Informatica Metadata Manager Command Reference
Version 10.2
September 2017

© Copyright Informatica LLC 2016, 2017

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

Informatica, the Informatica logo, and PowerCenter are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html. Other company and product names may be trade marks or trademarks of their respective owners.

U.S. GOVERNMENT RIGHTS: Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

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

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

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

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

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

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

This 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.

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

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

This product includes software copyright 1996-2006 Per Boiten. 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 software 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.opensp.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.


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

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

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


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

NOTICES

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

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, please report them to us in writing at Informatica LLC 2100 Seaport Blvd. Redwood City, CA 94063.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMASTIC PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR ANY WARRANTY OF NON-INFRINGEMENT.

Publication Date: 2017-09-04
# Table of Contents

**Preface** ................................................................. 9

Informatica Resources .......................................................... 9
  Informatica Network ......................................................... 9
  Informatica Knowledge Base ............................................... 9
  Informatica Documentation ................................................ 9
  Informatica Product Availability Matrixes .............................. 10
  Informatica Velocity ........................................................ 10
  Informatica Marketplace ..................................................... 10
  Informatica Global Customer Support .................................... 10

**Chapter 1: mmcmd** .......................................................... 11

mmcmd Overview ............................................................. 12
Certificate Validation for mmcmd ........................................... 13
MMCmdConfig.properties File ............................................... 13
Running Commands ............................................................ 14
mmcmd Commands ............................................................. 14
assignConnection .............................................................. 16
  assignConnection Syntax ................................................... 17
  assignConnection Options .................................................. 17
assignParameterFile ........................................................... 18
  assignParameterFile Syntax ................................................ 19
  assignParameterFile Options .............................................. 19
backupConfiguration .......................................................... 20
  backupConfiguration Syntax ................................................ 20
  backupConfiguration Options ............................................. 21
cancel ......................................................................... 22
  cancel Syntax ................................................................. 22
  cancel Options ............................................................... 22
connect ........................................................................ 23
  connect Syntax ............................................................... 24
  connect Options ............................................................. 24
createLinkRuleSet ............................................................. 25
  createLinkRuleSet Syntax ................................................... 25
  createLinkRuleSet Options ................................................ 25
createLoadTemplate ........................................................... 27
  createLoadTemplate Syntax ................................................ 27
  createLoadTemplate Options .............................................. 27
createResource ............................................................... 28
  createResource Syntax ...................................................... 28
  createResource Options .................................................... 29
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>getResource Options</td>
<td>53</td>
</tr>
<tr>
<td>getResourceFiles</td>
<td>54</td>
</tr>
<tr>
<td>getResourceFiles Syntax</td>
<td>55</td>
</tr>
<tr>
<td>getResourceFiles Options</td>
<td>55</td>
</tr>
<tr>
<td>getServiceLog</td>
<td>56</td>
</tr>
<tr>
<td>getServiceLog Syntax</td>
<td>56</td>
</tr>
<tr>
<td>getServiceLog Options</td>
<td>56</td>
</tr>
<tr>
<td>help</td>
<td>58</td>
</tr>
<tr>
<td>help Syntax</td>
<td>58</td>
</tr>
<tr>
<td>help Options</td>
<td>58</td>
</tr>
<tr>
<td>import</td>
<td>58</td>
</tr>
<tr>
<td>import Syntax</td>
<td>58</td>
</tr>
<tr>
<td>import Options</td>
<td>58</td>
</tr>
<tr>
<td>importLinkRuleSets</td>
<td>60</td>
</tr>
<tr>
<td>importLinkRuleSets Syntax</td>
<td>60</td>
</tr>
<tr>
<td>importLinkRuleSets Options</td>
<td>60</td>
</tr>
<tr>
<td>importModel</td>
<td>62</td>
</tr>
<tr>
<td>importModel Syntax</td>
<td>62</td>
</tr>
<tr>
<td>importModel Options</td>
<td>62</td>
</tr>
<tr>
<td>link</td>
<td>63</td>
</tr>
<tr>
<td>link Syntax</td>
<td>64</td>
</tr>
<tr>
<td>link Options</td>
<td>64</td>
</tr>
<tr>
<td>listLoadTemplates</td>
<td>65</td>
</tr>
<tr>
<td>listLoadTemplates Syntax</td>
<td>65</td>
</tr>
<tr>
<td>listLoadTemplates Options</td>
<td>65</td>
</tr>
<tr>
<td>listModels</td>
<td>67</td>
</tr>
<tr>
<td>listModels Syntax</td>
<td>67</td>
</tr>
<tr>
<td>listModels Options</td>
<td>67</td>
</tr>
<tr>
<td>listResources</td>
<td>68</td>
</tr>
<tr>
<td>listResources Syntax</td>
<td>68</td>
</tr>
<tr>
<td>listResources Options</td>
<td>69</td>
</tr>
<tr>
<td>load</td>
<td>70</td>
</tr>
<tr>
<td>load Syntax</td>
<td>70</td>
</tr>
<tr>
<td>load Options</td>
<td>70</td>
</tr>
<tr>
<td>migrateBGLinks</td>
<td>72</td>
</tr>
<tr>
<td>migrateBGLinks Syntax</td>
<td>72</td>
</tr>
<tr>
<td>migrateBGLinks Options</td>
<td>72</td>
</tr>
<tr>
<td>purgeMetadata</td>
<td>73</td>
</tr>
<tr>
<td>purgeMetadata Syntax</td>
<td>74</td>
</tr>
<tr>
<td>purgeMetadata Options</td>
<td>74</td>
</tr>
<tr>
<td>restoreConfiguration</td>
<td>75</td>
</tr>
<tr>
<td>restoreConfiguration Syntax</td>
<td>75</td>
</tr>
</tbody>
</table>
# Table of Contents

- deleteRepository .................................................. 100
  deleteRepository Syntax ........................................ 100
  deleteRepository Options ....................................... 100
- restorePCRepository ................................................. 102
  restorePCRepository Syntax ..................................... 103
  restorePCRepository Options ................................... 103
- restoreRepository ................................................... 104
  restoreRepository Syntax ....................................... 104
  restoreRepository Options ..................................... 104

## Chapter 4: mmXConPluginUtil .............................................. 107

- mmXConPluginUtil Overview ...................................... 107
- Running Commands .................................................. 108
- mmXConPluginUtil Commands ..................................... 108
- generateImageMapping ............................................. 108
  generateImageMapping Syntax .................................. 108
  generateImageMapping Options ................................ 109
- generatePlugin ....................................................... 109
  generatePlugin Syntax ........................................... 109
  generatePlugin Options ......................................... 109

## Chapter 5: rcfmu .......................................................... 110

- rcfmu Overview ..................................................... 110
- rcfmu Migration Rules for Resource Properties ................. 110
- Running rcfmu ....................................................... 111
- rcfmu Syntax ......................................................... 112
- rcfmu Options ....................................................... 112
  JDBC Parameters for Secure Databases .......................... 114

## Chapter 6: rmu ............................................................ 116

- rmu Overview ......................................................... 116
- rmu Migration Rules for Resource Properties ................... 117
- Running rmu .......................................................... 118
- rmu Syntax ........................................................... 118
- rmu Options ........................................................ 118
  rmu Configuration File Format .................................. 119
  rmu Sample Configuration File .................................. 120

Index ................................................................. 122
Preface

The Metadata Manager Command Reference provides information about Metadata Manager command line programs. This guide is written for Metadata Manager administrators who use command line programs to load and manage resources, back up and restore the repository, and migrate resources across Metadata Manager versions.

Informatica Resources

Informatica Network


As a member, you can:

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

Informatica Knowledge Base

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

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

Informatica Documentation

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

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

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

Informatica Velocity

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

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

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

Informatica Marketplace

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

Informatica Global Customer Support

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

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

If you are an Informatica Network member, you can use Online Support at http://network.informatica.com.
CHAPTER 1

mmcmd

This chapter includes the following topics:

- mmcmd Overview, 12
- Certificate Validation for mmcmd, 13
- MMCmdConfig properties File, 13
- Running Commands, 14
- mmcmd Commands, 14
- assignConnection, 16
- assignParameterFile, 18
- backupConfiguration, 20
- cancel, 22
- connect, 23
- createLinkRuleSet, 25
- createLoadTemplate, 27
- createResource, 28
- deleteLinkRuleSet, 30
- deleteLoadTemplate, 32
- deleteResource, 34
- encrypt, 35
- exit, 36
- export, 36
- exportLinkRuleSetDefs, 38
- exportLinkRuleSets, 39
- exportLoadLog, 41
- exportModel, 43
- exportObject, 45
- generateDefaultLoadTemplate, 47
- getLinkReport, 49
- getLoadTemplate, 51
- getResource, 52
- getResourceFiles, 54
- getServiceLog, 56
mmcmd Overview

mmcmd is a command line program that loads and manages resources, imports and exports models and custom resources, creates and deletes Metadata Manager repository contents, and restores PowerCenter® repository contents.

mmcmd is installed when you run the Informatica services installer or the Informatica client installer. You can also install mmcmd on any machine when you install Informatica utilities. mmcmd is installed as a batch file on Windows and as a shell script on UNIX.

mmcmd is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities\mmcmd`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\mmcmd`
- `<Informatica utilities installation directory>\MetadataManager\utilities\mmcmd`

Run mmcmd from the command line. You can issue commands directly or from a script, batch file, or other program.

Use mmcmd in the following modes:
Command Line Mode

You invoke and exit mmcmd each time you issue a command. You can write scripts with the command line syntax. Each command that you write in command line mode must include connection information to the Metadata Manager Service.

Interactive Mode

You establish and maintain an active connection to the Metadata Manager Service. In interactive mode, you can issue a series of commands. To start interactive mode, enter `mmcmd` at the command line. To exit interactive mode, use the `exit` command.

Certificate Validation for mmcmd

If you configure a secure connection between the Metadata Manager web application and the Metadata Manager Service, you must configure mmcmd to use the truststore file. mmcmd uses the truststore file to validate the security certificates. mmcmd does not accept a security certificate that has errors.

To configure mmcmd to use the truststore file, edit the `MMCmdConfig.properties` file. Set the `TrustStore.Path` property to the path and file name of the truststore file.

If you do not configure a secure connection for the Metadata Manager web application, do not specify a truststore file. Leave the `TrustStore.Path` property in the `MMCmdConfig.properties` file empty.

MMCmdConfig.properties File

Use the `MMCmdConfig.properties` file to configure mmcmd properties such as the truststore file, server polling interval, and server connection timeout period.

`MMCmdConfig.properties` is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities\mmcmd\config`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\MM\mmcmd\config`
- `<Informatica utilities installation directory>\MetadataManager\utilities\mmcmd\config`

**Note**: There are separate copies of the `MMCmdConfig.properties` file for mmcmd and for mmRepoCmd.

You can configure the following properties:

**TrustStore.Path**

Required if you configure a secure connection for the Metadata Manager web application. Path and file name of the truststore file that contains the public key.

If you do not configure a secure connection for the Metadata Manager web application, leave this property empty.

**Server.PollInterval**

Amount of time in milliseconds that the command line program waits before querying the Metadata Manager application. The program queries for the status of the last command when you run a command in wait mode. Default is 6000.
Server.ConnectionTimeOut

Number of milliseconds after which the remote connection to the Metadata Manager Service times out. Default is 86,400,000 (24 hours).

Running Commands

When you run mmcmd, you enter options for each command, followed by the required arguments. Command options are preceded by a hyphen and are not case sensitive. Arguments follow the option.

For example, the following command starts a resource load for the Oracle_DB resource:

```
mmcmd load -url http://localhost:10250 -r Oracle_DB -u dave -pw ******
```

If you omit or incorrectly enter one of the required options, the command fails, and mmcmd returns an error message.

1. At the command prompt, switch to the directory where mmcmd is located.
2. Enter `mmcmd` on Windows or `mmcmd.sh` on UNIX followed by the command name and its required options and arguments.

