connection object for the Teradata database.

Note: Based on a recommendation from Teradata, Informatica uses ODBC to connect to Teradata. ODBC is a native interface for Teradata. To process Teradata bigint data, use the Teradata ODBC driver version 03.06.00.02 or later.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

To connect to a Teradata database on UNIX:

1. To configure connectivity for the integration service process, log in to the machine as a user who can start a service process.
2. Set the TERADATA_HOME, ODBCHOME, and PATH environment variables.

   TERADATA_HOME. Set the variable to the Teradata driver installation directory. The defaults are as follows:

   Using a Bourne shell:

   ```
   $ TERADATA_HOME=/teradata/usr; export TERADATA_HOME
   ```

   Using a C shell:

   ```
   $ setenv TERADATA_HOME /teradata/usr
   ```

   ODBCHOME. Set the variable to the ODBC installation directory. For example:

   Using a Bourne shell:

   ```
   $ ODBCHOME=/usr/odbc; export ODBCHOME
   ```

   Using a C shell:

   ```
   $ setenv ODBCHOME /usr/odbc
   ```

   PATH. To run the *ivtestlib* utility, to verify that the UNIX ODBC manager can load the driver files, set the variable as follows:

   Using a Bourne shell:

   ```
   PATH="${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin"
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin
   ```

3. Set the shared library environment variable.

   The Teradata software contains a number of shared library components that the integration service process loads dynamically. To locate the shared libraries during run time, set the shared library environment variable.

   The shared library path must also include installation directory of the the Informatica service *(server_dir)* .

   Set the shared library environment variable based on the operating system. The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH

Operating System	Variable
AIX	LIBPATH
HP-UX	SHLIB_PATH

For example, use the following syntax for Solaris:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:
$TERADATA_HOME/lib:$TERADATA_HOME/odbc/lib";
export LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/lib:
$TERADATA_HOME/odbc/lib"
```

For HP-UX

- Using a Bourne shell:

```
$ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib; export SHLIB_PATH
```

- Using a C shell:

```
$ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

   This file exists in $ODBCHOME directory.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

   Add an entry for the Teradata data source under the section [ODBC Data Sources] and configure the data source.

   For example:

```
MY_TERADATA_SOURCE=Teradata Driver
[MY_TERADATA_SOURCE]
Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=208.199.59.208
DateTimeFormat=AAA
SessionMode=ANSI
DefaultDatabase=
Username=
Password=
```

5. Set the DateTimeFormat to AAA in the Teradata data ODBC configuration.
6. Optionally, set the SessionMode to ANSI. When you use ANSI session mode, Teradata does not roll back the transaction when it encounters a row error.

   If you choose Teradata session mode, Teradata rolls back the transaction when it encounters a row error. In Teradata mode, the integration service process cannot detect the rollback, and does not report this in the session log.

7. To configure connection to a single Teradata database, enter the DefaultDatabase name. To create a single connection to the default database, enter the user name and password. To connect to multiple databases, using the same ODBC DSN, leave the DefaultDatabase field empty.

   For more information about Teradata connectivity, see the Teradata ODBC driver documentation.

8. Verify that the last entry in the odbc.ini is InstallDir and set it to the odbc installation directory.

   For example:

   ```
   InstallDir=/usr/odbc
   ```

9. Edit the .cshrc or .profile to include the complete set of shell commands.
10. Save the file and either log out and log in again, or run the source command.

    Using a Bourne shell:

    ```
    $ source .profile
    ```

    Using a C shell:

    ```
    $ source .cshrc
    ```

11. For each data source you use, make a note of the file name under the Driver=<parameter> in the data source entry in odbc.ini. Use the *ivtestlib* utility to verify that the UNIX ODBC manager can load the driver file.

    For example, if you have the driver entry:

    ```
    Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
    ```

    run the following command:

    ```
    ivtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
    ```

12. Test the connection using BTEQ or another Teradata client tool.

Connecting to a Neoview Database

Install and configure HP ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the DataDirect Driver Manager in the DataDirect driver package shipped with the Informatica product to configure the Neoview data source details in the odbc.ini file.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

To connect to a Neoview database on UNIX:

1. To configure connectivity for the integration service process, log in to the machine as a user who can start a service process.
2. Set the ODBCHOME and PATH environment variables.

   ODBCHOME. Set the variable to the ODBC installation directory. For example:

   Using a Bourne shell:

   ```
   $ ODBCHOME=/usr/odbc; export ODBCHOME
   ```

   Using a C shell:

   ```
   $ setenv ODBCHOME /usr/odbc
   ```

   PATH. Set the variable to the ODBCHOME/bin directory. For example:

Using a Bourne shell:

```
PATH="${PATH}:$ODBCHOME/bin"
```

Using a C shell:

```
$ setenv PATH ${PATH}:$ODBCHOME/bin
```

3. Set the shared library environment variable.

   The shared library path must contain the ODBC libraries. It must also include the Informatica services installation directory `(server_dir)`.

   Set the shared library environment variable based on the operating system. The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH
HP-UX	SHLIB_PATH

   For example, use the following syntax for Solaris:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib”

     export LD_LIBRARY_PATH
     ```

   - Using a C shell:

     ```
     $ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib"
     ```

   For HP-UX

   - Using a Bourne shell:

     ```
     $ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib; export SHLIB_PATH
     ```

   - Using a C shell:

     ```
     $ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib
     ```

   For AIX

   - Using a Bourne shell:

     ```
     $ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
     ```

   - Using a C shell:

     ```
     $ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
     ```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

   This file exists in $ODBCHOME directory.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

   Add an entry for the Neoview data source under the section [ODBC Data Sources] and configure the data source.

   For example:

   ```
   MY_NEOVIEW_SOURCE=HP ODBC Driver
   [MY_NEOVIEW_SOURCE]
   Driver=/export/home/adpqa/thirdparty/Neoview/lib64/libhpodbc_drvr64.so
   Catalog=NEO
   Schema=INFA
   ```

```
DataLang=0
FetchBufferSize=SYSTEM_DEFAULT
Server=TCP:10.1.41.221:18650
SQL_ATTR_CONNECTION_TIMEOUT=SYSTEM_DEFAULT
SQL_LOGIN_TIMEOUT=SYSTEM_DEFAULT
SQL_QUERY_TIMEOUT=NO_TIMEOUT
ServiceName=HP_DEFAULT_SERVICE
```

For more information about Neoview connectivity, see the HP ODBC driver documentation.

5. Verify that the last entry in the odbc.ini is InstallDir and set it to the odbc installation directory.

   For example:

   ```
   InstallDir=/usr/odbc
   ```

6. Edit the .cshrc or .profile to include the complete set of shell commands.
7. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

8. For each data source you use, make a note of the file name under the Driver=<parameter> in the data source entry in odbc.ini. Use the ddtestlib (under $ODBCHOME/bin) utility to verify that the UNIX ODBC manager can load the driver file.

   For example, if you have the following driver entry:

   ```
   Driver=/export/home/adpqa/thirdparty/Neoview/lib64/libhpodbc_drvr64.so
   ```

   Run the following command:

   ```
   ddtestlib /export/home/adpqa/thirdparty/Neoview/lib64/libhpodbc_drvr64.so
   ```

The following code shows an example of a Neoview entry in the odbc.ini file:

```
Admin_Load_DataSource=HP ODBC Driver
[Admin_Load_DataSource]
Driver=/export/home/adpqa/thirdparty/Neoview/lib64/libhpodbc_drvr64.so
Catalog=NEO
Schema=INFA
DataLang=0
FetchBufferSize=SYSTEM_DEFAULT
Server=TCP:10.1.41.221:18650
SQL_ATTR_CONNECTION_TIMEOUT=SYSTEM_DEFAULT
SQL_LOGIN_TIMEOUT=SYSTEM_DEFAULT
SQL_QUERY_TIMEOUT=NO_TIMEOUT
ServiceName=HP_DEFAULT_SERVICE
```

Connecting to a Netezza Database

Install and configure Netezza ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the DataDirect Driver Manager in the DataDirect driver package shipped with the Informatica product to configure the Netezza data source details in the odbc.ini file.

Configuring ODBC Connectivity

Use the following procedure as a guideline to configure connectivity. For specific connectivity instructions, see the database documentation.

To connect to a Netezza database on UNIX:

1. To configure connectivity for the integration service process, log in to the machine as a user who can start a service process.
2. Set the ODBCHOME, NZ_ODBC_INI_PATH, and PATH environment variables.

   ODBCHOME. Set the variable to the ODBC installation directory. For example:

   Using a Bourne shell:

   ```
   $ ODBCHOME=<Informatica server home>/ODBC6.1; export ODBCHOME
   ```

   Using a C shell:

   ```
   $ setenv ODBCHOME =<Informatica server home>/ODBC6.1
   ```

   PATH. Set the variable to the ODBCHOME/bin directory. For example:

   Using a Bourne shell:

   ```
   PATH="${PATH}:$ODBCHOME/bin"
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:$ODBCHOME/bin
   ```

   NZ_ODBC_INI_PATH. Set the variable to point to the directory that contains the odbc.ini file. For example, if the odbc.ini file is in the $ODBCHOME directory:

   Using a Bourne shell:

   ```
   NZ_ODBC_INI_PATH=$ODBCHOME; export NZ_ODBC_INI_PATH
   ```

   Using a C shell:

   ```
   $ setenv NZ_ODBC_INI_PATH $ODBCHOME
   ```

3. Set the shared library environment variable.

   The shared library path must contain the ODBC libraries. It must also include the Informatica services installation directory `(server_dir)`.