   For example:

   ```
   mmcmd(.sh) command_name [-option1] argument_1 [-option2] argument_2...
   ```

   The command names are not case sensitive.

mmcmd Commands

The following table describes the mmcmd commands:

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assignConnection</td>
<td>Configures connection assignments for a resource based on the properties in the specified resource configuration file.</td>
</tr>
<tr>
<td>assignParameterFile</td>
<td>Assigns parameter files to PowerCenter workflows for a PowerCenter resource based on the properties in the specified resource configuration file.</td>
</tr>
<tr>
<td>backupConfiguration</td>
<td>Backs up the resource configurations, source files associated with resources, linking rules associated with resources, and custom models for a Metadata Manager instance.</td>
</tr>
<tr>
<td>cancel</td>
<td>Cancels a resource load.</td>
</tr>
<tr>
<td>connect</td>
<td>Connects the mmcmd program to the Metadata Manager Service in the interactive mode.</td>
</tr>
<tr>
<td>createLinkRuleSet</td>
<td>Creates a linking rule set for a pair of resources, a rule set definition for a pair of models, or a rule set parameter definition for a pair of resources in the Metadata Manager repository.</td>
</tr>
<tr>
<td>createLoadTemplate</td>
<td>Creates a load template file.</td>
</tr>
<tr>
<td>Command Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>createResource</td>
<td>Creates a resource based on the properties in the specified resource configuration file.</td>
</tr>
<tr>
<td>deleteLinkRuleSet</td>
<td>Removes a linking rule set for a pair of resources or a rule set definition for a pair of models from the Metadata Manager repository.</td>
</tr>
<tr>
<td>deleteLoadTemplate</td>
<td>Deletes a load template.</td>
</tr>
<tr>
<td>deleteResource</td>
<td>Deletes the resource and all metadata for the resource from the Metadata Manager repository.</td>
</tr>
<tr>
<td>encrypt</td>
<td>Encrypts the text you specify. You can specify the encrypted text when you use the -ep option in a command or in a resource configuration file.</td>
</tr>
<tr>
<td>exit</td>
<td>In interactive mode, disconnects mmcmd from the Metadata Manager Service and closes the mmcmd program.</td>
</tr>
<tr>
<td>export</td>
<td>Exports a custom resource from the Metadata Manager repository to an XML file. You can import it into another Metadata Manager repository.</td>
</tr>
<tr>
<td>exportLinkRuleSetDefs</td>
<td>Exports all linking rule set definitions for a model to XML files.</td>
</tr>
<tr>
<td>exportLinkRuleSets</td>
<td>Exports all linking rule sets for a resource to XML files.</td>
</tr>
<tr>
<td>exportLoadLog</td>
<td>Exports the load details for a resource to a Microsoft Excel file.</td>
</tr>
<tr>
<td>exportModel</td>
<td>Exports a model from the Metadata Manager repository. You can import it into another Metadata Manager repository.</td>
</tr>
<tr>
<td>exportObject</td>
<td>Exports a metadata catalog object from the Metadata Manager repository. You can export metadata objects to the Adobe PDF, HTML, or Microsoft Excel file types.</td>
</tr>
<tr>
<td>generateDefaultLoadTemplate</td>
<td>Generates a default load template to load all top level classes for the specified model.</td>
</tr>
<tr>
<td>getLinkReport</td>
<td>Exports the link report. The link summary report contains the resource, connection, assigned database, and assigned schema details.</td>
</tr>
<tr>
<td>geLoadTemplate</td>
<td>Exports a load template file.</td>
</tr>
<tr>
<td>getResource</td>
<td>Writes properties for the specified resource to a resource configuration file.</td>
</tr>
<tr>
<td>getResourceFiles</td>
<td>Retrieves all the source files associated with a resource, including rule sets. Metadata Manager retrieves parameter files for PowerCenter resources and retrieves model files for data modeling resources.</td>
</tr>
<tr>
<td>getServiceLog</td>
<td>Exports the service log file from Metadata Manager for a specified date.</td>
</tr>
<tr>
<td>help</td>
<td>Returns help for an mmcmd command.</td>
</tr>
<tr>
<td>import</td>
<td>Imports the metadata for a custom resource from an XML file into the Metadata Manager repository.</td>
</tr>
<tr>
<td>importLinkRuleSets</td>
<td>Imports all linking rule sets from XML files in the specified path into the Metadata Manager repository.</td>
</tr>
<tr>
<td>Command Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>importModel</td>
<td>Imports a model from a file into the Metadata Manager repository.</td>
</tr>
<tr>
<td>link</td>
<td>Creates the links between resources to run data lineage analysis across metadata sources. Before you create links for a resource, you must configure connection assignments or linking rules for the resource.</td>
</tr>
<tr>
<td>listLoadTemplates</td>
<td>Lists all the load template files for a custom resource.</td>
</tr>
<tr>
<td>listModels</td>
<td>Lists all models in Metadata Manager.</td>
</tr>
<tr>
<td>listResources</td>
<td>Lists all resources in the Metadata Manager repository.</td>
</tr>
<tr>
<td>load</td>
<td>Starts a resource load. Metadata Manager adds the resource load to the load queue.</td>
</tr>
<tr>
<td>migrateBGLinks</td>
<td>Restores the related catalog objects for a business glossary after you upgrade from version 9.5.x.</td>
</tr>
<tr>
<td>purgeMetadata</td>
<td>Deletes metadata for a resource from the Metadata Manager repository. You cannot recover the purged metadata. Back up the Metadata Manager repository database before you purge metadata.</td>
</tr>
<tr>
<td>restoreConfiguration</td>
<td>Restores the resource configurations, source files associated with resources, linking rules associated with resources, and custom models from a back-up file.</td>
</tr>
<tr>
<td>resume</td>
<td>Resume a failed resource load. If a resource load fails when PowerCenter runs the workflows that load the metadata into the warehouse, you can resume the resource load.</td>
</tr>
<tr>
<td>search</td>
<td>Searches for objects in the Metadata Manager repository using a keyword search.</td>
</tr>
<tr>
<td>status</td>
<td>View the status of a running or completed resource load.</td>
</tr>
<tr>
<td>testSourceConnection</td>
<td>Tests connection to the source system of a resource.</td>
</tr>
<tr>
<td>updateLinkRuleSet</td>
<td>Updates a linking rule set for a pair of resources or a rule set definition for a pair of models in the Metadata Manager repository.</td>
</tr>
<tr>
<td>updateLoadTemplate</td>
<td>Updates a load template file.</td>
</tr>
<tr>
<td>updateResource</td>
<td>Updates a resource based on the properties in the specified resource configuration file.</td>
</tr>
<tr>
<td>version</td>
<td>Displays the current version of Metadata Manager.</td>
</tr>
</tbody>
</table>

**assignConnection**

Configures connection assignments for a resource based on the properties in the specified resource configuration file. Connection assignments are connections between two metadata sources. Metadata Manager uses connections to run data lineage across metadata sources.

Use the assignConnection command when you move resources from a development to a production environment. After you create a resource based on a resource configuration file, you might need to change
the connection assignments in the resource configuration file. You then use the assignConnection command to update the resource with the modified connection assignments.

**assignConnection Syntax**

The command uses the following syntax:

```
[<-dn|--domainName> domainName]  
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]  
[<-mm|--mmServiceName> mmServiceName]  
<<-url>>  
<<-u|--user> user>  
[<-ep|--encryptedPassword]  
[<-pw|--password> password]  
[<-n|--namespace> namespace]  
[<-kt|--keyTab> keyTab]  
<<-r|--resource> resource>  
<<rcf|--resourceConfigurationFile> resourceConfigurationFile>  
[-s|--skipConfFetch]  
[<-pdir> paramFileDir]
```

**assignConnection Options**

The command uses the following options:

**[<-dn | --domainName>]**

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

**[<-hp | --gateway>]**

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

**[<-mm | --mmServiceName>]**

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

**<<-url>>**

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

**<<-u | --user>>**

Metadata Manager user name.
[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+gtFyB2KYLXID9jgC+6WbM0g/94A08RlnOC1vd0=
```

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n | --namespace]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[-kt | --keyTab]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>
Name of the Metadata Manager resource for which you want to configure connections. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>
XML file name and path for the resource configuration file that contains the modified connection assignments. If you do not include a path, mmcmd looks for the XML file in the mmcmd directory.

The source files of the resource must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If you do not specify the path, mmcmd looks for the source files in the mmcmd directory.

[-s | --skipConFetch]
During refresh, skips retrieving the connection objects you specify in the resource configuration file.

Before you use this option, verify that the connection object is available so that the connection assignment does not fail.

[-pdir-]
Directory where the source files of the Metadata Manager resources are stored.

**assignParameterFile**

Assigns parameter files to PowerCenter workflows for a PowerCenter resource based on the properties in the specified resource configuration file.

Use the assignParameterFile command when you move PowerCenter resources from a development to a production environment. After you create a PowerCenter resource based on a resource configuration file, you might need to change the PowerCenter parameter file assignments in the resource configuration file. You
then use the assignParameterFile command to update the resource with the modified parameter file assignments.

assignParameterFile Syntax

The command uses the following syntax:

```
[<-dn | --domainName> domainName]
[<-hp | --gateway> gateway_host1:port gateway_host2:port...]
[<-mm | --mmServiceName> mmServiceName]
<<-url>> http[s]://<host>[:<port>>
<<-u | --user> user>
[-ep|--encryptedPassword] 
[-pw|--password> password]
[-n|--namespace> namespace] 
[-kt|--keyTab> keyTab] 
<<-r|--resource> resource>
<<rcf|--resourceConfigurationFile> resourceConfigurationFile>
[<pdir> paramFileDir]
```

assignParameterFile Options

The command uses the following options:

**[<-dn | --domainName>]**

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

**[<-hp | --gateway>]**

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

**[<-mm | --mmServiceName>]**

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

**<<-url>>**

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http[s]://<host>[:<port>>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

**<<-u | --user>>**

Metadata Manager user name.
[<-ep | --encryptedPassword>]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -p WP+gtfYwB2KYLXlD9jgC+6WHbM0g/94A08Rln0Clvd0=
```

[<pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note**: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[<-r | --resource>]
Name of the PowerCenter resource for which you want to configure PowerCenter parameter files. If the resource name contains spaces, enclose the resource name in quotes.

[<-rcf | --resourceConfigurationFile>]
XML file name and path for the resource configuration file that contains the modified PowerCenter parameter file assignments. If you do not include a path, mmcmd looks for the XML file in the mmcmd directory.

The parameter files must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If not specified, mmcmd looks for the parameter files in the mmcmd directory.

[<-pdir>]
Directory where the parameter files of the PowerCenter resource are stored.

backupConfiguration

Backs up the resource configurations, source files associated with resources, linking rules associated with resources, and custom models for a Metadata Manager instance.

backupConfiguration Syntax

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
<<url> http(s)://<host>[:<port>>
```
The command uses the following options:

[-dn | --domainName]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[-hp | --gateway]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

- hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

- ep -pw Wf+gtfYwB2KYLXID9jgC+6WbMOg/94A08R1nOC1vd0=

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

- pw Administrator
**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-file>>
Path and file name of the back-up file. If you do not specify a .cbkp extension, mmcmd appends `.cbkp` to the file name. If you do not include a path, mmcmd saves the back-up file in the mmcmd directory.

**cancel**

Cancels a resource load.

**cancel Syntax**

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<-url> http(s)://<host>:<port>>
[<-u|--user> user>]
[<-ep|--encryptedPassword]  
[<-pw|--password> password]  
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]  
[<-r|--resource> resource>]
```

**cancel Options**

The command uses the following options:

[<-dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

[-url]
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http[s]://<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[-u | --user]
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtYwB2KYLXg9jgC+6WbMg/94A08Rl0Clvd0=

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n | --namespace]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[-kt | --keyTab]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[-r | --resource]
Name of the resource for which you want to cancel the load. If the resource name contains spaces, enclose the resource name in quotes.

connect

Connects the mmcmd program to the Metadata Manager Service in the interactive mode. After mmcmd successfully connects, you can issue commands without reentering the connection information.
connect Syntax

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
<<url> http(s)://<host>:<port>>
<<u|--user> user
[-ep|--encryptedPassword]
[<pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
```

connect Options

The command uses the following options:

```
[<dn|--domainName>]
  Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.
  This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<hp|--gateway>]
  Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
  If there are multiple gateway nodes, separate the gateways with a space. For example:
  -hp host1:6001 host2:6002
  Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<mm|--mmServiceName>]
  Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<url>>
  Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.
  If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<u|--user>>
  Metadata Manager user name.

[-ep|--encryptedPassword]
  Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
  -ep -pw WP+qtfYwB2KYLXID9jgc+6W6bMOg/94A08R1n0C1vd0=
```
[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

## createLinkRuleSet

Creates a linking rule set for a pair of resources, a rule set definition for a pair of models, or a rule set parameter definition for a pair of resources in the Metadata Manager repository. Creates the rule set, rule set definition, or rule set parameter definition based on a linking rules file.

### createLinkRuleSet Syntax

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
[<url> http(s)://<host>:<port>]
[<ul|--user> user]
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<file> rule set xml|rule set definition xml|rule set parameter xml]
```

### createLinkRuleSet Options

The command uses the following options:

[<-dn|--domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.
[<-hp | --gateway>]
  Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
  If there are multiple gateway nodes, separate the gateways with a space. For example:

  -hp host1:6001 host2:6002

  **Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
  Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
  Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.
  If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
  Metadata Manager user name.

[-ep | --encryptedPassword]
  Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

  -ep -pw WP+qtfYwB2KYLXID9JgC+6WbM0g/94A08R1nOC1vd0=

[<-pw | --password>]
  Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

  -pw Administrator

  **Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
  Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
  Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-file>>
  XML file name and path for the linking rules file that you use to create the rule set, the rule set definition, or the rule set parameter definition.
If you specify a rule set file, this command creates a rule set for the resources named in the file. If you
specify a rule set definition file, this command creates a rule set definition for the models named in the
file. If you specify a rule set parameter file, this command creates a rule set for the resources named in
the file when a rule set definition exists for the models.

Default path is the mmcmd directory.

createLoadTemplate

Creates a load template file.

createLoadTemplate Syntax

The command uses the following syntax:

```bash
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<-url> http(s)://<host>:<port>]
[<-u|--user> user]
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-f|--File> File]
```

createLoadTemplate Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name
of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is
missing or contains connectivity information that is out of date, you must use the --gateway option
instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option.
Also required if the domain uses Kerberos authentication and the domains.infa file is missing or
contains connectivity information that is out of date. Host names and port numbers of the gateway
nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```bash
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities
are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

Metadata Manager user name.

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KLhX9jgC+6WHbiMOg/94A08R1nOC1vd0=
```

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

Name of the load template file.

---

**createResource**

Creates a resource based on the properties in the specified resource configuration file. Use the createResource command when you move resources from a development to a production environment.

**createResource Syntax**

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
[<url> http(s)://<host>:<port>]
[<u|--user> user]
[<ep|--encryptedPassword>]
```
createResource Options

The command uses the following options:

[-dn | --domainName]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[-hp | --gateway]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:
- hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<-u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
-ep -pw WP+qtfYwB2KYLXI09jgC6WHeM0g/94A0SR1n0C1vd0=

[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:
-pw Administrator

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource that you want to create. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>

File name and path for the resource configuration file that contains the resource properties. You can import a resource configuration file (.rcf file). Alternatively, you can import a resource configuration file that also contains all the rule sets and rule set parameter definitions associated with the resource (.rcz file). If you do not include a path, mmcmd looks for the file in the mmcmd directory.

The source files of the resource must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If you do not specify a path, mmcmd looks for the source files in the mmcmd directory.

[<-pdir>]

Directory where Metadata Manager stores the source files for the resources.

[<-rpw | --resourcePassword>]

Required if the resource uses a password and the resource configuration file does not contain the resource password. Resource password in plain text.

[<-sjp | --secureJDBCParameters>]

Secure JDBC parameters that you want to append to the JDBC connection URL. Use this option with database management resources to specify secure connection parameters such as passwords. Metadata Manager does not display secure parameters or parameter values in the resource configuration properties. Enter the parameters as name=value pairs separated by the delimiter character that the database driver requires.

If secure communication is enabled for the metadata source database, enter the secure JDBC parameters in this option.

deleteLinkRuleSet

Removes a linking rule set for a pair of resources or a rule set definition for a pair of models from the Metadata Manager repository.
deleteLinkRuleSet Syntax

The command uses the following syntax:

```plaintext
[-<mm | --mmServiceName> mmServiceName]
[-url> http(s)://<host>:<port>]
[-u | --user> user]
[-ep | --encryptedPassword]
[-pw | --password> password]
[-n | --namespace> namespace]
[-k | --keyTab> keyTab]
[-rn|--rule set id|--rule set definition id|--rule set parameter id> string>
[-force]
```

deleteLinkRuleSet Options

The command uses the following options:

`[-<dn | --domainName>]`

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

`[-hp | --gateway>]`

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

`[-mm | --mmServiceName>]`

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

`[-url>]`

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

`[-u | --user>]`

Metadata Manager user name.

`[-ep | --encryptedPassword]`

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
deleteLoadTemplate

Deletes a load template file.

deleleLoadTemplate Syntax

The command uses the following syntax:

```bash
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
[<url> http(s): //<host>:<port>>
[<u|--user> user]
[<ep|--encryptedPassword>]
[<pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
[<na|--Name> Name]
```

deleleLoadTemplate Options

The command uses the following options:

- `-ep` `-pw WP+qtFYw82YLYXID9jgC+6WbMOg/94A08RlnOC1vd0=

```bash
[<pw|--password>]
```

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the `--keyTab` option. Password for the Metadata Manager user. For example:

```bash
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the `--encryptedPassword` option in addition to this option.

```bash
[<n|--namespace>]
```

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

```bash
[<kt|--keyTab>]
```

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

```bash
[<rn|--rule setId|rule set definition id|rule set parameter id>]
```

Name of the rule set or rule set definition that you want to delete. If you delete a rule set for a resource by removing the rule set parameter definition, this option specifies the ID of the rule set parameter definition.

```bash
[-force]
```

Deletes the rule set definition and all parameters associated with it. If you delete a rule set definition that has parameters associated with it, specify this option to delete the rule set definition.
[<-dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.
This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
If there are multiple gateway nodes, separate the gateways with a space. For example:

```-hp host1:6001 host2:6002```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
Metadata Manager user name.

[<-ep | --encryptedPassword>]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```-ep -pw WP+qtfYwB2KYLXID9jgC+6W9bM0g/94A08R1nOC1vd0=`

[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```-pw Administrator```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
deleteResource

Deletes the resource and all metadata for the resource from the Metadata Manager repository.

deleteResource Syntax

The command uses the following syntax:

[-dn | --domainName> domainName]
[-hp | --gateway>] gateway_host1:port gateway_host2:port...
[-mm | --mmServiceName> mmServiceName]
[<-url] http(s):<host>[:port>]
[-<u|--user> user>]
[-<ep|--encryptedPassword>]
[-<pw|--password> password>]
[-<n|--namespace> namespace>]
[-<kt|--keyTab> keyTab]
[-<r|--resource> resource>
[-f]

deleteResource Options

The command uses the following options:

[-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the -gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the -gateway option instead.

[-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the -domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

- hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

Metadata Manager user name.

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94A08R1nOC1vd0=
```

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

Name of the Metadata Manager resource that you want to delete. If the resource name contains spaces, enclose the resource name in quotes.

Delete the resource without confirmation. If you omit this option, the command prompts you for confirmation before it deletes the resource.

**encrypt**

Encrypts the text that you specify. Specify text to encrypt when you use the --encryptedPassword (-ep) option in a command and when you use the password parameter in a resource configuration file.

The command generates and displays the encrypted data. The command uses the Informatica default encryption key to encrypt data.
encrypt Syntax

The command uses the following syntax:

`<<-data> data>`

encrypt Options

The command uses the following options:

`<<-data>>`

Text that you want to encrypt.

exit

Disconnects mmcmd from the Metadata Manager Service and closes the mmcmd program.

Note: Use this command in the mmcmd interactive mode only.

export

Exports a custom resource from the Metadata Manager repository to an XML file. You can import it into another Metadata Manager repository.

export Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<url> http(s)//<host>:<port>>
<<u|--user> user>
[<-ep|--encryptedPassword]  
[<-pw|--password> password]  
[<-n|--namespace> namespace]  
[<-kt|--keyTab> keyTab]
<<r|--resource> resource>  
<<f|--file> file>`

export Options

The command uses the following options:

`[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.
[<-hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
If there are multiple gateway nodes, separate the gateways with a space. For example:
  -hp host1:6001 host2:6002
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
  -ep -pw WP+qtFywB2KLYXjD9jgC+6WHbM0g/94A08R1n0C1vd0=

[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:
  -pw Administrator
Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>
Name of the custom resource that you want to export. If the name contains spaces, enclose the name in quotes.
exportLinkRuleSetDefs

Exports all linking rule set definitions for a model to XML files. You can import the rule set definitions into another Metadata Manager repository.

exportLinkRuleSetDefs Syntax

The command uses the following syntax:

```
[<--dn|--domainName> domainName]
[<--hp|--gateway> gateway_host1:port gateway_host2:port...]
[<--mm|--mmServiceName> mmServiceName]
[<--url> http(s)://<host>:<port>]
[<--u|--user> user]
[<--ep|--encryptedPassword]
[<--pw|--password> password]
[<--n|--namespace> namespace]
[<--kt|--keyTab> keyTab]
[<--m|--model> Model_Name]
[<--d|--dir> Export_Directory]
[<--o|--overwrite]
```

exportLinkRuleSetDefs Options

The command uses the following options:

```
[<--dn|--domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<--hp|--gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

```
[<--mm|--mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.
```
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)//<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

Metadata Manager user name.

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```bash
-ep -pw WP+qtfYwB2KLYID9jgC+6WHbM0g/94A08R1nOC1vd0=
```

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```bash
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

Name of the model that uses the rule set definitions you want to export.

Directory to which you want to export the rule set definition files.

Overwrites existing rule set definition files during export.

**exportLinkRuleSets**

Exports all linking rule sets for a resource to XML files. Optionally exports the rule set parameter definitions associated with the resource. You can import the rule sets and rule set parameter definitions into another Metadata Manager repository.
The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<-url> http(s)://<host>:<port>]
[<-u|--user> user]
[<-ep|--encryptedPassword]
[<pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<r|--resource> Resource Name]
[<-d|--dir> Export Directory]
[<-o|--overwrite]
[<includeDefs]
```

The command uses the following options:

```
[-dn | --domainName]
```

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

```
[-hp|--gateway]
```

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

```
[-mm|--mmServiceName]
```

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

```
[-url>
```

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

```
<-u|--user>
```

Metadata Manager user name.

```
[-ep|--encryptedPassword]
```

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
exportLoadLog Syntax

The command uses the following syntax:

```
[<-pw | --password>]
Exports the load details for a resource to a Microsoft Excel file.
[<-n | --namespace>]
[<-kt | --keyTab>]
<<-r | --resource>>
[-includeDefs]
[-o | --overwrite]
<<-d | --dir>>
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

**Example:**

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

Name of the resource that uses the rule sets you want to export.

Directory to which you want to export the rule set files.

Overwrites existing rule set files during export.

Exports the rule set parameter definitions in addition to the rule set definitions.

---

**exportLoadLog**

Exports the load details for a resource to a Microsoft Excel file.

**exportLoadLog Syntax**

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-s|--severity> info|warn|error>
<<-f|--file> file>
```
exportLoadLog Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

-hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtYwB2KLYX1D9jgC+6WHbM0g/94A08R1n0C1vd0=

[<pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.
[<n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[<r | --resource>]
Name of the resource for which you want to export the load log information.

[<s | --severity>]
Error severity level.
Specify one of the following levels:
- info. Metadata Manager writes informational, warning, and error messages to the log file.
- warn. Metadata Manager writes warning and error messages to the log file.
- error. Metadata Manager writes error messages to the log file.

[<f | --file>]
File name and path of the Microsoft Excel file to which you want to export the load details. You must specify a file with the .xlsx extension. If you do not specify a path, Metadata Manager creates the file in the mmcmd directory.

exportModel
Exports a model from the Metadata Manager repository to a file. You can import the file into another Metadata Manager repository.