   Set the shared library environment variable based on the operating system. For 32-bit UNIX platforms, set the Netezza library folder to <NetezzaInstallationDir>/lib. For 64-bit UNIX platforms, set the Netezza library folder to <NetezzaInstallationDir>/lib64. The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH
HP-UX	SHLIB_PATH

   For example, use the following syntax for Solaris:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/
     lib64”
     export LD_LIBRARY_PATH
     ```

   - Using a C shell:

     ```
     $ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/
     lib:<NetezzaInstallationDir>/lib64"
     ```

For HP-UX

- Using a Bourne shell:

```
$ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64;
export SHLIB_PATH
```

- Using a C shell:

```
$ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64; export
LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

   This file exists in $ODBCHOME directory.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

   Add an entry for the Netezza data source under the section [ODBC Data Sources] and configure the data source.

   For example:

   ```
   [NZSQL]
   Driver = /export/home/appsqa/thirdparty/netezza/lib64/libnzodbc.so
   Description = NetezzaSQL ODBC
   Servername = netezza1.informatica.com
   Port = 5480
   Database = infa
   Username = admin
   Password = password
   Debuglogging = true
   StripCRLF = false
   PreFetch = 256
   Protocol = 7.0
   ReadOnly = false
   ShowSystemTables = false
   Socket = 16384
   DateFormat = 1
   TranslationDLL =
   TranslationName =
   TranslationOption =
   NumericAsChar = false
   ```

   For more information about Netezza connectivity, see the Netezza ODBC driver documentation.

5. Verify that the last entry in the odbc.ini file is InstallDir and set it to the ODBC installation directory.

   For example:

   ```
   InstallDir=/usr/odbc
   ```

6. Edit the .cshrc or .profile file to include the complete set of shell commands.
7. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

Connecting to an ODBC Data Source

Install and configure native client software on the machine where the PowerCenter Integration Service and PowerCenter Repository Service run. Also install and configure any underlying client access software required by the ODBC driver. To ensure compatibility between Informatica and the databases, use the appropriate database client libraries. To access sources on Windows, such as Microsoft Excel or Access, you must install PowerChannel.

The Informatica installation includes DataDirect ODBC drivers. If the odbc.ini file contains connections that use earlier versions of the ODBC driver, update the connection information to use the new drivers. Use the System DSN to specify an ODBC data source.

To connect to an ODBC data source:

1. On the machine where the PowerCenter Integration Service runs, log in as a user who can start a service process.
2. Set the ODBCHOME and PATH environment variables.

   ODBCHOME. Set to the DataDirect ODBC installation directory. For example, if the install directory is /opt/ODBC6.1.

   Using a Bourne shell:

   ```
   $ ODBCHOME=/opt/ODBC6.1; export ODBCHOME
   ```

   Using a C shell:

   ```
   $ setenv ODBCHOME /opt/ODBC6.1
   ```

   PATH. To run the ODBC command line programs, like *ivtestlib*, set the variable to include the odbc bin directory.

   Using a Bourne shell:

   ```
   $ PATH=${PATH}:$ODBCHOME/bin; export PATH
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:$ODBCHOME/bin
   ```

   Run the *ivtestlib* utility to verify that the UNIX ODBC manager can load the driver files.
3. Set the shared library environment variable.

   The ODBC software contains a number of shared library components that the service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

   The shared library path must also include the Informatica installation directory *(server_dir)*.

   Set the shared library environment variable based on the operating system. The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH
HP-UX	SHLIB_PATH

For example, use the following syntax for Solaris and Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib; export LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBCHOME:${LD_LIBRARY_PATH}
```

For HP-UX

- Using a Bourne shell:

```
$ SHLIB_PATH=${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib; export SHLIB_PATH
```

- Using a C shell:

```
$ setenv SHLIB_PATH ${SHLIB_PATH}:$HOME/server_dir:$ODBCHOME/lib
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

   This file exists in $ODBCHOME directory.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

   Add an entry for the ODBC data source under the section [ODBC Data Sources] and configure the data source.

   For example:

   ```
   MY_MSSQLSERVER_ODBC_SOURCE=<Driver name or Data source description>
   [MY_SQLSERVER_ODBC_SOURCE]
   Driver=<path to ODBC drivers>
   Description=DataDirect 6.1 SQL Server Wire Protocol
   Database=<SQLServer_database_name>
   LogonID=<username>
   Password=<password>
   Address=<TCP/IP address>,<port number>
   QuoteId=No
   AnsiNPW=No
   ApplicationsUsingThreads=1
   ```

   This file might already exist if you have configured one or more ODBC data sources.

5. Verify that the last entry in the odbc.ini is InstallDir and set it to the odbc installation directory.

   For example:

   ```
   InstallDir=/usr/odbc
   ```

6. If you use the odbc.ini file in the home directory, set the ODBCINI environment variable.

   Using a Bourne shell:

   ```
   $ ODBCINI=/$HOME/.odbc.ini; export ODBCINI
   ```

   Using a C shell:

   ```
   $ setenv ODBCINI $HOME/.odbc.ini
   ```

7. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

8. Use the *ivtestlib* utility to verify that the UNIX ODBC manager can load the driver file you specified for the data source in the odbc.ini file.

   For example, if you have the driver entry:

   ```
   Driver = /opt/odbc/lib/DWxxxx.so
   ```

   run the following command:

   ```
   ivtestlib /opt/odbc/lib/DWxxxx.so
   ```

9. Install and configure any underlying client access software needed by the ODBC driver.

   Note: While some ODBC drivers are self-contained and have all information inside the .odbc.ini file, most are not. For example, if you want to use an ODBC driver to access Oracle, you must install the Oracle SQL*NET software and set the appropriate environment variables. Verify such additional software configuration separately before using ODBC.

Sample odbc.ini File

```
[ODBC Data Sources]
DB2 Wire Protocol=DataDirect 6.1 DB2 Wire Protocol
Informix Wire Protocol=DataDirect 6.1 Informix Wire Protocol
Oracle Wire Protocol=DataDirect 6.1 Oracle Wire Protocol
Oracle=DataDirect 6.1 Oracle
SQLServer Wire Protocol=DataDirect 6.1 SQL Server Wire Protocol
Sybase Wire Protocol=DataDirect 6.1 Sybase Wire Protocol

[ODBC]
IANAAppCodePage=4
InstallDir=/home/ksuthan/odbc/61/solaris32/installed
Trace=0
TraceDll=/export/home/build_root/odbc_6.1/install/lib/DWtrc25.so
TraceFile=odbctrace.out
UseCursorLib=0

[DB2 Wire Protocol]
Driver=/export/home/build_root/odbc_6.1/install/lib/Dwdb225.so
Description=DataDirect 6.1 DB2 Wire Protocol
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationUsingThreads=1
CatalogSchema=
CharsetFor65535=0
#Collection applies to OS/390 and AS/400 only
Collection=
ConnectionRetryCount=0
ConnectionRetryDelay=3
#Database applies to DB2 UDB only
Database=<database_name>
DynamicSections=200
GrantAuthid=PUBLIC
GrantExecute=1
IpAddress=<DB2_server_host>
LoadBalancing=0
#Location applies to OS/390 and AS/400 only
Location=<location_name>
LogonID=
Password=
PackageOwner=
ReportCodePageConversionErrors=0
SecurityMechanism=0
TcpPort=<DB2_server_port>
UseCurrentSchema=1
WithHold=1

[Informix Wire Protocol]
Driver=/export/home/build_root/odbc_6.1/install/lib/Dwifcl25.so
```

```
Description=DataDirect 6.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ReportCodePageConversionErrors=0
ServerName=<Informix_server>
TrimBlankFromIndexName=1

[Test]
Driver=/export/home/build_root/odbc_6.1/install/lib/Dwora25.so
Description=DataDirect 6.1 Oracle Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ArraySize=60000
CachedCursorLimit=32
CachedDescLimit=0
CatalogIncludesSynonyms=1
CatalogOptions=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
DefaultLongDataBuffLen=1024
DescribeAtPrepare=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
HostName=hercules
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LogonID=ksuthan
Password=an3d45jk
PortNumber=1531
ProcedureRetResults=0
ReportCodePageConversionErrors=0
ServiceType=0
ServiceName=
SID=SUN10G
TimeEscapeMapping=0
UseCurrentSchema=1

[Oracle]
Driver=/export/home/build_root/odbc_6.1/install/lib/Dwor825.so
Description=DataDirect 6.1 Oracle
AlternateServers=
ApplicationUsingThreads=1
ArraySize=60000
CatalogIncludesSynonyms=1
CatalogOptions=0
ClientVersion=9iR2
ConnectionRetryCount=0
ConnectionRetryDelay=3
DefaultLongDataBuffLen=1024
DescribeAtPrepare=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LogonID=
OptimizeLongPerformance=0
Password=
ProcedureRetResults=0
ReportCodePageConversionErrors=0
```