Note: You cannot export the Business Glossary model from Metadata Manager. To export business glossary assets and templates, use the Analyst tool.

exportModel Syntax
The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<-url> http(s)://<host>[:<port>]]
[<-u|--user> user]
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-m|--modelName> modelName]
[<f|--file> file]
[<-includeRuleSets]
```

exportModel Options
The command uses the following options:
[<dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94A08R1nOC1vd0=
```

[-pw | --password] 
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
exportObject

Exports a metadata catalog object from the Metadata Manager repository.

You can export the metadata object to the following file types:

- Adobe PDF
- HTML
- Microsoft Excel

**Note:** The include options are not applicable for all metadata catalog objects. If you use an include option that is not applicable for the selected metadata object, mmcmd ignores the option.

**exportObject Syntax**

The command uses the following syntax:

```bash
[-<kt | --keyTab>]  
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[-<m | --modelName>]
Name of the model you want to export. If the model name contains spaces, enclose the model name in quotes.

You can export a packaged model, a universal model, a custom model, or multiple custom models to one export file. You cannot export a packaged model and a custom model to one export file. Similarly, you cannot export a universal model and a custom model to one export file.

[-<f | --file>]
File name and path for the model export file. If you do not include a path, mmcmd exports the model to a file in the mmcmd directory.

[-includeRuleSets]
Exports all rule set definitions associated with the model. If you specify this option, the exportModel command creates a zip file that contains the model export XML file plus an XML file for each rule set definition. If you do not specify this option, the exportModel command creates an XML file.
exportObject Options

The command uses the following options:

[-dn | --domainName]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[-hp | --gateway]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

-hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<-url>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<-u | --user>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtfYwB2KYLXID9jgC+6WbM0g/94A08R1nOClvd0=

[-pw | --password]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.
[<n | --namespace>]
  Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain
  uses native authentication. Name of the security domain to which the Metadata Manager user belongs.
  The security domain name is case sensitive.

[<kt | --keyTab>]
  Required if the domain uses Kerberos authentication and you do not specify a password. Path and file
  name of the keytab file for the Metadata Manager user.

[<l | --location>]
  Name and location of the metadata object in the catalog hierarchy that you want to export.

[<f | --file>]
  PDF, HTML, or XLS file name and path for the exported metadata object. If you do not include a path,
  mmcmd exports the metadata object to a file in the mmcmd directory.

[-includeChildren]
  Includes the object you selected and its child objects in the exported file.

[-includeBasicProperties]
  Includes basic object properties in the exported file.

[-includeAdvancedProperties]
  Includes advanced object properties in the exported file.

[-includeComments]
  Includes comments on the object in the exported file.

[-includeAssociations]
  Includes related catalog objects for the object in the exported file.

[-includeLinks]
  Includes links for the object in the exported file.

[-includeBusinessTerms]
  Includes related business terms for the object in the exported file.

[-includeCategories]
  Includes related categories for the object in the exported file.

[-includeImpactUpstream]
  Includes objects that the selected metadata object is impacted by in the exported file.

[-includeImpactDownstream]
  Includes objects that the selected metadata object impacts in the exported file.

generateDefaultLoadTemplate

Generates a default load template to load all top level classes for the specified model.
generateDefaultLoadTemplate Syntax

The command uses the following syntax:

```bash
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[<-ep|--encryptedPassword]
[<pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
<<-m|--modelName> Name>
<<out|--outputDirectory> Name
```

generateDefaultLoadTemplate Options

The command uses the following options:

`[-dn | --domainName]`

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

`[-hp | --gateway]`

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

`[-mm | --mmServiceName]`

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

`<<url>>`

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

`<<u|--user>>`

Metadata Manager user name.

`[-ep | --encryptedPassword]`

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
-ep -pw WP+qtfYwB2KLYID9jgC+6WHbMOg/94A08R1n0C1vd0=

[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-m | --modelName>>
Name of the model associated with the custom resource.

<<-out | --outputDirectory>>
Directory where the default load template file is saved.

getLinkReport
Exports the link summary report. The link summary report contains the resource, connection, assigned database, and assigned schema details.

getLinkReport Syntax
The command uses the following syntax:

[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<url> http(s)://<host>:<port>>
[<-u|--user> user>
[<ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-r|--resource> resource>
[<-f|--file> file>

getLinkReport Options
The command uses the following options:
[-dn | --domainName]  
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[-hp | --gateway]  
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName]  
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

```
<<-url>>
```

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

```
<<-u | --user>>
```

Metadata Manager user name.

[-ep | --encryptedPassword]  
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+gtFywB2KYLXID9jgC+6WHbM0g/94A08R1nOC1vd0=
```

[-pw | --password]  
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n | --namespace]  
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
getLoadTemplate

Exports a load template file.

getLoadTemplate Syntax

The command uses the following syntax:

```
[<-dn | --domainName> domainName]
[<-hp | --gateway> gateway_host1:port gateway_host2:port...]
[<-mm | --mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-na|--Name> Name>
<<-f|--File> File>
```

getLoadTemplate Options

The command uses the following options:

```
[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.
getResource

Writes properties for the specified resource to a resource configuration file. Use the getResource command when you move resources from a development to a production environment.

By default, the command writes all properties except the resource password to the resource configuration file. Optionally, you can include the resource password in the file.
getResource Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<-url> http(s)://<host>:<port>]
[<-u|--user> user]
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-r|--resource> resource]
[<-rcf|--resourceConfigurationFile> resourceConfigurationFile]
[<-includeRuleSets]
[<-includeFiles]
[<-includePassword]
```

getResource Options

The command uses the following options:

```
[<-dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.
This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

```
[<-url>]
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.
```

```
[<-u | --user>]
Metadata Manager user name.
```
[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+gtfYwB2KYLXID9jgC+6WHbMOg/94A08R1nOC1vd0=
```

[<pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>
Name of the Metadata Manager resource whose properties you want to write to a configuration file. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>
XML file name and path to which Metadata Manager writes the resource properties. Creates a file with the .rcf extension. If you do not include a path, mmcmd writes the XML file in the mmcmd directory.

[-includeRuleSets]
Exports the resource configuration file with all rule sets and rule set parameter definitions associated with the resource. Creates a file with the .rcz extension instead of the .rcf extension.

[-includeFiles]
Exports the resource configuration file with PowerCenter parameter files and all other files that you upload and associate with the resource except for rule sets.

[-includePassword]
Includes the encrypted resource password in the resource configuration file.

**get(ResourceFiles)**

Retrieves all the source files associated with a resource, including rule sets. Metadata Manager retrieves parameter files for PowerCenter resources and retrieves model files for data modeling resources.
**getResourceFiles Syntax**

The command uses the following syntax:

```bash
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...] as needed
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host1>:<port1>
<<-user> user
[<-ep|--encryptedPassword]
[<pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
[<destDir> destDir]
```

**getResourceFiles Options**

The command uses the following options:

[<-dn | --domainName>]
- Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.
- This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]
- Required if the domain uses Kerberos authentication and you do not specify the --domainName option.
- Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
- If there are multiple gateway nodes, separate the gateways with a space. For example:
  ```bash
  -hp host1:6001 host2:6002
  ```
- **Note**: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
- Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
- Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host1>:<port>.
- If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
- Metadata Manager user name.

[<-ep | --encryptedPassword]
- Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
getServiceLog

Exports the service log file from Metadata Manager for a specified date.

getServiceLog Syntax

The command uses the following syntax:

```bash
<ep> <pw> WP+qtfYwB2kLYID9jgC+6WHbMOg/94A08R1nOClvd0=

[<-pw|--password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n|--namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt|--keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r|--resource>>
Name of the Metadata Manager resource for which you want to retrieve the source files.

[<-destDir>]
Directory where the source files of the resource are stored. If not specified, the source files are saved in the current directory.

getServiceLog Options

The command uses the following options:
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:
-hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

Metadata Manager user name.

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94A08R1nOC1vd0=

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:
-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
[<kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[<dt | --date>]
Date of the service log details that you want to export. Format must be yyyy-mm-dd.

[<f | --file>]
Name of the file to which you want to export the service log details.

help
Returns help for an mmcmd command.

help Syntax
The command uses the following syntax:

    help [Operation]

help Options
The command uses the following options:

[Operation]
Name of the command for which you want to view the syntax. If you omit the operation, mmcmd returns the syntax for all mmcmd commands.

import
Imports the metadata for a custom resource from an XML file into the Metadata Manager repository.
Use import to import a custom resource into the Metadata Manager repository that you exported from another Metadata Manager repository. The import command imports the custom resource metadata, but it does not create the resource.

import Syntax
The command uses the following syntax:

    [<dn|--domainName> domainName]
    [<hp|--gateway> gateway_host1:port gateway_host2:port...]
    [mm|--mmServiceName> mmServiceName]
    [url|--url] http(s)://<host>:<port>>
    [user|--user> user>
    [encryptedPassword]
    [password]
    [namespace]
    [<kt|--keyTab> keyTab]
    [f|--file> file]
import Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

-hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s): //<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+gtfYw2KYLXID9jgC+6WHbMOg/94A08R1n0C1vd0=

[-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

XML file name and path for the custom resource that you want to import. If you do not include a path, mmcmd assumes the file is in the mmcmd directory.

importLinkRuleSets

Imports all linking rule sets from XML files in the specified path into the Metadata Manager repository. Use importlinkrulesets to import rule sets into the Metadata Manager repository that you exported from another Metadata Manager repository.

importLinkRuleSets Syntax

The command uses the following syntax:

```
[<-dn | --domainName>域名Name]
[<-hp | --gateway> gateway_host:port gateway_host2:port...]
[<-mm |--mmServiceName> mmServiceName]
[<url> http(s)://<host>:<port>>
[<-u|--user> user>
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-d|--dir> Import Directory>
[<-up|--update]
```

importLinkRuleSets Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:
-hp host1:6001 host2:6002

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

[<-url>]
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[<-u | --user>]
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94A08R1n0C1vd0=

[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[<-d | --dir>]
Directory from which you want to import the rule set files.

[-up | --update]
Updates an existing rule set during import.
**importModel**

Imports a model from a file into the Metadata Manager repository. Use `importModel` to import a model into the Metadata Manager repository that you exported from another Metadata Manager repository.

**Note:** You cannot import a Business Glossary model in Metadata Manager. To import business glossary assets and templates, use the Analyst tool.

**importModel Syntax**

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
<<url> http[s]://<host>:<port>>
<<u|--user> user>
<<p|--password> password>
<<n|--namespace> namespace]
<<kt|--keyTab> keyTab]
[<m|--modelName> modelName]
<<f|--file> file>
```

**importModel Options**

The command uses the following options:

- **[<dn|--domainName>]**
  
  Required if the domain uses Kerberos authentication and you do not specify the `--gateway` option. Name of the Informatica domain.

  This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the `--gateway` option instead.

- **[<hp|--gateway>]**
  
  Required if the domain uses Kerberos authentication and you do not specify the `--domainName` option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

  If there are multiple gateway nodes, separate the gateways with a space. For example:

  `-hp host1:6001 host2:6002`

  **Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

- **[<mm|--mmServiceName>]**
  
  Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

- **<<url>>**
  
  Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http{s}://<host>:<port>`. 
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

```bash
<-u | --user>
Metadata Manager user name.
```

```bash
[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbM0g/94A08R1n0C1vd0=
```

```bash
[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

```bash
<-n | --namespace>
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
```

```bash
[<-kt | --keyTab>
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.
```

```bash
[<-m | --modelName>
Name of the model in the XML file that you want to import. If the model name contains spaces, enclose the model name in quotes. For example, "My Model." If you do not include a model name, mmcmd imports all models in the XML file.
```

```bash
[<-f | --file>>
File name and path for the model export file that you want to import. The file can be a model export XML file or a zip file that contains the model XML file plus the associated rule set definitions. If you do not include a path, mmcmd assumes the file is located in the mmcmd directory.
```

**link**

 Creates the links between resources that share a connection assignment to run data lineage analysis across metadata sources.

Before you create links for a resource, you must configure connection assignments for the resource.
link Syntax

The command uses the following syntax:

```plaintext
[<-dn |--domainName> domainName]
[<-hp |--gateway> gateway_host1:port gateway_host2:port...]
[<-mm |--mmServiceName> mmServiceName]
<<-url>> http(s)://<host>:<port>>
<<-u |--user> user
[-ep |--encryptedPassword]
[<pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
[-wait]
[-sf|--skipFilter]
```

link Options

The command uses the following options:

```plaintext
[<-dn | --domainName>]
```

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

```plaintext
[<-hp | --gateway>]
```

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

```plaintext
[<-mm | --mmServiceName>]
```

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

```plaintext
<<-url>>
```

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

```plaintext
<<-u | --user>>
```

Metadata Manager user name.