```
ServerName=<Oracle_server>
TimestampEscapeMapping=0
UseCurrentSchema=1

[SQLServer Wire Protocol]
Driver=/export/home/build_root/odbc_6.1/install/lib/Dwmsss25.so
Description=DataDirect 6.1 SQL Server Wire Protocol
Address=<SQLServer_host, SQLServer_server_port>
AlternateServers=
AnsiNPW=Yes
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
LoadBalancing=0
LogonID=
Password=
QuotedId=No
ReportCodePageConversionErrors=0

[Sybase Wire Protocol]
Driver=/export/home/build_root/odbc_6.1/install/lib/Dwase25.so
Description=DataDirect 6.1 Sybase Wire Protocol
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
ArraySize=50
Charset=
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EnableQuotedIdentifiers=0
InitializationString=
Language=
LoadBalancing=0
LogonID=
NetworkAddress=<Sybase_host, Sybase_server_port>
OptimizePrepare=1
PacketSize=0
Password=
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
TruncateTimeTypeFractions=0
WorkStationID=
```

INDEX

A

Abort
  option to disable PowerCenter Integration Service 203
  option to disable PowerCenter Integration Service process 203
  option to disable the Web Services Hub 316
accounts
  changing the password 10
  managing 9
activity data
  Web Services Report 407
adaptive dispatch mode
  description 354
  overview 228
Additional JDBC Parameters
  description 194
address validation properties
  configuring 156
Administrator
  role 104
Administrator tool
  code page 426
  HTTPS, configuring 55
  log errors, viewing 376
  logging in 9
  logs, viewing 372
  reports 400
  SAP BW Service, configuring 309
  secure communication 55
administrators
  application client 59
  default 58
  domain 58
advanced profiling properties
  configuring 167
advanced properties
  Metadata Manager Service 196
  PowerCenter Integration Service 210
  PowerCenter Repository Service 264
  Web Services Hub 317, 319
Agent Cache Capacity (property)
  description 264
agent port
  description 193
AggregateTreatNullsAsZero
  option 212
  option override 212
AggregateTreatRowsAsInsert
  option 212
  option override 212
Aggregator transformation
  caches 237, 242
  treating nulls as zero 212
  treating rows as insert 212
alerts
  configuring 26
  description 2
  managing 26
  notification email 27
  subscribing to 26
  tracking 27
  viewing 27
Allow Writes With Agent Caching (property)
  description 264
Analyst Service
  Analyst Service security process properties 150
  application service 15
  Audit Trails 151
  creating 152
  custom service process properties 151
  environment variables 151
  log events 378
  Maximum Heap Size 150
  node process properties 150
  privileges 81
  process properties 149
  properties 147
anonymous login
  LDAP directory service 60
application
  backing up 184
  changing the name 182
  deploying 176
  enabling 182
  properties 176
  refreshing 185
application service process
  disabling 30
  enabling 30
  failed state 30
  port assignment 3
  standby state 30
  state 30
  stopped state 30
application services
  Analyst Service 15
  authorization 7
  Content Management Service 15
  Data Integration Service 15
  dependencies 42
  description 3
  disabling 30
  enabling 30
  licenses, assigning 362
  licenses, unassigning 363
  Metadata Manager Service 15
  Model Repository Service 15
  overview 15
  permissions 113
  PowerCenter Integration Service 15
  PowerCenter Repository Service 15
  PowerExchange Listener Service 15

PowerExchange Logger Service 15
removing 31
Reporting Service 15
resilience, configuring 134
SAP BW Service 15
secure communication 53
user synchronization 7
Web Services Hub 15
application sources
code page 428
application targets
code page 428
applications
monitoring 390
as
permissions by command 452
privileges by command 452
ASCII mode
ASCII data movement mode, setting 209
overview 238, 421
associated repository
Web Services Hub, adding to 321
Web Services Hub, editing for 322
associated Repository Service
new Integration Service 201
Web Services Hub 315, 321, 322
audit trails
creating 284
Authenticate MS-SQL User (property)
description 264
authentication
description 60
LDAP 7, 60
log events 377
native 7, 60
Service Manager 7
authorization
application services 7
Data Integration Service 7
log events 377
Metadata Manager Service 7
Model Repository Service 7
PowerCenter Repository Service 7
Reporting Service 7
Service Manager 2, 7
auto-select
network high availability 142
Average Service Time (property)
Web Services Report 407
Avg DTM Time (property)
Web Services Report 407
Avg. No. of Run Instances (property)
Web Services Report 407
Avg. No. of Service Partitions (property)
Web Services Report 407

B

backing up
domain configuration database 38
list of backup files 281
performance 284
repositories 280
backup directory
Model Repository Service 253
node property 33
backup node
license requirement 208
new Integration Service 201
node assignment, configuring 208
BackupDomain command
description 38
baseline system
CPU profile 357
basic dispatch mode
overview 228
blocking
description 233
blocking source data
PowerCenter Integration Service handling 233
Browse privilege group
description 83
buffer memory
buffer blocks 237
DTM process 237

C

Cache Connection
property 165
cache files
directory 220
overview 242
permissions 238
Cache Removal Time
property 165
caches
default directory 242
memory 237
memory usage 237
overview 238
transformation 242
case study
processing ISO 8859-1 data 434
processing Unicode UTF-8 data 436
catalina.out
troubleshooting 370
category
domain log events 377
certificate
keystore file 315, 318
changing
password for user account 10
character data sets
handling options for Microsoft SQL Server and PeopleSoft on Oracle 212
character encoding
Web Services Hub 318
character sizes
double byte 424
multibyte 424
single byte 424
classpaths
Java SDK 220
ClientStore
option 210
clustered file systems
high availability 132
COBOL
connectivity 490
Code Page (property)
PowerCenter Integration Service process 220
PowerCenter Repository Service 259
code page relaxation
compatible code pages, selecting 433

configuring the Integration Service 432
data inconsistencies 432
overview 432
troubleshooting 433
code page validation
overview 431
relaxed validation 432
code pages
Administrator tool 426
application sources 428
application targets 428
choosing 424
compatibility diagram 430
compatibility overview 424
conversion 433
Custom transformation 430
data movement modes 238
descriptions 442
domain configuration database 426
External Procedure transformation 430
flat file sources 428
flat file targets 428
for PowerCenter Integration Service process 218
global repository 275
ID 442
lookup database 430
Metadata Manager Service 428
names 442
overview 423
pmcmd 427
PowerCenter Client 426
PowerCenter Integration Service process 427, 440
PowerCenter repository 259
relational sources 428
relational targets 428
relationships 431
relaxed validation for sources and targets 432
repository 274, 427, 440
repository, Web Services Hub 315
sort order overview 427
sources 428, 442
stored procedure database 430
supported code pages 440, 442
targets 428, 442
UNIX 423
validation 431
validation for sources and targets 213
Windows 424
column level security
restricting columns 122
command line programs
privileges 452
resilience, configuring 134
compatibility
between code pages 424
between source and target code pages 433
compatibility properties
PowerCenter Integration Service 212
compatible
defined for code page compatibility 424
Complete
option to disable PowerCenter Integration Service 203
option to disable PowerCenter Integration Service process 203
complete history statistics
Web Services Report 410
configuration properties
Listener Service 288
Logger Service 293
PowerCenter Integration Service 213
Configuration Support Manager
using to analyze node diagnostics 417
using to review node diagnostics 413
connect string
examples 190, 261, 492
PowerCenter repository database 263
syntax 190, 261, 492
connecting
Integration Service to IBM DB2 (Windows) 495, 505
Integration Service to Informix (Windows) 507
Integration Service to Microsoft Access 496
Integration Service to Microsoft SQL Server 497
Integration Service to ODBC data sources (UNIX) 521
Integration Service to Oracle (UNIX) 509
Integration Service to Oracle (Windows) 498
Integration Service to Sybase ASE (UNIX) 512
Integration Service to Sybase ASE (Windows) 499
Microsoft Excel to Integration Service 496
SQL data service 170
to UNIX databases 504
to Windows databases 495
connecting to databases
JDBC 492
connection objects
privileges for PowerCenter 94
connection pooling
overview 324
connection pools
properties 338
connection properties
Informatica domain 330
connection resources
assigning 351
connection strings
native connectivity 492
connection timeout
high availability 127
connections
adding pass-through security 171
creating a database connection 327
database properties 331
default permissions 118
deleting 330
editing 329
overview 323
pass-through security 170
permission types 118
permissions 117
testing 329
connectivity
COBOL 490
connect string examples 190, 261, 492
Data Analyzer 492
diagram of 487
Integration Service 490
Metadata Manager 492
overview 224, 487
PowerCenter Client 491
PowerCenter Repository Service 489
Content Management Service
application service 15
creating 158
overview 153
control file
overview 241
permissions 238

CPU detail
License Management Report 402
CPU profile
computing 357
description 357
node property 33
CPU summary
License Management Report 401
CPU usage
Integration Service 236
CreateIndicatorFiles
option 213
custom filters
date and time 398
elapsed time 398
multi-select 399
custom metrics
privilege to promote 96, 102
custom properties
configuring for Data Integration Service 169, 174
configuring for Metadata Manager 197
configuring for Web Services Hub 320
domain 47
PowerCenter Integration Service process 221
PowerCenter Repository Service 266
PowerCenter Repository Service process 267
Web Services Hub 317
custom resources
defining 351
naming conventions 352
custom roles
assigning to users and groups 106
creating 105
deleting 106
description 103, 105
editing 105
Metadata Manager Service 476
PowerCenter Repository Service 475
privileges, assigning 105
Reporting Service 477
Custom transformation
directory for Java components 219

D

Data Analyzer
administrator 59
connectivity 492
Data Profiling reports 298
JDBC-ODBC bridge 492
Metadata Manager Repository Reports 298
ODBC (Open Database Connectivity) 487
repository 299
data cache
memory usage 237
data handling
setting up prior version compatibility 212
Data Integration Service
application service 15
authorization 7
configuring Data Integration Service security 172
creating 175
custom properties 169, 174
enabling 169
HTTP configuration properties 168
HTTP proxy server properties 168
log events 378
Maximum Heap Size 173
privileges 81
properties 164
result set cache properties 173
Data Integration Service process
HTTP configuration properties 172
Data Integration Services
monitoring 388
data lineage
PowerCenter Repository Service, configuring 266
data movement mode
ASCII 421
changing 422
description 421
effect on session files and caches 422
for PowerCenter Integration Service 201
option 209
overview 421
setting 209
Unicode 422
data movement modes
overview 238
Data Object Cache
configuring 165
properties 165
data object caching
with pass-through security 171
data service security
configuring Data Integration Service 172
database
domain configuration 37
Reporting Service 299
repositories, creating for 259
database array operation size
description 263
database client
environment variables 221, 267
database connection timeout
description 263
database connections
resilience 138
updating for domain configuration 40
database drivers
Integration Service 487
Repository Service 487
Database Hostname
description 194
Database Name
description 194
Database Pool Expiration Threshold (property)
description 264
Database Pool Expiration Timeout (property)
description 264
Database Pool Size (property)
description 263
Database Port
description 194
database properties
Informatica domain 45
database resilience
domain configuration 128
Lookup transformation 128
PowerCenter Integration Service 128
repository 128, 136
sources 128
targets 128
database user accounts
guidelines for setup 482

databases
connecting to (UNIX) 504
connecting to (Windows) 495
connecting to IBM DB2 495, 505
connecting to Informix 507
connecting to Microsoft Access 496
connecting to Microsoft SQL Server 497
connecting to Neoview (UNIX) 516, 518
connecting to Neoview (Windows) 501, 502
connecting to Oracle 498, 509
connecting to Sybase ASE 499, 512
connecting to Teradata (Windows) 500, 513
Data Analyzer repositories 482
Metadata Manager repositories 482
PowerCenter repositories 482
DataDirect ODBC drivers
platform-specific drivers required 492
DateDisplayFormat
option 213
DateHandling40Compatibility
option 212
dates
default format for logs 213
deadlock retries
setting number 212
DeadlockSleep
option 212
Debug
error severity level 210, 319
Debugger
running 210
default administrator
description 58
modifying 58
passwords, changing 58
deleting
connections 330
dependencies
application services 42
grids 42
nodes 42
viewing for services and nodes 42
deployed mapping jobs
monitoring 391
deployment
applications 176
deployment groups
privileges for PowerCenter 94
design objects
description 90
privileges 90
Design Objects privilege group
description 90
direct permission
description 112
directories
cache files 220
external procedure files 220
for Java components 219
lookup files 220
recovery files 220
reject files 220
root directory 220
session log files 220
source files 220
target files 220
temporary files 220
workflow log files 220
dis
permissions by command 453
privileges by command 453
disable mode
services and service processes 30
disabling
Metadata Manager Service 192
PowerCenter Integration Service 203
PowerCenter Integration Service process 203
Reporting Service 301, 302
Web Services Hub 316
dispatch mode
adaptive 354
configuring 354
Load Balancer 228
metric-based 354
round-robin 354
dispatch priority
configuring 355
dispatch queue
overview 226
service levels, creating 355
dispatch wait time
configuring 355
domain
administration privileges 77
administrator 58
Administrator role 104
associated repository for Web Services Hub 315
log event categories 377
metadata, sharing 274
privileges 75
reports 400
resources, viewing 351
secure communication 53
security administration privileges 77
user activity, monitoring 400
user security 29
user synchronization 7
users with privileges 108
Domain Administration privilege group
description 77
domain administrator
description 58
domain configuration
description 37
log events 377
migrating 39
domain configuration database
backing up 38
code page 426
connection for gateway node 40
description 37
migrating 39
restoring 38
updating 40
domain objects
permissions 113
domain permissions
direct 112
effective 112
inherited 112
domain properties
Informatica domain 44
domain reports
License Management Report 400
running 400
Web Services Report 407

Domain tab
  Connections view 19
  Informatica Administrator 13
  Navigator 13
  Services and Nodes view 13
domains
  multiple 25
DTM (Data Transformation Manager)
  buffer memory 237
  distribution on grids 235
  master DTM 235
  preparer DTM 235
  process 229
  worker DTM 235
DTM timeout
  Web Services Hub 319

E

editing
  connections 329
effective permission
  description 112
enabling
  Metadata Manager Service 192
  PowerCenter Integration Service 203
  PowerCenter Integration Service process 203
  Reporting Service 301, 302
  Web Services Hub 316
encoding
  Web Services Hub 318
environment variables
  database client 221, 267
  LANG_C 423
  LC_ALL 423
  LC_CTYPE 423
  Listener Service process 289
  Logger Service process 295
  NLS_LANG 435, 437
  PowerCenter Integration Service process 221
  PowerCenter Repository Service process 267
  troubleshooting 32
Error
  severity level 210, 319
error logs
  messages 239
Error Severity Level (property)
  Metadata Manager Service 196
  PowerCenter Integration Service 210
Everyone group
  description 58
ExportSessionLogLibName
  option 213
external procedure files
  directory 220
external resilience
  description 128

F

failover
  PowerCenter Integration Service 138
  PowerCenter Repository Service 136
  PowerExchange Listener Service 286
  PowerExchange Logger Service 292
  safe mode 206
  services 128
file/directory resources
  defining 351
  naming conventions 352
filtering data
  SAP NetWeaver BI, parameter file location 312
flat files
  connectivity 490
  exporting logs 376
  output files 241
  source code page 428
  target code page 428
folders
  Administrator tool 27
  creating 27, 28
  managing 27
  objects, moving 28
  operating system profile, assigning 280
  overview 14
  permissions 113
  privileges 89
  removing 28
Folders privilege group
  description 89
FTP
  achieving high availability 142
  connection resilience 128
  server resilience 137
FTP connections
  resilience 138

G

gateway
  managing 37
  resilience 127
gateway node
  configuring 37
  description 2
  log directory 37
  logging 369
GB18030
  description 419
general properties
  Informatica domain 44
  license 365
  Listener Service 287
  Logger Service 293
  Metadata Manager Service 193
  PowerCenter Integration Service 209
  PowerCenter Integration Service process 220
  PowerCenter Repository Service 262
  SAP BW Service 311
  Web Services Hub 317, 318
global objects
  privileges for PowerCenter 94
Global Objects privilege group
  description 94
global repositories
  code page 274, 275
  creating 275
  creating from local repositories 275
  moving to another Informatica domain 277
global settings
  configuring 386
globalization
  overview 418

graphics display server
  requirement 400
grid
  troubleshooting 352
grid assignment properties
  PowerCenter Integration Service 208
grids
  assigning to a PowerCenter Integration Service 349
  configuring 348
  creating 348
  dependencies 42
  description 234, 348
  DTM processes, distributing 235
  for new PowerCenter Integration Service 201
  Informatica Administrator tabs 19
  license requirement 208
  operating system profile 349
  permissions 113, 348
  service processes, distributing 234
  sessions and workflows, running 234
group description
  invalid characters 69
groups
  default Everyone 58
  invalid characters 69
  managing 69
  overview 22
  parent group 69
  privileges, assigning 106
  roles, assigning 106
  synchronization 7
  valid name 69
Guaranteed Message Delivery files
  Log Manager 369

H

hardware configuration
  License Management Report 404
heartbeat interval
  description 264
high availability
  backup nodes 131
  base product 129
  clustered file systems 132
  description 8, 126
  environment, configuring 131
  example configurations 131
  external connection timeout 127
  external systems 131, 132
  Informatica services 131
  licensed option 208
  Listener Service 286
  Logger Service 292
  multiple gateways 131
  PowerCenter Integration Service 137
  PowerCenter Repository Service 136
  PowerCenter Repository Service failover 136
  PowerCenter Repository Service recovery 137
  PowerCenter Repository Service resilience 136
  PowerCenter Repository Service restart 136
  recovery 129
  recovery in base product 129, 130
  resilience 127, 133
  resilience in base product 129
  restart in base product 129
  rules and guidelines 132
  SAP BW services 131
  TCP KeepAlive timeout 142
  Web Services Hub 131
high availability option
  service processes, configuring 270
host names
  Web Services Hub 315, 318
host port number
  Web Services Hub 315, 318
HTTP configuration properties
  Data Integration Service 168
  Data Integration Service process 172
HTTP proxy
  domain setting 215
  password setting 215
  port setting 215
  server setting 215
  user setting 215
HTTP proxy properties