```plaintext
[-ep | --encryptedPassword]
```

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
-ep -pw WP+qtFyWb2KYLXID9jgC+6WHboMG/94A0SR1n0C1vd0=

\[-pw \text{ | --password}\]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the -keyTab option. Password for the Metadata Manager user. For example:

- pw Administrator

Note: To specify an encrypted password, you must specify the -encryptedPassword option in addition to this option.

\[-n \text{ | --namespace}\]

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs.

The security domain name is case sensitive.

\[-kt \text{ | --keyTab}\]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r \text{ | --resource>>}

Name of the Metadata Manager resource for which you want to create links. If the resource name contains spaces, enclose the resource name in quotes.

\[-wait\]

Causes mmcmd to wait for the command to complete before returning the command prompt.

\[-sf \text{ | --skipFilter}\]

Skips filtering of connection assignments during linking.

listLoadTemplates

Lists all of the load template files for a model.

listLoadTemplates Syntax

The command uses the following syntax:

\[<\text{-dn | --domainName} \text{ domainName}>\]
\[<\text{-hp | --gateway} \text{ gateway_host1:port gateway_host2:port...} >\]
\[<\text{-mm | --mmServiceName} \text{ mmServiceName}>\]
\[<\text{-url | http(s)://host>:<port>>}>\]
\[<\text{-u | --user} \text{ user}>\]
\[<\text{-ep | --encryptedPassword} >\]
\[<\text{-pw | --password} \text{ password}>\]
\[<\text{-n | --namespace} \text{ namespace}>\]
\[<\text{-kt | --keyTab} \text{ keyTab}>\]
\[<\text{-m | --modelName} \text{ Name}>\]

listLoadTemplates Options

The command uses the following options:
[-dn | --domainName]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[-hp | --gateway]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

-hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

[-url]

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[-u | --user]

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtFyWb2kYlXID9jgC+6WbMOg/94A08R1n0C1vd0=

[-pw | --password]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n | --namespace]

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
listModels

Lists all models in Metadata Manager.

listModels Syntax

The command uses the following syntax:

```bash
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
[<url> http(s)://<host>:<port>]
[<u|--user> user]
[<ep|--encryptedPassword>]
[<pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
[<c|--custom>]
```

listModels Options

The command uses the following options:

```bash
[<dn|--domainName>]
```

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

```bash
[<hp|--gateway>]
```

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

```bash
[<mm|--mmServiceName>]
```

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

**<u|--user>>**

Metadata Manager user name.

**[-ep|--encryptedPassword]**

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted.

```bash
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbM0g/94A08R1nOC1vd0=
```

**[-pw|--password]**

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option.

```bash
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

**[-n|--namespace]**

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

**[-kt|--keyTab]**

Required if the domain uses Kerberos authentication and you do not specify a password.

```bash
-keyTab
```

**[-c|--custom]**

Lists all custom models. If you do not specify this option, Metadata Manager lists all models.

### listResources

Lists all resources in the Metadata Manager repository.

### listResources Syntax

The command uses the following syntax:

```bash
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
[<url> http(s)://<host>:<port>]
[<u|--user> user]
[<ep|--encryptedPassword]
[<pw|--password> password]
```
listResources Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

- hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

- ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94A08R1n0C1vd0=

[-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

- pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.
load

Starts a resource load.

Metadata Manager adds the resource load to the load queue. You can view the status of the resource load using the mmcmd status command or in the Metadata Manager Load tab. When you run the load command, mmcmd returns the current status of the load and the time that the load started.

load Syntax

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
<<url> http(s)://<host>[:<port>>
<<u|--user> user>
[-ep|--encryptedPassword]
[-pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
<<r|--resource> resource>
[-wait]
```

load Options

The command uses the following options:

```
[<dn|--domainName>]
```

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

```
[<hp|--gateway>]
```

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm | --mmServiceName]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

 <<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

 <<-u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMoBv/94A08R1nOC1vd0=

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

 <<-r | --resource>>
Name of the Metadata Manager resource that you want to load. If the resource name contains spaces, enclose the resource name in quotes.

[-wait]
Causes mmcmd to wait for the command to complete before returning the command prompt.
migrateBGLinks

Restores the related catalog objects for a business glossary after you upgrade from version 9.5.x.

When you upgrade business glossaries, you perform the following tasks:

1. Export a business glossary from the previous version of Metadata Manager.
2. Import the business glossary into the Analyst tool.
3. Create and load the Business Glossary resource in the current version of Metadata Manager.

This command runs automatically when you load a Business Glossary resource. When this command runs, the load details show the following messages:

<date, time>: Task started: Linking and BG links migration
<date, time>: BG links migration started_
<date, time>: BG links migration succeeded
<date, time>: Task handled successfully: Linking and BG links migration

**Note:** Because this command runs automatically, do not run this command unless the migration fails and you fix the error or unless you are directed to run this command by Informatica Global Customer Support.

For more information about upgrading business glossaries, see the *Upgrading from Version 9.5.0* or *Upgrading from Version 9.5.1* guide.

migrateBGLinks Syntax

The command uses the following syntax:

```bash
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-nm|--mmServiceName> mmServiceName]
[<-url> http(s)://<host>:<port>]
[<-u|--user> user]
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-g|--Glossary> Glossary]
```

migrateBGLinks Options

The command uses the following options:

**[<-dn|--domainName>]**

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

**[<-hp|--gateway>]**

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```bash
-hp host1:6001 host2:6002
```
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>[:<port>].

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2kYLXID9jgC+6WHbM0g/94A08R1n0C1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-g | --Glossary>>

Name of the business glossary for which you want to restore related catalog objects after upgrade.

**purgeMetadata**

Deletes metadata for a resource from the Metadata Manager repository. You cannot recover the purged metadata. Back up the Metadata Manager repository database before you purge metadata.

After you purge a resource, you can optimize the index to free disk space used by the indexing files.
purgeMetadata Syntax

The command uses the following syntax:

```bash
[<-dn | --domainName> domainName]
[<-hp | --gateway> gateway_host1:port gateway_host2:port...]
[<-mm | --mmServiceName> mmServiceName]
<<-url>> http(s)://<host>:<port>>
<<-u | --user> user>
[-ep | --encryptedPassword]
[<-pw | --password> password]
[<-n | --namespace> namespace]
[<kt|--keyTab> keyTab]
<<-r|--resource> resource>
[<wait]```

purgeMetadata Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```bash
-hp host1:6001 host2:6002```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>]

Metadata Manager user name.

[<-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

Name of the Metadata Manager resource for which you want to purge metadata. If the resource name contains spaces, enclose the resource name in quotes.

Causes mmcmd to wait for the command to complete before returning the command prompt.

**restoreConfiguration**

Restores the resource configurations, source files associated with resources, linking rules associated with resources, and custom models from a back-up file.

**restoreConfiguration Syntax**

The command uses the following syntax:

```bash
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
[<url> http(s)://<host>[:<port>]]
[<u|--user> user]
[<ep|--encryptedPassword>]
[<pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
[<file> file]
[<pdir> paramFileDir]
```

**restoreConfiguration Options**

The command uses the following options:
[<dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.
This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
If there are multiple gateway nodes, separate the gateways with a space. For example:
```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

[<url>]
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[<u | --user>]
Metadata Manager user name.

[<ep | --encryptedPassword>]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94A08R1oOC1vd0=
```

[<pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:
```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-file>>
File name and path of the back-up file.

[<-pdir>]
Directory where the source files of the Metadata Manager resources are stored. If not specified, the source files that are saved in the backup are used.

resume
Resumes a failed resource load.
If a resource load fails when PowerCenter runs the workflows that load the metadata into the warehouse, you can resume the resource load. When you run the resume command, mmcmd returns the current status of the load and the time that the load resumed.

resume Syntax
The command uses the following syntax:

```
[<-dn | --domainName> domainName]
[<-hp | --gateway> gateway_host1:port gateway_host2:port...]
[<-mm | --mmServiceName> mmServiceName]
<<-url> http://<host>:<port>>
<<-u | --user> user>
[-e | --encryptedPassword]
[<-p | --password> password]
[<-n | --namespace> namespace]
[<-kt | --keyTab> keyTab]
<<-r | --resource> resource>
```

resume Options
The command uses the following options:

[<-dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

[<url>]
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[<u | --user>]
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WbMOg/94A08R1nOC1vd0=
```

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[<r | --resource>]
Name of the Metadata Manager resource for which you want to resume the load. If the resource name contains spaces, enclose the resource name in quotes.

search

Searches for objects in the Metadata Manager repository using a keyword search.

Perform a keyword search to search all properties of objects that match the keyword. mmcmd displays the results of the search in the command prompt. The search results list the locations of all objects that match the search criteria.
search Syntax

The command uses the following syntax:

```plaintext
[<-dn | --domainName> domainName]  
[<-hp | --gateway> gateway_host1:port gateway_host2:port...]  
[<-mm | --mmServiceName> mmServiceName]  
<<-url>> http(s)://<host>:<port>>  
<<-u | --user> user>  
[-ep | --encryptedPassword]  
[<--pw|--password> password]  
[<--n|--namespace> namespace]  
[<--kt|--keyTab> keyTab]  
<<--arg|--argument> argument>
```

search Options

The command uses the following options:

```plaintext
[<-dn | --domainName>]  
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]  
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]  
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>  
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[<-u | --user>]  
Metadata Manager user name.

[-ep | --encryptedPassword]  
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KLYID9jgC+6WHeMoC/94A08R1nOCrbd0=
```
[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-arg | --argument>><-arg | --argument>>

Keyword to search for. You can use search operators and wildcard characters in a keyword search.

---

**status**

Displays the status of a running or completed resource load. When you run the status command, mmcmd returns the current status of the load and the time that you ran the command.

**status Syntax**

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>[:<port>]
<<-u|--user> user
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
```

**status Options**

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.
[<-hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
If there are multiple gateway nodes, separate the gateways with a space. For example:
-hp host1:6001 host2:6002

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http://<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbM0g/94A08R1n0C1vd0=

[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:
-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>
Name of the Metadata Manager resource for which you want to view the status. If the resource name contains spaces, enclose the resource name in quotes.
testSourceConnection

Tests connection to the source system of a resource.

testSourceConnection Syntax

The command uses the following syntax:

```
[<-dn | --domainName> domainName]
[<-hp | --gateway> gateway_host1:port gateway_host2:port...]
[<-mm | --mmServiceName> mmServiceName]
<<url> http(s)://host1:<port>>
<<u | --user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
```

testSourceConnection Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://host1:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<u | --user>>

Metadata Manager user name.
The command uses the following syntax:

updateLinkRuleSet

domainName

gateway_host1:port gateway_host2:port...

mmServiceName

http(s)://<host>:<port>

user

encryptedPassword

password

namespace

keyTab

resource

rule set xml

rule set definition xml

rule set parameter xml

updateLinkRuleSet Options

The command uses the following options:

-ep | --encryptedPassword

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtfYWb2KYLXID9jgC+6WHzMOg/94A08R1nOC1vd0=

<--pw | --password>

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

<--n | --namespace>

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

<--kt | --keyTab>

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<--r | --resource>

Name of the Metadata Manager resource for which you want to test source connections.

updateLinkRuleSet

Updates a linking rule set for a pair of resources or a rule set definition for a pair of models in the Metadata Manager repository. Updates the rule set or rule set definition based on a linking rules file. If the rule set or rule set definition does not exist, this command creates it.

updateLinkRuleSet Syntax

The command uses the following syntax:

[<--dn|--domainName> domainName]
[<--hp|--gateway> gateway_host1:port gateway_host2:port...]
[<--mm|--mmServiceName> mmServiceName]
[<--url> http(s)://<host>:<port>]
[<--user> user]
[<--ep|--encryptedPassword] 
[<--pw|--password> password]
[<--n|--namespace> namespace]
[<--kt|--keyTab> keyTab]
[<--file> rule set xml|rule set definition xml|rule set parameter xml]
[<-dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(https)://<host>[:<port>].