  PowerCenter Integration Service 215
HTTP proxy server
  usage 215
HTTP proxy server properties
  Data Integration Service 168
HttpProxyDomain
  option 215
HttpProxyPassword
  option 215
HttpProxyPort
  option 215
HttpProxyServer
  option 215
HttpProxyUser
  option 215
HTTPS
  configuring 55
  keystore file 55, 315, 318
  keystore password 315, 318
  port for Administrator tool 55
  SSL protocol for Administrator tool 55
Hub Logical Address (property)
  Web Services Hub 319

I

IBM DB2
  connect string example 190, 261
  connect string syntax 492
  connecting to Integration Service (Windows) 495, 505
  Metadata Manager repository 486
  repository database schema, optimizing 263
  setting DB2CODEPAGE 496
  setting DB2INSTANCE 496
  single-node tablespace 483
IBM Tivoli Directory Service
  LDAP authentication 60
IgnoreResourceRequirements
  option 210
IME (Windows Input Method Editor)
  input locales 421
incremental aggregation
  files 242
incremental keys
  licenses 361
index caches
  memory usage 237
indicator files
  description 241

session output 241
Informatica Administrator
Domain tab 13
keyboard shortcuts 23
logging in 9
Logs tab 20
Monitoring tab 21
Navigator 22
overview 12, 25
Reports tab 20
repositories, backing up 280
repositories, restoring 281
repository notifications, sending 280
searching 21
Security page 21
service process, enabling and disabling 30
Services and Nodes view 14
services, enabling and disabling 30
tabs, viewing 12
tasks for Web Services Hub 314
Informatica Analyst
administrator 59
Informatica Developer
administrator 59
Informatica domain
alerts 26
connection properties 330
database properties 45
description 1
domain properties 44
general properties 44
log and gateway configuration 46
multiple domains 25
permissions 29
privileges 29
resilience 127, 134
resilience, configuring 134
restarting 43
shutting down 43
state of operations 129
user security 29
users, managing 66
Informatica services
restart 130
Information and Content Exchange (ICE)
log files 376
Information error severity level
description 210, 319
Informix
connect string syntax 492
connecting to Integration Service (Windows) 507
inherited permission
description 112
inherited privileges
description 107
input locales
configuring 421
IME (Windows Input Method Editor) 421
Integration Service
connectivity 490
ODBC (Open Database Connectivity) 487
internal host name
Web Services Hub 315, 318
internal port number
Web Services Hub 315, 318
internal resilience
description 127
ipc
permissions by command 454
privileges by command 454
isp
permissions by command 454
privileges by command 454

J

Java
configuring for JMS 219
configuring for PowerExchange for Web Services 219
configuring for webMethods 219
Java components
directories, managing 219
Java SDK
class path 220
maximum memory 220
minimum memory 220
Java SDK Class Path
option 220
Java SDK Maximum Memory
option 220
Java SDK Minimum Memory
option 220
Java transformation
directory for Java components 219
JCEProvider
option 210
JDBC (Java Database Connectivity)
overview 493
JDBC drivers
Data Analyzer 487
Data Analyzer connection to repository 492
installed drivers 492
Metadata Manager 487
Metadata Manager connection to databases 492
PowerCenter domain 487
Reference Table Manager 487
JDBC-ODBC bridge
Data Analyzer 492
jobs
monitoring 389
Joiner transformation
caches 237, 242
setting up for prior version compatibility 212
JoinerSourceOrder6xCompatibility
option 212
JVM Command Line Options
advanced Web Services Hub property 319

K

keyboard shortcuts
Informatica Administrator 23
Navigator 23
keystore file
Metadata Manager 195
Web Services Hub 315, 318
keystore password
Web Services Hub 315, 318

L

labels
privileges for PowerCenter 94

LANG_C environment variable
  setting locale in UNIX 423
LC_ALL environment variable
  setting locale in UNIX 423
LDAP authentication
  description 7, 60
  directory services 60
  nested groups 65
  self-signed SSL certificate 65
  setting up 60
  synchronization times 64
LDAP directory service
  anonymous login 60
  nested groups 65
LDAP groups
  importing 60
  managing 69
LDAP security domains
  configuring 62
  deleting 65
LDAP server
  connecting to 61
LDAP users
  assigning to groups 67
  enabling 67
  importing 60
  managing 66
license
  assigning to a service 362
  creating 361
  details, viewing 364
  for new PowerCenter Integration Service 201
  general properties 365
  Informatica Administrator tabs 19
  keys 361
  license file 361
  log events 377, 380
  managing 360
  removing 364
  unassigning from a service 363
  updating 363
  validation 360
  Web Services Hub 315, 318
license keys
  incremental 361, 363
  original 361
License Management Report
  CPU detail 402
  CPU summary 401
  emailing 406
  hardware configuration 404
  licensed options 405
  licensing 401
  multibyte characters 405
  node configuration 404
  repository summary 402
  running 400, 405
  Unicode font 405
  user detail 403
  user summary 403
license usage
  log events 377
licensed options
  high availability 208
  License Management Report 405
  server grid 208
licenses
  permissions 113
licensing
  License Management Report 401
  log events 379
  managing 360
licensing logs
  log events 360
Limit on Resilience Timeouts (property)
  description 264
linked domain
  multiple domains 25, 276
Listener Service
  log events 378
Listener Service process
  environment variables 289
  properties 289
LMAPI
  resilience 128
Load Balancer
  assigning priorities to tasks 228, 355
  configuring to check resources 210, 227, 356
  CPU profile, computing 357
  defining resource provision thresholds 357
  dispatch mode 228
  dispatch mode, configuring 354
  dispatch queue 226
  dispatching tasks in a grid 227
  dispatching tasks on a single node 227
  overview 226
  resource provision thresholds 227
  resources 227, 350
  service levels 228
  service levels, creating 355
  settings, configuring 353
load balancing
  SAP BW Service 308
  support for SAP NetWeaver BI system 308
Load privilege group
  description 85
LoadManagerAllowDebugging
  option 210
local repositories
  code page 274
  moving to another Informatica domain 277
  promoting 275
  registering 276
locales
  overview 420
localhost_.txt
  troubleshooting 370
locks
  managing 277
  viewing 278
Log Agent
  log events 377
log and gateway configuration
  Informatica domain 46
log directory
  for gateway node 37
  location, configuring 370
log errors
  Administrator tool 376
log event files
  description 369
  purging 371
log events
  authentication 377
  authorization 377
  code 377

components 377
description 369
details, viewing 372
domain 377
domain configuration 377
domain function categories 377
exporting with Mozilla Firefox 375
licensing 377, 379, 380
licensing logs 360
licensing usage 377
Log Agent 377
Log Manager 377
message 377
message code 377
node 377
node configuration 377
PowerCenter Repository Service 380
saving 374, 375
security audit trail 380
Service Manager 377
service name 377
severity levels 377
thread 377
time zone 371
timestamps 377
user activity 381
user management 377
viewing 372
Web Services Hub 381
Log Level (property)
Web Services Hub 319
Log Manager
architecture 369
catalina.out 370
configuring 371
directory location, configuring 370
domain log events 377
log event components 377
log events 377
log events, purging 371
log events, saving 375
logs, viewing 372
message 377
message code 377
node 377
node.log 370
PowerCenter Integration Service log events 379
PowerCenter Repository Service log events 380
ProcessID 377
purge properties 371
recovery 369
SAP NetWeaver BI log events 380
security audit trail 380
service name 377
severity levels 377
thread 377
time zone 371
timestamp 377
troubleshooting 370
user activity log events 381
using 368
Logger Service
log events 379
Logger Service process
environment variables 295
properties 295
logging in
Administrator tool 9
Informatica Administrator 9
logical data objects
monitoring 397
logs
components 377
configuring 370
domain 377
error severity level 210
in UTF-8 210
location 370
PowerCenter Integration Service 379
PowerCenter Repository Service 380
purging 371
SAP BW Service 380
saving 375
session 240
user activity 381
viewing 372
workflow 239
Logs tab
Informatica Administrator 20
LogsInUTF8
option 210
lookup caches
persistent 242
lookup databases
code pages 430
lookup files
directory 220
Lookup transformation
caches 237, 242
database resilience 128

M

Manage List
linked domains, adding 276
managing
accounts 9
user accounts 9
mapping properties
configuring 179
master gateway
resilience to domain configuration database 128
master gateway node
description 2
master service process
description 234
master thread
description 230
Max Concurrent Resource Load
description, Metadata Manager Service 196
Max Heap Size
description, Metadata Manager Service 196
Max Lookup SP DB Connections
option 212
Max MSSQL Connections
option 212
Max Sybase Connections
option 212
MaxConcurrentRequests
advanced Web Services Hub property 319
description, Metadata Manager Service 195
Maximum Active Connections
description, Metadata Manager Service 196
SQL data service property 178

maximum active users
description 264
Maximum Catalog Child Objects
description 196
Maximum Concurrent Connections
configuring 174
Maximum Concurrent Refresh Requests
property 165
Maximum CPU Run Queue Length
node property 33, 357
maximum dispatch wait time
configuring 355
Maximum Heap Size
advanced Web Services Hub property 319
configuring Analyst Service 150
configuring Data Integration Service 173
configuring Model Repository Service 249
maximum locks
description 264
Maximum Memory Percent
node property 33, 357
Maximum Processes
node property 33, 357
Maximum Restart Attempts (property)
Informatica domain 31
Maximum Wait Time
description, Metadata Manager Service 196
MaxISConnections
Web Services Hub 319
MaxQueueLength
advanced Web Services Hub property 319
description, Metadata Manager Service 195
MaxStatsHistory
advanced Web Services Hub property 319
memory
DTM buffer 237
maximum for Java SDK 220
Metadata Manager 196
minimum for Java SDK 220
message code
Log Manager 377
metadata
adding to repository 434
choosing characters 434
sharing between domains 274
Metadata Manager
administrator 59
components 186
configuring PowerCenter Integration Service 198
connectivity 492
ODBC (Open Database Connectivity) 487
repository 187
starting 192
user for PowerCenter Integration Service 198
Metadata Manager File Location (property)
description 193
Metadata Manager repository
content, creating 191
content, deleting 192
creating 187
heap size 486
optimizing IBM DB2 database 486
system temporary tablespace 486
Metadata Manager Service
advanced properties 196
application service 15
authorization 7
code page 428
components 186
creating 188
custom properties 197
custom roles 476
description 186
disabling 192
general properties 193
log events 379
privileges 82
properties 192, 193
recycling 192
steps to create 187
user synchronization 7
users with privileges 108
Metadata Manager Service privileges
Browse privilege group 83
Load privilege group 85
Model privilege group 85
Security privilege group 86
Metadata Manager Service properties
PowerCenter Repository Service 266
metric-based dispatch mode
description 354
Microsoft Access
connecting to Integration Service 496
Microsoft Active Directory Service
LDAP authentication 60
Microsoft Excel
connecting to Integration Service 496
using PmNullPasswd 497
using PmNullUser 497
Microsoft SQL Server
configuring Data Analyzer repository database 484
connect string syntax 190, 261, 492
connecting from UNIX 505
connecting to Integration Service 497
repository database schema, optimizing 263
setting Char handling options 212
migrate
domain configuration 39
Minimum Severity for Log Entries (property)
PowerCenter Repository Service 264
Model privilege group
description 85
model repository
backing up 253
creating 253
creating content 253
deleting 253
deleting content 253
restoring content 254
Model Repository Service
cache management 256
application service 15
authorization 7
backup directory 253
Creating 257
Disabling 247
Enabling 247
log events 379
logs 255
Maximum Heap Size 249
Overview 243
privileges 86
properties 248
user synchronization 7
users with privileges 108

modules
  disabling 167
monitoring
  applications 390
  Data Integration Services 388
  deployed mapping jobs 391
  description 382
  global settings, configuring 386
  jobs 389
  logical data objects 397
  preferences, configuring 387
  reports 385
  setup 386
  SQL data services 392
  statistics 384
  web services 395
Monitoring privilege group
  domain 80
Monitoring tab
  Informatica Administrator 21
mrs
  permissions by command 464
  privileges by command 464
ms
  permissions by command 465
  privileges by command 465
MSExchangeProfile
  option 213
multibyte data
  entering in PowerCenter Client 421

N

native authentication
  description 7, 60
native groups
  adding 69
  deleting 71
  editing 70
  managing 69
  moving to another group 70
  users, assigning 67
native security domain
  description 60
native users
  adding 66
  assigning to groups 67
  deleting 68
  editing 67
  enabling 67
  managing 66
  passwords 66
Navigator
  Domain tab 13
  keyboard shortcuts 23
  Security page 22
Neoview
  connecting from an integration service (Windows) 501, 502
  connecting from Informatica clients(Windows) 501, 502
  connecting to an Informatica client (UNIX) 516, 518
  connecting to an integration service (UNIX) 516, 518
nested groups
  LDAP authentication 65
  LDAP directory service 65
network
  high availability 142
NLS_LANG
  setting locale 435, 437
node assignment
  PowerCenter Integration Service 208
  Web Services Hub 317, 318
node configuration
  License Management Report 404
  log events 377
node configuration file
  location 32
node diagnostics
  analyzing 417
  downloading 415
node properties
  backup directory 33
  configuring 32, 33
  CPU Profile 33
  maximum CPU run queue length 33, 357
  maximum memory percent 33, 357
  maximum processes 33, 357
node.log
  troubleshooting 370
nodemeta.xml
  for gateway node 37
  location 32
nodes
  adding to Informatica Administrator 32
  configuring 33
  defining 32
  dependencies 42
  description 1, 2
  gateway 2, 37
  host name and port number, removing 33
  Informatica Administrator tabs 18
  Log Manager 377
  managing 32
  node assignment, configuring 208
  permissions 113
  port number 33
  properties 32
  removing 36
  resources, viewing 351
  restarting 35
  shutting down 35
  starting 35
  TCP/IP network protocol 487
  Web Services Hub 315
  worker 2
normal mode
  PowerCenter Integration Service 204
notifications
  sending 280
Novell e-Directory Service
  LDAP authentication 60
null values
  PowerCenter Integration Service, configuring 212
NumOfDeadlockRetries
  option 212

O

object queries
  privileges for PowerCenter 94
ODBC (Open Database Connectivity)
  DataDirect driver issues 492
  establishing connectivity 492
  Integration Service 487

Metadata Manager 487
PowerCenter Client 487
requirement for PowerCenter Client 491
ODBC Connection Mode
description 196
ODBC data sources
connecting to (UNIX) 521
connecting to (Windows) 495
odbc.ini file
sample 523
oie
permissions by command 465
privileges by command 465
Open LDAP Directory Service
LDAP authentication 60
operating mode
effect on resilience 134, 271
normal mode for PowerCenter Integration Service 204
PowerCenter Integration Service 204
PowerCenter Repository Service 271
safe mode for PowerCenter Integration Service 204
operating system profile
configuration 216
creating 71
deleting 71
editing 72
folders, assigning to 280
grids 349
overview 215
pmimpprocess 216
properties 72
troubleshooting 217
operating system profiles
permissions 113, 116
optimizing
PowerCenter repository 483
Oracle
connect string syntax 190, 261, 492
connecting to Integration Service (UNIX) 509
connecting to Integration Service (Windows) 498
setting locale with NLS_LANG 435, 437
Oracle Net Services
using to connect Integration Service to Oracle (UNIX) 509
using to connect Integration Service to Oracle (Windows) 498
original keys
licenses 361
output files
overview 238, 241
permissions 238
target files 241
OutputMetaDataForFF
option 213
overview
connection pooling 324
connections 323
Content Management Service 153

P

page size
minimum for optimizing repository database schema 263
parent groups
description 69
pass-through pipeline
overview 230
pass-through security
adding to connections 171
connecting to SQL data service 170
enabling caching 171
properties 168
web service operation mappings 170
password
changing for a user account 10
passwords
changing for default administrator 58
native users 66
requirements 66
PeopleSoft on Oracle
setting Char handling options 212
Percent Partitions in Use (property)
Web Services Report 407
performance
details 240
PowerCenter Integration Service 264
PowerCenter Repository Service 264
repository copy, backup, and restore 284
repository database schema, optimizing 263
performance detail files
permissions 238
permissions
application services 113
as commands 452
connections 117
description 111
direct 112
dis commands 453
domain objects 113
effective 112
folders 113
grids 113
inherited 112
ipc commands 454
isp commands 454
licenses 113
mrs commands 464
ms commands 465
nodes 113
oie commands 465
operating system profiles 113, 116
output and log files 238
pmcmd commands 468
pmrep commands 470
ps commands 465
pwx commands 466
recovery files 238
rtm commands 467
search filters 113
sql commands 467
SQL data service 119
types 112
virtual schema 119
virtual stored procedure 119
virtual table 119
web service 123
web service operation 123
working with privileges 111
persistent lookup cache
session output 242
pipeline partitioning
multiple CPUs 232
overview 232
symmetric processing platform 236
plug-ins
registering 283
unregistering 283

$PMBadFileDir
option 220
$PMCacheDir
option 220
pmcmd
code page issues 427
communicating with PowerCenter Integration Service 427
permissions by command 468
privileges by command 468
$PMExtProcDir
option 220
$PMFailureEmailUser
option 209
pmimpprocess
description 216
$PMLookupFileDir
option 220
PmNullPasswd
reserved word 490
PmNullUser
reserved word 490
pmrep
permissions by command 470
privileges by command 470
$PMRootDir
description 219
option 220
required syntax 219
shared location 219
PMServer3XCompatibility
option 212
$PMSessionErrorThreshold
option 209
$PMSessionLogCount
option 209
$PMSessionLogDir
option 220
$PMSourceFileDir
option 220
$PMStorageDir
option 220
$PMSuccessEmailUser
option 209
$PMTargetFileDir
option 220
$PMTempDir
option 220
$PMWorkflowLogCount
option 209
$PMWorkflowLogDir
option 220
port
application service 3
node 33
node maximum 33
node minimum 33
range for service processes 33
port number
Metadata Manager Agent 193
Metadata Manager application 193
post-session email
Microsoft Exchange profile, configuring 213
overview 241
PowerCenter
connectivity 487
repository reports 298
PowerCenter Client
administrator 59
code page 426
connectivity 491
multibyte characters, entering 421
ODBC (Open Database Connectivity) 487
resilience 134
TCP/IP network protocol 487
PowerCenter domains
connectivity 488
TCP/IP network protocol 487
PowerCenter Integration Service
advanced properties 210
application service 15
architecture 223
assign to grid 201, 349
assign to node 201
associated repository 217
blocking data 233
clients 137
compatibility and database properties 212
configuration properties 213
configuring for Metadata Manager 198
connectivity overview 224
creating 201
data movement mode 201, 209
data movement modes 238
data, processing 233
date display format 213
disable process with Abort option 203
disable process with Stop option 203
disable with Abort option 203
disable with Complete option 203
disable with Stop option 203
disabling 203
enabling 203
export session log lib name, configuring 213
fail over in safe mode 205
failover 138
failover, on grid 140