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
Metadata Manager user name.

[<-ep | --encryptedPassword]  
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtFyWb2kylXid9jgC+6WHbMOg/94A08R1n0C1vd0=
```

[<-pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note:** To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
updateLoadTemplate

Updates a load template file.

updateLoadTemplate Syntax

The command uses the following syntax:

```
[<-dn | --domainName> domainName]
[<-hp | --gateway> gateway_host1:port gateway_host2:port...]
[<-mm | --mmServiceName> mmServiceName]
[<-url> http(s)://<host>:<port>]
[<-user> user]
[<--ep | --encryptedPassword] [--password> password]
[<-n | --namespace> namespace]
[<-kt | --keyTab> keyTab]
[<-f | --file> File]
```

updateLoadTemplate Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option.

Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXjgC+6WHbM0g/94A08R1n0C1vd0=
```

[<pw | --password>]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[<kt | --keyTab>]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-f | --File>>
Name of the load template file that you want to update.

updateResource

Updates a resource based on the properties in the specified resource configuration file.

Use the updateResource command when you move resources from a development to a production environment. After you create a resource based on a resource configuration file, you might need to change the properties in the resource configuration file. Use the updateResource command to update the resource with the modified properties.
updateResource Syntax

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
<<url>> http(s)://<host>:<port>>
<<u|--user> user>
[<ep|--encryptedPassword]
[<pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
[<-r|--resource> resource]
[<rcf|--resourceConfigurationFile> resourceConfigurationFile>
[<pdir|--paramFileDir>]
[<rpw|--resourcePassword> resourcePassword]
[<sjp|--secureJDBCParameters> secureJDBCParameters]
```

updateResource Options

The command uses the following options:

```
[<dn|--domainName>]
```

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

```
[<hp|--gateway>]
```

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

```
[<mm|--mmServiceName>]
```

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

```
<<url>>
```

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

```
<<u|--user>
```

Metadata Manager user name.
[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+gtFywB2KYLXID9jgC+6WHbMOg/94A08R1nOC1vd0=
```

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n | --namespace]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[-kt | --keyTab]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>
Name of the Metadata Manager resource that you want to update. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>
File name and path for the resource configuration file that contains the modified resource properties. You can import a resource configuration file (.rcf file). Alternatively, you can import a resource configuration file that also contains all the rule sets and rule set parameter definitions associated with the resource (.rcz file). If you do not include a path, mmcmd looks for the file in the mmcmd directory.

The source files of the resource must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If you do not specify a path, mmcmd looks for the source files in the mmcmd directory.

[-pdir]
Directory where the source files of the Metadata Manager resources are stored.

[-rpw | --resourcePassword]
Required if the resource uses a password and the resource configuration file does not contain the resource password. Resource password in plain text.

[-sjp | --secureJDBCParameters]
Secure JDBC parameters that you want to append to the JDBC connection URL. Use this option with database management resources to specify secure connection parameters such as passwords. Metadata Manager does not display secure parameters or parameter values in the resource configuration properties. Enter the parameters as name=value pairs separated by the delimiter character that the database driver requires.

If secure communication is enabled for the metadata source database, enter the secure JDBC parameters in this option.
version

Displays the current version of Metadata Manager.
Chapter 2

mmLineageMigrator

This chapter includes the following topics:

- mmLineageMigrator Overview, 90
- Running mmLineageMigrator, 90
- mmLineageMigrator Syntax, 91
- mmLineageMigrator Options, 91

mmLineageMigrator Overview

mmLineageMigrator is a command line program that migrates data lineage linking information after you upgrade from Metadata Manager 9.6.x to the current version. mmLineageMigrator migrates data lineage linking information from the Metadata Manager repository to the data lineage graph database.

mmLineageMigrator reads data lineage linking information from the Metadata Manager repository, creates a file-based graph database to store the information, and then copies the information to the graph database. The program creates the graph database files in the Metadata Manager lineage graph location that you specify. mmLineageMigrator does not change any table or view in the Metadata Manager repository.

Note: Because this program runs automatically, do not run this program unless the migration fails and you fix the error or unless you are directed to run this program by Informatica Global Customer Support.

Running mmLineageMigrator

You run mmLineageMigrator from the command line. You can issue commands directly or from a script, batch file, or other program. On Windows, mmLineageMigrator is a batch file with a .bat extension. On UNIX, mmLineageMigrator is a script file with a .sh extension.

mmLineageMigrator is located in the following directory:

`<Informatica services installation directory>\services\MetadataManagerService\utilities \mmLineageMigrator`

mmLineageMigrator is not installed with the Informatica client or with the Informatica command line utilities.

1. Disable the Metadata Manager Service.
2. At a command prompt, navigate to the directory where mmLineageMigrator is located.
3. Enter `mmLineageMigrator` on Windows or `mmLineageMigrator.sh` on UNIX followed by the required options and arguments.
4. When the migration finishes, restart the Metadata Manager Service.

**mmLineageMigrator Syntax**

`mmLineageMigrator` options and arguments specify connection information for the Metadata Manager repository database and the Metadata Manager lineage graph location.

`mmLineageMigrator` uses the following syntax:

```
mmLineageMigrator.bat
<<dt|--DatabaseType> databaseType>
<<du|--DatabaseUserName> databaseUserName>
<<gd|--GraphDir> graphDirectory>
<<dp|--DatabasePassword> databasePassword>
<<url|--DbUrl> databaseURL>
[-h|--help]
```

**mmLineageMigrator Options**

`mmLineageMigrator` uses the following options:

`<<<<-dt>>>>`

Database type for the Metadata Manager repository database.
Specify one of the following types:
- DB2
- ORACLE
- SQLSERVER

`<<<<-du>>>>`

Database user name for the Metadata Manager repository database.

`<<<<-gd>>>>`

Directory where the program creates the graph database files. Must match the Metadata Manager lineage graph location that you configure for the Metadata Manager Service in the Administrator tool. If the directory contains spaces, enclose it in double quotes.

`<<<<-dp>>>>`

Password for the Metadata Manager repository database user.

`<<<<-url>>>>`

JDBC URL for the Metadata Manager repository database.
The syntax depends on the repository database type:
- For IBM DB2, use the following syntax:
  ```
  "jdbc:informatica:db2://[host name]:[port];DatabaseName=[database name]"
  ```
If the Metadata Manager repository database uses a secure connection to communicate with external
components, you must append additional parameters to the JDBC URL.

Configure the parameters as follows:

- **TrustStore**: Password used to access the truststore file.
- **TrustStorePassword**: Password used to access the truststore file.

Note: If secure communication is enabled for the Metadata Manager repository database, you must
append additional JDBC parameters to the JDBC URL.

[-h]

Displays help for the mmLineageMigrator command line program. The help option lists the
mmLineageMigrator options and arguments.

### JDBC Parameters for Secure Databases

If the Metadata Manager repository database uses a secure connection to communicate with external
components, you must append additional parameters to the JDBC URL.

Append the following parameters to the URL:

```
;EncryptionMethod=SSL;TrustStore=<truststore location>;TrustStorePassword=<password>;HostNameInCertificate=<host name>;ValidateServerCertificate=<true|false>;KeyStore=<keystore location>;KeyStorePassword=<password>
```

Configure the parameters as follows:

- **EncryptionMethod**: Encryption method for data transfer between Metadata Manager and the database server. Must be set to SSL.
- **TrustStore**: Path and file name of the truststore file that contains the security certificate of the database server.
- **TrustStorePassword**: Password used to access the truststore file.
HostNameInCertificate

Host name of the machine that hosts the secure database. If you specify a host name, the Metadata Manager Service validates the host name included in the connection string against the host name in the security certificate.

ValidateServerCertificate

Indicates whether the Metadata Manager Service validates the certificate that the database server presents. If you set this parameter to true, the Metadata Manager Service validates the certificate. If you specify the HostNameInCertificate parameter, the Metadata Manager Service also validates the host name in the certificate.

If you set this parameter to false, the Metadata Manager Service does not validate the certificate that the database server presents. The Metadata Manager Service ignores any truststore information that you specify.

KeyStore

Path and file name of the keystore file that contains the security certificates that the Metadata Manager Service presents to the database server.

KeyStorePassword

Password used to access the keystore file.
CHAPTER 3

mmRepoCmd

This chapter includes the following topics:

- mmRepoCmd Overview, 94
- Certificate Validation for mmRepoCmd, 95
- MMCmdConfig.properties File, 95
- mmRepoCmd Rules and Guidelines, 96
- mmRepoCmd Commands, 96
- backupRepository, 97
- createRepository, 99
- deleteRepository, 100
- restorePCRepository, 102
- restoreRepository, 104

mmRepoCmd Overview

mmRepoCmd is a command line program that creates, deletes, backs up, and restores Metadata Manager repository contents. It also restores a PowerCenter repository back-up file that contains Metadata Manager objects to the PowerCenter repository database.

mmRepoCmd is installed when you run the Informatica services installer or the Informatica client installer. You can also install mmRepoCmd on any machine when you install Informatica utilities. mmRepoCmd is installed as a batch file on Windows and as a shell script on UNIX.

mmRepoCmd is located in the following directories:

- `<Informatica services installation directory>/services/MetadataManagerService/utilities/mmrepocmd`
- `<Informatica client installation directory>/clients/PowerCenterClient/CommandLineUtilities-MM/mmrepocmd`
- `<Informatica utilities installation directory>/MetadataManager/utilities/mmrepocmd`

mmRepoCmd writes log events to the mmRepoCmd.log file. If you run mmRepoCmd from the command line, it creates the log file in the directory where the program is installed.

If the Metadata Manager Service calls this program, the program creates the log file in the following directory:
Certificate Validation for mmRepoCmd

If you configure a secure connection between the Metadata Manager web application and the Metadata Manager Service, you must configure mmRepoCmd to use the truststore file. mmRepoCmd uses the truststore file to validate the security certificates. mmRepoCmd does not accept a security certificate that has errors.

To configure mmRepoCmd to use the truststore file, edit the MMCmdConfig.properties file. Set the TrustStore.Path property to the path and file name of the truststore file.

If you do not configure a secure connection for the Metadata Manager web application, do not specify a truststore file. Leave the TrustStore.Path property in the MMCmdConfig.properties file empty.

**MMCmdConfig.properties File**

Use the MMCmdConfig.properties file to configure mmRepoCmd properties such as the truststore file, server polling interval, and server connection timeout period.

MMCmdConfig.properties is located in the following directories:

- `<Informatica services installation directory>/logs/<node name>/services/MetadataManagerService/Utilities\mmreopcmd\config`
- `<Informatica client installation directory>/clients\PowerCenterClient\CommandLineUtilities\MM\mmreopcmd\config`
- `<Informatica utilities installation directory>/MetadataManager/Utilities\mmreopcmd\config`

**Note:** There are separate copies of the MMCmdConfig.properties file for mmcmd and for mmRepoCmd.

You can configure the following properties:

**TrustStore.Path**

Required if you configure a secure connection for the Metadata Manager web application. Path and file name of the truststore file that contains the public key.

If you do not configure a secure connection for the Metadata Manager web application, leave this property empty.

**Server.PollInterval**

Amount of time in milliseconds that the command line program waits before querying the Metadata Manager application. The program queries for the status of the last command when you run a command in wait mode. Default is 6000.