for Metadata Manager 186
general properties 209
grid and node assignment properties 208
high availability 137
HTTP proxy properties 215
log events 379
logs in UTF-8 210
name 201
normal operating mode 204
operating mode 204
output files 241
performance 264
performance details 240
PowerCenter Repository Service, associating 201
process 224
recovery 129, 141
resilience 137
resilience period 210
resilience timeout 210
resilience to database 128
resource requirements 210
restart 138
safe mode, running in 205
safe operating mode 205
session recovery 141
shared storage 218
sources, reading 233
state of operations 129, 141
system resources 236
version 212

workflow recovery 141
PowerCenter Integration Service process
$PMBadFileDir 220
$PMCacheDir 220
$PMExtProcDir 220
$PMLookupFileDir 220
$PMRootDir 220
$PMSessionLogDir 220
$PMSourceFileDir 220
$PMStorageDir 220
$PMTargetFileDir 220
$PMTempDir 220
$PMWorkflowLogDir 220
code page 218, 427
code pages, specifying 220
custom properties 221
disable with Complete option 203
disabling 203
enabling 203
environment variables 221
general properties 220
Java component directories 219
supported code pages 440
PowerCenter Integration Service process nodes
license requirement 208
PowerCenter repository
associated with Web Services Hub 321
code pages 259
content, creating for Metadata Manager 190
data lineage, configuring 266
optimizing for IBM DB2 483
PowerCenter Repository Reports
installing 298
PowerCenter Repository Service
Administrator role 104
advanced properties 264
application service 15
associating with a Web Services Hub 315
authorization 7
Code Page (property) 259
configuring 262
connectivity requirements 489
creating 259
custom roles 475
data lineage, configuring 266
enabling and disabling 269
failover 136
for Metadata Manager 186
general properties 262
high availability 136
log events 380
Metadata Manager Service properties 266
operating mode 271
performance 264
PowerCenter Integration Service, associating 201
privileges 87
properties 262
recovery 129, 137
repository agent caching 264
repository properties 262
resilience 136
resilience to database 128, 136
restart 136
service process 270
state of operations 129, 137
user synchronization 7
users with privileges 108
PowerCenter Repository Service process
configuring 266
environment variables 267
properties 266
PowerCenter security
managing 21
PowerExchange for JMS
directory for Java components 219
PowerExchange for Web Services
directory for Java components 219
PowerExchange for webMethods
directory for Java components 219
PowerExchange Listener Service
application service 15
creating 290
disabling 289
enabling 289
failover 286
privileges 96
properties 287
restart 286
restarting 290
PowerExchange Logger Service
application service 15
creating 296
disabling 295
enabling 295
failover 292
privileges 96
properties 293
restart 292
restarting 295
preferences
monitoring 387
Preserve MX Data (property)
description 264
primary node
for new Integration Service 201
node assignment, configuring 208
privilege groups
Administration 98
Alerts 99
Browse 83
Communication 99
Content Directory 100
Dashboard 101
description 75
Design Objects 90
Domain Administration 77
Folders 89
Global Objects 94
Indicators 101
Load 85
Manage Account 102
Model 85
Monitoring 80
Reports 102
Run-time Objects 92
Security 86
Security Administration 77
Sources and Targets 91
Tools 81, 88
privileges
Administration 98
Alerts 99
Analyst Service 81
as commands 452
assigning 106

command line programs 452
Communication 99
Content Directory 100
Dashboard 101
Data Integration Service 81
description 74
design objects 90
dis commands 453
domain 75
domain administration 77
domain tools 81
folders 89
Indicators 101
inherited 107
ipc commands 454
isp commands 454
Manage Account 102
Metadata Manager Service 82
Model Repository Service 86
monitoring 80
mrs commands 464
ms commands 465
oie commands 465
pmcmd commands 468
pmrep commands 470
PowerCenter global objects 94
PowerCenter Repository Service 87
PowerCenter Repository Service tools 88
PowerExchange Listener Service 96
PowerExchange Logger Service 96
ps commands 465
pwx commands 466
Reporting Service 96
Reports 102
rtm commands 467
run-time objects 92
security administration 77
sources 91
sql commands 467
targets 91
troubleshooting 108
working with permissions 111
process identification number
Log Manager 377
ProcessID
Log Manager 377
message code 377
profiling properties
configuring 167
Profiling Warehouse Connection Name
configuring 166
properties
Metadata Manager Service 193
provider-based security
users, deleting 68
ps
permissions by command 465
privileges by command 465
purge properties
Log Manager 371
pwx
permissions by command 466
privileges by command 466

R

Rank transformation
caches 237, 242
recovery
base product 130
files, permissions 238
high availability 129
Integration Service 129
PowerCenter Integration Service 141
PowerCenter Repository Service 129, 137
PowerExchange for IBM WebSphere MQ 130
safe mode 206
workflow and session, manual 130
recovery files
directory 220
registering
local repositories 276
plug-ins 283
reject files
directory 220
overview 240
permissions 238
repagent caching
description 264
Reporting Service
application service 15
authorization 7
configuring 304
creating 297, 299
custom roles 477
data source properties 306
database 299
disabling 301, 302
enabling 301, 302
general properties 305
managing 301
options 299
privileges 96
properties 304
Reporting Service properties 305
repository properties 307
user synchronization 7
users with privileges 108
using with Metadata Manager 187
Reporting Service privileges
Administration privilege group 98
Alerts privilege group 99
Communication privilege group 99
Content Directory privilege group 100
Dashboard privilege group 101
Indicators privilege group 101
Manage Account privilege group 102
Reports privilege group 102
reports
Administrator tool 400
Data Profiling Reports 298
domain 400
License 400
Metadata Manager Repository Reports 298
monitoring 385
Web Services 400
Reports tab
Informatica Administrator 20
repositories
associated with PowerCenter Integration Service 217
backing up 280
backup directory 33

code pages 274, 275, 427
content, creating 190, 272
content, deleting 190, 273
database schema, optimizing 263
database, creating 259
Metadata Manager 186
moving 277
notifications 280
overview of creating 258
performance 284
persisting run-time statistics 210
restoring 281
security log file 284
supported code pages 440
Unicode 419
UTF-8 419
version control 273
repository
Data Analyzer 299
repository agent cache capacity
description 264
repository agent caching
PowerCenter Repository Service 264
Repository Agent Caching (property)
description 264
repository domains
description 274
managing 274
moving to another Informatica domain 277
prerequisites 274
registered repositories, viewing 277
user accounts 275
repository locks
managing 277
releasing 279
viewing 278
repository metadata
choosing characters 434
repository notifications
sending 280
repository password
associated repository for Web Services Hub 321, 322
option 217
repository properties
PowerCenter Repository Service 262
Repository Service process
description 270
repository summary
License Management Report 402
repository user name
associated repository for Web Services Hub 315, 321, 322
option 217
repository user password
associated repository for Web Services Hub 315
request timeout
SQL data services requests 178
Required Comments for Checkin(property)
description 264
resilience
application service configuration 134
base product 130
command line program configuration 134
domain configuration 134
domain configuration database 128
domain properties 127
external 128
external components 138
external connection timeout 127
FTP connections 128
gateway 127
high availability 127, 133
in exclusive mode 134, 271
internal 127
LMAPI 128
managing 133
period for PowerCenter Integration Service 210
PowerCenter Client 134
PowerCenter Integration Service 137
PowerCenter Repository Service 136
repository database 128, 136
services 127
services in base product 130
TCP KeepAlive timeout 142
Resilience Timeout (property)
description 264
option 210
resource provision thresholds
defining 357
description 357
overview 227
setting for nodes 33
resources
configuring 350
configuring Load Balancer to check 210, 227, 356
connection, assigning 351
defining custom 351
defining file/directory 351
defining for nodes 350
Load Balancer 227
naming conventions 352
node 227
predefined 350
user-defined 350
viewing for nodes 351
restart
base product 130
configuring for service processes 31
Informatica services, automatic 130
PowerCenter Integration Service 138
PowerCenter Repository Service 136
PowerExchange Listener Service 286
PowerExchange Logger Service 292
services 128
restoring
domain configuration database 38
PowerCenter repository for Metadata Manager 191
repositories 281
result set cache properties
Data Integration Service 173
roles
Administrator 104
assigning 106
custom 105
description 75
managing 103
overview 23
troubleshooting 108
root directory
process variable 220
round-robin dispatch mode
description 354
row error log files
permissions 238
rtm
permissions by command 467
privileges by command 467

run-time objects
description 92
privileges 92
Run-time Objects privilege group
description 92
run-time statistics
persisting to the repository 210
Web Services Report 409

S

safe mode
configuring for PowerCenter Integration Service 207
PowerCenter Integration Service 205
samples
odbc.ini file 523
SAP BW Service
application service 15
associated PowerCenter Integration Service 312
creating 309
disabling 310
enabling 310
general properties 311
log events 380
log events, viewing 313
managing 308
properties 311
SAP Destination R Type (property) 309, 311
SAP BW Service log
viewing 313
SAP Destination R Type (property)
SAP BW Service 309, 311
SAP NetWeaver BI Monitor
log messages 313
saprfc.ini
DEST entry for SAP NetWeaver BI 309, 311
search filters
permissions 113
Search section
Informatica Administrator 21
secure communication
Administrator tool 55
application services 53
domain 53
Service Manager 53
web applications 55
web service client 55
security
audit trail, creating 284
audit trail, viewing 380
passwords 66
permissions 29
privileges 29, 74, 77
roles 75
Security Administration privilege group
description 77
security domains
configuring LDAP 62
deleting LDAP 65
description 60
native 60
Security page
Informatica Administrator 21
keyboard shortcuts 23
Navigator 22
Security privilege group
description 86
SecurityAuditTrail
logging activities 284
server grid
licensed option 208
service levels
creating and editing 355
description 355
overview 228
Service Manager
authentication 7
authorization 2, 7
description 2
log events 377
secure communication 53
single sign-on 7
service name
log events 377
Web Services Hub 315
service process
distribution on a grid 234
enabling and disabling 30
restart, configuring 31
viewing status 35
service process variables
list of 220
Service Upgrade Wizard
upgrading services 50, 51
upgrading users 50, 51
service variables
list of 209
services
enabling and disabling 30
failover 128
resilience 127
restart 128
Service Upgrade Wizard 50, 51
services and nodes
viewing dependencies 42
Services and Nodes view
Informatica Administrator 14
session caches
description 238
session logs
directory 220
overview 240
permissions 238
session details 240
session output
cache files 242
control file 241
incremental aggregation files 242
indicator file 241
performance details 240
persistent lookup cache 242
post-session email 241
reject files 240
session logs 240
target output file 241
SessionExpiryPeriod (property)
Web Services Hub 319
sessions
caches 238
DTM buffer memory 237
output files 238
performance details 240
running on a grid 235
session details file 240
sort order 427

severity
log events 377
shared file systems
high availability 132
shared library
configuring the PowerCenter Integration Service 213
shared storage
PowerCenter Integration Service 218
state of operations 218
shortcuts
keyboard 23
Show Custom Properties (property)
user preference 11
shutting down
Informatica domain 43
SID/Service Name
description 194
single sign-on
description 7
SMTP configuration
alerts 26
sort order
code page 427
SQL data services 178
source data
blocking 233
source databases
code page 428
connecting through ODBC (UNIX) 521
source files
directory 220
source pipeline
pass-through 230
reading 233
target load order groups 233
sources
code pages 428, 442
database resilience 128
privileges 91
reading 233
Sources and Targets privilege group
description 91
sql
permissions by command 467
privileges by command 467
SQL data service
changing the service name 183
inherited permissions 119
permission types 120
permissions 119
SQL data services
monitoring 392
properties 178
SSL certificate
LDAP authentication 61, 65
stack traces
viewing 372
startup type
configuring applications 178
configuring SQL data services 178
state of operations
domain 129
PowerCenter Integration Service 129, 141, 218
PowerCenter Repository Service 129, 137
shared location 218
statistics
for monitoring 384
Web Services Hub 407
Stop option
disable Integration Service process 203
disable PowerCenter Integration Service 203
disable the Web Services Hub 316
stopping
Informatica domain 43
stored procedures
code pages 430
Subscribe for Alerts
user preference 11
subset
defined for code page compatibility 424
Sun Java System Directory Service
LDAP authentication 60
superset
defined for code page compatibility 424
Sybase ASE
connect string syntax 492
connecting to Integration Service (UNIX) 512
connecting to Integration Service (Windows) 499
symmetric processing platform
pipeline partitioning 236
synchronization
LDAP users 60
times for LDAP directory service 64
users 7
system locales
description 420
system memory
increasing 69
system-defined roles
Administrator 104
assigning to users and groups 106
description 103

T

table owner name
description 263
tablespace name
for repository database 263, 307
tablespaces
single node 483
target databases
code page 428
connecting through ODBC (UNIX) 521
target files
directory 220
output files 241
target load order groups
mappings 233
targets
code pages 428, 442
database resilience 128
output files 241
privileges 91
session details, viewing 240
tasks
dispatch priorities, assigning 228, 355
dispatching 226
TCP KeepAlive timeout
high availability 142
TCP/IP network protocol
nodes 487
PowerCenter Client 487
PowerCenter domains 487
requirement for Integration Service 491

temporary files
directory 220
Teradata
connect string syntax 492
connecting to an Informatica client (Windows) 500, 513
connecting to an integration service (Windows) 500, 513
testing
database connections 329
thread identification
Logs tab 377
thread pool size
configuring maximum 166
threads
creation 230
Log Manager 377
mapping 230
master 230
post-session 230
pre-session 230
reader 230
transformation 230
types 231
writer 230
time zone
Log Manager 371
timeout
SQL data service connections 178
writer wait timeout 213
Timeout Interval (property)
description 196
timestamps
Log Manager 377
TLS Protocol
configuring 146
Tools privilege group
domain 81
PowerCenter Repository Service 88
Tracing
error severity level 210, 319
TreatCHARAsCHAROnRead
option 212
TreatDBPartitionAsPassThrough
option 213
TreatNullInComparisonOperatorsAs
option 213
troubleshooting
catalina.out 370
code page relaxation 433
environment variables 32
grid 352
localhost_.txt 370
node.log 370
TrustStore
option 210

U

UCS-2
description 419
Unicode
GB18030 419
repositories 419
UCS-2 419
UTF-16 419
UTF-32 419
UTF-8 419
Unicode mode
code pages 238
overview 421
Unicode data movement mode, setting 209
UNIX
code pages 423
connecting to ODBC data sources 521
UNIX environment variables
LANG_C 423
LC_ALL 423
LC_CTYPE 423
unregistering
local repositories 276
plug-ins 283
UpdateColumnOptions
substituting column values 122
upgrading
Service Upgrade Wizard 50, 51
URL scheme
Metadata Manager 195
Web Services Hub 315, 318
user accounts
changing the password 10
created during installation 58
default 58
enabling 67
managing 9
overview 58
user activity
log event categories 381
user connections
closing 279
managing 277
viewing 278
user description
invalid characters 66
user detail
License Management Report 403
user locales
description 420
user management
log events 377
user preferences
description 11
editing 11
user security
description 6
user summary
License Management Report 403
user-based security
users, deleting 68
users
assigning to groups 67
invalid characters 66
large number of 69
license activity, monitoring 400
managing 66
notifications, sending 280
overview 23
privileges, assigning 106
provider-based security 68
roles, assigning 106
synchronization 7
system memory 69
user-based security 68
valid name 66
UTF-16
description 419

UTF-32
description 419
UTF-8
description 419
repository 427
repository code page, Web Services Hub 315
writing logs 210

V

valid name
groups 69
user account 66
ValidateDataCodePages
option 213
validating
code pages 431
licenses 360
source and target code pages 213
version control
enabling 273
repositories 273
viewing
dependencies for services and nodes 42
virtual column properties
configuring 179
virtual schema
inherited permissions 119
permissions 119
virtual stored procedure
inherited permissions 119
permissions 119
virtual table
inherited permissions 119
permissions 119
virtual table properties
configuring 179

W

Warning
error severity level 210, 319
web applications
secure communication 55
web service
changing the service name 183
downloading the WSDL 183
enabling 183
operation properties 181
permission types 124
permissions 123
properties 180
web service client
secure communication 55
web service operation
permissions 123
web services
monitoring 395
Web Services Hub
advanced properties 317, 319
application service 6, 15
associated PowerCenter repository 321
associated Repository Service 315, 321, 322
associated repository, adding 321
associated repository, editing 322
associating a PowerCenter repository Service 315
character encoding 318
creating 315
custom properties 317
disable with Abort option 316
disable with Stop option 316
disabling 316
domain for associated repository 315
DTM timeout 319
enabling 316
general properties 317, 318
host names 315, 318
host port number 315, 318
Hub Logical Address (property) 319
internal host name 315, 318
internal port number 315, 318
keystore file 315, 318
keystore password 315, 318
license 315, 318
location 315
log events 381
MaxISConnections 319
node 315
node assignment 317, 318
password for administrator of associated repository 321, 322
properties, configuring 317
security domain for administrator of associated repository 321
service name 315
SessionExpiryPeriod (property) 319
statistics 407
tasks on Informatica Administrator 314
URL scheme 315, 318
user name for administrator of associated repository 321, 322
user name for associated repository 315
user password for associated repository 315
version 315
Web Services Hub Service
custom properties 320
Web Services Report
activity data 407
Average Service Time (property) 407
Avg DTM Time (property) 407
Avg. No. of Run Instances (property) 407
Avg. No. of Service Partitions (property) 407
complete history statistics 410
contents 407
Percent Partitions in Use (property) 407
run-time statistics 409
Within Restart Period (property)
Informatica domain 31
worker node
configuring as gateway 37
description 2
worker service process
description 234
workflow log files
directory 220
workflow logs
overview 239
permissions 238
workflow output
email 241
workflow logs 239
workflow schedules
safe mode 206
workflows
running on a grid 234
writer wait timeout
configuring 213

WriterWaitTimeOut
option 213

X

X Virtual Frame Buffer
for License Report 400
for Web Services Report 400
XML
exporting logs in 375
XMLWarnDupRows
option 213

Z

ZPMSENDSTATUS
log messages 313