**Server.ConnectionTimeOut**

Number of milliseconds after which the remote connection to the Metadata Manager Service times out. Default is 86,400,000 (24 hours).
mmRepoCmd Rules and Guidelines

Use the following rules and guidelines with mmRepoCmd:

- To run mmRepoCmd commands, the Metadata Manager Service must be enabled and available.
- When you back up repository contents, mmRepoCmd uses the default encryption key to encrypt sensitive data in the binary back-up file. For maximum security, limit users that can access the back-up file directory.
- When you restore repository contents, mmRepoCmd uses the encryption key for the Informatica domain to encrypt sensitive data in the Metadata Manager repository.
- mmRepoCmd does not back up index files for a loaded resource. You must manually create the index for resources after you restore a Metadata Manager repository.
- To restore the Metadata Manager repository for a Metadata Manager Service in a different Informatica domain, you must first migrate the Metadata Manager users and groups. Before you restore the Metadata Manager repository, export the users and groups from the original domain and import them into the new domain.

To export and import users and groups, use the infacmd command line program.
- After you restore repository contents, recycle the Metadata Manager Service. Recycle the Metadata Manager Service so that it drops and recreates the caches that store model and resource information.
- Back up and restore the Metadata Manager repository with the same Metadata Manager version. You cannot restore a back-up file from a different version.

mmRepoCmd Commands

The following table describes the mmRepoCmd commands:

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backupRepository</td>
<td>Backs up the Metadata Manager repository to a back-up file.</td>
</tr>
<tr>
<td>createRepository</td>
<td>Creates the Metadata Manager warehouse tables and imports models for metadata sources into the Metadata Manager repository.</td>
</tr>
<tr>
<td>deleteRepository</td>
<td>Deletes Metadata Manager repository contents, including all metadata and repository database tables.</td>
</tr>
<tr>
<td>restorePCRepository</td>
<td>Restores a PowerCenter repository back-up file that contains Metadata Manager objects to the PowerCenter repository database.</td>
</tr>
<tr>
<td>restoreRepository</td>
<td>Restores Metadata Manager repository contents from a back-up file.</td>
</tr>
</tbody>
</table>
backupRepository

Backs up the Metadata Manager repository to a back-up file. Backs up all tables in the Metadata Manager repository except staging tables and temporary tables.

Back up repository contents so that you can recover them after a hardware or software problem or to migrate a repository across domains or Metadata Manager Services. You can restore repository contents to the same database, to a different database, or to a different database type. To migrate a repository, back up repository contents, change the repository database, and restore the contents to the new database.

The backupRepository command creates a binary back-up file. It creates the back-up file in the backup subdirectory of the Metadata Manager file location that you set for the Metadata Manager Service.

By default, the backupRepository command creates the back-up file in the following directory:

```
<Informatica services installation directory>\services\MetadataManagerService\mm_files
\<Metadata Manager Service name>\backup
```

backupRepository Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<url> http(s)://<host>[:<port>]]
[<-u|--user> user]
[<-ep|--encryptedPassword]  
[<-p|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-f|--file> file]
[<-nt|--numThreads> numThreads]
```

backupRepository Options

The command uses the following options:

**[<-dn | --domainName>]**

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

**[<-hp | --gateway>]**

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
--hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.
[-mm | --mnServiceName]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

[-url]
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>[:<port>].

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[-u | --user]
Metadata Manager user name.

[ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtJvWz2KL9jgC+6WbMOg/94A0SR1nOC1vd0=
```

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

**Note**: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n | --namespace]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[-kt | --keyTab]
Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[-f | --file]
Name of the file to which you want to back up the Metadata Manager repository database.

mmRepoCmd stores the back-up file in the backup subdirectory of the Metadata Manager file location that is set for the Metadata Manager Service. The back-up file name must be unique in the directory.

[-nt | --numThreads]
Number of processing threads that the Metadata Manager Service uses when it reads data from the Metadata Manager repository database. Must be a positive integer. Default is 5.
createRepository

Creates the Metadata Manager warehouse tables and imports models for metadata sources into the Metadata Manager repository.

Create repository contents after you create the Metadata Manager Service or if you deleted the repository contents. You cannot create contents for a repository that already includes contents.

createRepository Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]  
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]  
[<-mm|--mmServiceName> mmServiceName]  
<<-url> http(s)://<host>[:<port>]  
<<-u|--user> user>  
[<-ep|--encryptedPassword>    
[<-pw|--password> password]  
[<-n|--namespace> namespace]  
[<-kt|--keyTab> keyTab]  
```

createRepository Options

The command uses the following options:

```
[<-dn | --domainName>]  
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]  
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

**Note:** If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]  
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>[:<port>].

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.
<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXC9jgC+6WHbMOg/94A08R1nOC1vd0=
```

[-pw | --password]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n | --namespace]

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[-kt | --keyTab]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

---

**deleteRepository**

Deletes Metadata Manager repository contents, including all metadata and repository database tables.

Delete the repository contents 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 mmRepoCmd to back up the database before you delete contents.

**deleteRepository Syntax**

The command uses the following syntax:

```
[<dn|--domainName> domainName]
[<hp|--gateway> gateway_host1:port gateway_host2:port...]
[<mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[-pw|--password> password]
[<n|--namespace> namespace]
[<kt|--keyTab> keyTab]
[-f]
```

**deleteRepository Options**

The command uses the following options:
[<dn | --domainName>]
Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.
This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<hp | --gateway>]
Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.
If there are multiple gateway nodes, separate the gateways with a space. For example:
-hp host1:6001 host2:6002
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<mm | --mmServiceName>]
Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<url>>
Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s): //<host>:<port>.
If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<u | --user>>
Metadata Manager user name.

[-ep | --encryptedPassword]
Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:
-ep -pw WP+gtfYwB2KYLXID9jgC+6WHbMOg/94A08R1n0C1vd0=

[-pw | --password]
Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:
-pw Administrator
Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<n | --namespace>]
Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.
restorePCRepository

Restores a PowerCenter repository back-up file that contains Metadata Manager objects to the PowerCenter repository database. This command restores different contents to the PowerCenter repository based on the operating mode of the PowerCenter Repository Service.

The PowerCenter repository back-up file includes the metadata objects that Metadata Manager uses to load metadata into the Metadata Manager warehouse. These metadata objects include sources, targets, sessions, and workflows. In the PowerCenter repository, the metadata objects used by Metadata Manager are stored in the Metadata Load folder.

The restorePCRepository command restores different contents based on the following PowerCenter Repository Service operating modes:

**Exclusive mode**

If the PowerCenter Repository Service is running in exclusive mode, this command replaces all contents in the PowerCenter repository database. If the PowerCenter repository database contains contents, this command overwrites all contents.

Run this command when the PowerCenter Repository Service is running in exclusive mode if either of the following conditions are true:

- The PowerCenter repository has no content associated with it.
- The repository contains content that has not been upgraded.

**Normal mode**

If the PowerCenter Repository Service is running in normal mode, this command creates the Metadata Load folder and restores the folder contents. If the Metadata Load folder contains contents, this command overwrites all contents of the Metadata Load folder. It does not overwrite other PowerCenter repository database contents.

Run this command when the PowerCenter Repository Service is running in normal mode if the following conditions are true:

- The PowerCenter repository database contains contents.
- You only want to restore the contents of the Metadata Load folder.

**Note:** You must run this command from an mmRepoCmd instance that is installed with the Informatica services. You cannot run this command from an mmRepoCmd instance that is installed with Informatica utilities or with the Informatica client.
restorePCRepository Syntax

The command uses the following syntax:

```bash
<<-dn | --domainName> domainName>
[-sdn | --securityDomain> security_domain]
[-hp | --gateway> gateway_host1:port gateway_host2:port...]
<<-du | --domainUser> domainUser>
[-dp | --domainPassword> domainPassword]
[-mm | --mmServiceName> mmServiceName>
[-kt | --keyTab> keyTab]
<<pcRepositoryName> pcRepositoryName>
<<pcRepositoryUser> pcRepositoryUser>
[-pcRepositoryNamespace> pcRepositoryNamespace]
<<pcRepositoryPassword> pcRepositoryPassword>
```

restorePCRepository Options

The command uses the following options:

```bash
<<-dn | --domainName>>
    Name of the Informatica domain.

[-sdn | --securityDomain>]
    Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain
    uses native authentication. Name of the security domain to which the Informatica domain user belongs.
    The security domain name is case sensitive.

[-hp | --gateway>]
    Required if the domains.infa file is missing or contains connectivity information that is out of date. Host
    names and port numbers of the gateway nodes in the domain. If there are multiple gateway nodes,
    separate the gateways with a space. For example:
    -hp host1:6001 host2:6002

<<-du | --domainUser>>
    User name used to connect to the Informatica domain.

[-dp | --domainPassword>]
    Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos
    authentication and you do not specify the --keyTab option for the domain user. Password for the
    Informatica domain user.

<<-mm | --mmServiceName>>
    Name of the Metadata Manager Service for which you want to restore the PowerCenter repository.

[-kt | --keyTab>]
    Required if the domain uses Kerberos authentication and you do not specify a domain user password.
    Path and file name of the keytab file for the domain user.

<<pcRepositoryName>>
    Name of the PowerCenter repository that you want to restore.

<<pcRepositoryUser>>
    User account for the PowerCenter repository. Use the repository user account you configured for the
    Repository Service.
restoreRepository

Restores Metadata Manager repository contents from a back-up file. You can restore repository contents to
the same database, to a different database, or to a different database type. You can restore repository
contents to an empty repository.

When you restore a Metadata Manager repository, mmRepoCmd creates the repository tables in the
Metadata Manager repository and then restores the contents. If the repository contains a table with the same
name as a table that mmRepoCmd is trying to restore, mmRepoCmd drops the existing table, creates a new
table, and restores the contents to the new table.

restoreRepository Syntax

The command uses the following syntax:

[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
[<-url> http(s)://<host>[:<port>]]
[<-u|--user> user]
[<-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-f|--file> file]
[<-nt|--numThreads> numThreads]
[<-ci|--commitInt> commitInt]

restoreRepository Options

The command uses the following options:

[<-dn|--domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name
of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is
missing or contains connectivity information that is out of date, you must use the --gateway option
instead.

[<-hp|--gateways>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option.
Also required if the domain uses Kerberos authentication and the domains.infa file is missing or
contains connectivity information that is out of date. Host names and port numbers of the gateway
nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:
Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-hp host1:6001 host2:6002]

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[-mm|--mmServiceName]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

[-url]

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: http(s)://<host>:<port>.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

[-u|--user]

Metadata Manager user name.

[-ep|--encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

-ep -pw WP+qtFWygB2KYLID9jyG+6WbMOg/94A08R1nOC1vd0=

[-pw|--password]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

-pw Administrator

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[-n|--namespace]

Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the Metadata Manager user belongs. The security domain name is case sensitive.

[-kt|--keyTab]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[-f|--file]

Name of the file from which you want to restore Metadata Manager repository database contents.

The back-up file must exist in the backup subdirectory of the Metadata Manager file location that is set for the Metadata Manager Service.

[-nt|--numThreads]

Number of processing threads that the Metadata Manager Service uses when it writes data to the Metadata Manager repository database. Must be a positive integer. Default is 5.
Number of rows after which the Metadata Manager Service commits the data into the Metadata Manager repository. The restoreRepository command uses a batch commit each time it writes this number of rows. Using a batch commit reduces the size of the undo tablespace required if the command fails and mmRepoCmd rolls back the restore operation.

If set to 0, the command commits all rows at the end of the restore operation. Default is 10,000.
mmXConPluginUtil

This chapter includes the following topics:

- mmXConPluginUtil Overview, 107
- Running Commands, 108
- mmXConPluginUtil Commands, 108
- generateImageMapping, 108
- generatePlugin, 109

mmXConPluginUtil Overview

mmXConPluginUtil is a command line program that generates the image mapping information or the plug-in for a universal XConnect.

mmXConPluginUtil is installed when you run the Informatica services installer. mmXConPluginUtil is installed as a batch file on Windows and as a shell script on UNIX.

mmXConPluginUtil is located in the following directory:

```<Informatica services installation directory>\services\MetadataManagerService\utilities\mmxconpluginutil```

mmXConPluginUtil writes log events to the following log file:

```<Informatica services installation directory>\services\MetadataManagerService\utilities\mmxconpluginutil\mmxconnectpluginutil.log```

You run mmXConPluginUtil from the command line. The program creates the image mapping file or the plug-in in the following directory, where the owner and name are defined in the plug-in definition file:

```<Informatica services installation directory>\services\MetadataManagerService\utilities\mmxconpluginutil\<owner>.<name>```

For more information about creating universal XConnects, see the Metadata Manager Administrator Guide.
Running Commands

When you run mmXConPluginUtil, you enter options for each command, followed by the required options and arguments. Command names are not case sensitive. Command options are preceded by a hyphen and are not case sensitive. Arguments follow the option.

For example, the following command generates the plug-in for a universal XConnect for QlikView:

```
mmXConPluginUtil generatePlugin -x C:\\MMPlugInDefs\\HypoStores_QlikViewDef.xml
```

If you omit or incorrectly enter one of the required options, the command fails, and mmXConPluginUtil returns an error message.

1. At the command prompt, switch to the directory where mmXConPluginUtil is located.
2. Enter mmXConPluginUtil on Windows or mmXConPluginUtil.sh on UNIX followed by the command name and its required options and arguments.
   
   For example:
   
   ```
   mmXConPluginUtil(.sh) command_name -option argument
   ```

mmXConPluginUtil Commands

The following table describes the mmXConPluginUtil commands:

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generateImageMapping</td>
<td>Generates the image mapping information for a universal XConnect.</td>
</tr>
<tr>
<td>generatePlugin</td>
<td>Generates the plug-in for a universal XConnect.</td>
</tr>
</tbody>
</table>

generateImageMapping

Generates the image mapping information for a universal XConnect. You need the image mapping information if you want to use custom icons for the groups and classes in the model. The image mapping information is a CSV file that lists each group and class in the model with the corresponding icon file.

The command uses the name and owner elements in the XML definition file to generate the image mapping file name in the following format:

```
m=<owner>.<name>-xconnect.txt
```

generateImageMapping Syntax

The command uses the following syntax:

```
<<<x> xconnect definition file>
```
**generateImageMapping Options**

The command uses the following options:

```bash
<<-x>>
```

File path and file name of the plug-in definition XML file. If the file path or file name contains spaces, enclose the entire file path, including the file name, in double quotes.

**generatePlugin**

Generates the plug-in for a universal XConnect. The `generatePlugin` command generates the plug-in as an XConnect archive (XAR) file.

The command uses the name and owner elements in the XML definition file to generate the plug-in name in the following format:

```
mm-<owner>.<name>-xconnect.xar
```

After you create the plug-in, you can create the model. To create the model, copy the plug-in to the following directory, and then restart the Metadata Manager Service:

```
<Informatica services installation directory>\services\MetadataManagerService\mm-plugins\xconnect\<Metadata Manager Service name>
```

**generatePlugin Syntax**

The command uses the following syntax:

```bash
<<-x> xconnect definition file>
```

**generatePlugin Options**

The command uses the following options:

```bash
<<-x>>
```

File path and file name of the plug-in definition XML file. If the file path or file name contains spaces, enclose the entire file path, including the file name, in double quotes.
This chapter includes the following topics:

- rcfmu Overview, 110
- rcfmu Migration Rules for Resource Properties, 110
- Running rcfmu, 111
- rcfmu Syntax, 112
- rcfmu Options, 112

rcfmu Overview

rcfmu is a command line program that migrates a resource configuration file from a previous version of Metadata Manager to the current version.

rcfmu creates a new resource configuration file in the directory where you run it or in a directory that you specify. It does not replace the original resource configuration file.

rcfmu writes migration errors to the migration log file. If rcfmu cannot migrate the resource configuration file, check the log file, fix the errors, and rerun rcfmu. The migration log file is <Informatica Installation Directory>\services\MetadataManagerService\utilities\rcfmuUtil\resourcemigration.log.

After you migrate a resource configuration file, you can upload it into the repository.

rcfmu Migration Rules for Resource Properties

To reflect model changes, rcfmu might create or remove resource properties for some resource types. It might also update the names, values, and value sets of some resource properties.

rcfmu applies different migration rules to the following types of properties:

**Unchanged Properties**

If a property is unchanged between versions, rcfmu copies the property from the original resource configuration file to the new resource configuration file.
New Properties

If a property exists in the new resource but not in the original resource, rcfmu creates the property in the new resource configuration file. It applies one of the following rules to determine the value of the property in the new resource configuration file:

- If the property is required, rcfmu assigns the model-provided default value to the property.
- If the property is optional and the model provides a default value, rcfmu assigns the model-provided default value to the property.
- If the property is optional and the model provides no default value, rcfmu assigns a null value to the property.

Renamed Properties

If the property has a different name, rcfmu copies the property value from the original resource configuration file to the corresponding property in the new resource configuration file.

Properties with Value Set Changes

If the property has a different set of values, rcfmu maps the original set of values to the new set of values.

Deleted Properties

If a property exists in the original resource but not in the new resource, rcfmu omits the resource property from the new resource configuration file.

To view the renamed properties, properties with value set changes, and deleted properties for different resource types, see the Informatica Release Guide.

Running rcfmu

You invoke rcfmu from the command line. You can issue commands directly or from a script, batch file, or other program. On Windows, rcfmu is a batch file with a .bat extension. On UNIX, rcfmu is a script file with a .sh extension.

rcfmu is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities rcfmuUtil`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities \MAN\rcfmuUtil`
- `<Informatica utilities installation directory>\MetadataManager\utilities\rcfmuUtil`

1. At a command prompt, navigate to the directory where rcfmu is located.
2. Enter `rcfmu` on Windows or `rcfmu.sh` on UNIX followed by the required arguments.
rcfmu Syntax

rcfmu options and arguments specify connection information for the original repository database.

rcfmu uses the following syntax:

rcfmu.bat
<<dt> databaseType>
<<u> userName>
<<rn> resourceNewName>
[<<ep> encryptedPasswordFlag]
<<smv> sourceMMVersion>
<<rcf> resourceConfigurationFile>
[<<src> sourceFilesDirectoryPath]
<<pw> password>
<<durl> databaseURL>
<<connection_assignment> Retain|Discard>
[<<nr> newRCFDirectoryPath]

rcfmu Options

rcfmu uses the following options:

<<dt>>
Database type for the original Metadata Manager repository database.
Specify one of the following types:
• DB2
• Oracle
• "Microsoft SQL Server"

<<u>>
Database user name for the original Metadata Manager repository database.

<<rn>>
Name of the new resource. If the name contains spaces, enclose it in double quotes.

[<<ep>>]
Required to specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the database user name is encrypted.

<<smv>>
Metadata Manager source version.
Specify one of the following versions:
• 9.1.0
• 9.1.0.HF1~SNAPSHOT
• 9.1.0.HF2~SNAPSHOT
• 9.1.0.HF3~SNAPSHOT
• 9.1.0.HF4~SNAPSHOT
• 9.1.0.HF5~SNAPSHOT
Tip: To get the Metadata Manager source version number, run the mmcmd version command in the original Metadata Manager version.

File path and file name of the resource configuration file that you want to migrate.

File path of metadata source files for the original resource. Required for Embarcadero ERStudio, MicroStrategy, and SAP PowerDesigner resources.

Password for the database user name.

JDBC URL for the original Metadata Manager repository database.

The syntax depends on the repository database type:

- For IBM DB2, use the following syntax:
  
  "jdbc:informatica:db2://[host name]:[port];DatabaseName=[database name]"

- For Microsoft SQL Server, use the following syntax:
  
  "jdbc:informatica:sqlserver://[host name]:[port];SelectMethod=cursor;DatabaseName=[database name]"

To authenticate the database user credentials using Windows authentication and establish a trusted connection to a Microsoft SQL Server repository, append ;AuthenticationMethod=ntlm to the URL.

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.

If you run the program from a machine on which Informatica is not installed, configure the PATH variable to point to the location of the DDJDBCAuth04.dll file.
If the original Metadata Manager repository database uses a secure connection to communicate with external components, you must append additional parameters to the JDBC URL. Configure the parameters as follows:

Append the following parameters to the URL:

- **TrustStore**
- **TrustStorePassword**

If the Oracle database is clustered, use the following syntax:

```
"jdbc:informatica:oracle://[host name]:[port];ServiceName=[service name];AlternateServers = {[host2]:[port]);LoadBalancing=true"
```

If the Oracle database uses the Advanced Security Option, use the following syntax:

```
"jdbc:informatica:oracle://[host name]:[port];SID={SID};EncryptionLevel={encryption level};EncryptionTypes={encryption types};DataIntegrityLevel={data integrity level};DataIntegrityTypes={data integrity types}"
```

**Note:** If secure communication is enabled for the Metadata Manager repository database, you must append additional JDBC parameters to the JDBC URL.

`&-connection_assignment&`

Specifies whether to retain connection assignments in the new resource configuration file. Enter one of the following arguments:

- **Retain.** rcfmu migrates connection assignments to the new resource configuration file. If a connection name changed, you must reassign the connection in the new resource.
- **Discard.** rcfmu does not migrate any connection assignment. However, Metadata Manager automatically configures connection assignments for the new resource when you load it.

`&-nr&`

File path for the new resource configuration file. If you do not specify a file path, rcfmu creates the new resource configuration file in the directory where you run it.

### JDBC Parameters for Secure Databases

If the original Metadata Manager repository database uses a secure connection to communicate with external components, you must append additional parameters to the JDBC URL.

Append the following parameters to the URL:

```
;EncryptionMethod=SSL;TrustStore=<truststore location>;TrustStorePassword=<password>;HostNameInCertificate=<host name>;ValidateServerCertificate=<true|false>;KeyStore=<keystore location>;keyStorePassword=<password>
```

Configure the parameters as follows:

**EncryptionMethod**

Encryption method for data transfer between Metadata Manager and the database server. Must be set to SSL.

**TrustStore**

Path and file name of the truststore file that contains the security certificate of the database server.

**TrustStorePassword**

Password used to access the truststore file.
**HostNameInCertificate**

Host name of the machine that hosts the secure database. If you specify a host name, the Metadata Manager Service validates the host name included in the connection string against the host name in the security certificate.

**ValidateServerCertificate**

Indicates whether the Metadata Manager Service validates the certificate that the database server presents. If you set this parameter to true, the Metadata Manager Service validates the certificate. If you specify the HostNameInCertificate parameter, the Metadata Manager Service also validates the host name in the certificate.

If you set this parameter to false, the Metadata Manager Service does not validate the certificate that the database server presents. The Metadata Manager Service ignores any truststore information that you specify.

**KeyStore**

Path and file name of the keystore file that contains the security certificates that the Metadata Manager Service presents to the database server.

**KeyStorePassword**

Password used to access the keystore file.
rmu Overview

rmu is a command line program that migrates resources from a previous version of Metadata Manager to the current version. rmu migrates deprecated resources and creates new resources that you can use in the current version of Metadata Manager.

You can migrate one resource or all resources in a repository. If you migrate individual resources, migrate and reload JDBC and data management resources before you migrate and reload other types of resources. If you do not migrate and reload resources in this order, you might lose connection information for business intelligence and data modeling resources.

If you migrate one resource, you can specify a name for the new resource. If you do not specify a name for the new resource or you migrate all resources, rmu generates the new resource names. If you migrate an Embarcadero ERStudio, MicroStrategy, or SAP PowerDesigner resource, rmu creates one new resource for each metadata source file.

rmu takes an XML configuration file as an argument. The configuration file specifies connection information for the original repository database. It also specifies authentication information for the original resource and the new resource.

When you migrate a resource, rmu first creates a new resource configuration file and then creates a new resource from the resource configuration file. If errors occur during the migration process, check the migration log file to determine the cause of the errors, and then rerun rmu. The migration log file is \Informeatica\Installation Directory\services\MetadataManagerService\utilities\rcfmuUtil\resourcemigration.log.

After you run rmu, you can view the new resource on the Load tab or the Browse tab.

Metadata Manager displays one of the following statuses for the new resource:
rmu Migration Rules for Resource Properties

To reflect model changes, rmu might create or remove resource properties for some resource types. It might also update the names, values, and value sets of some resource properties.

rmu applies different migration rules to the following types of properties:

**Unchanged Properties**

If a property is unchanged between versions, rmu copies the property from the original resource to the new resource.

**New Properties**

If a property exists in the new resource but not in the original resource, rmu creates the property in the new resource. It applies one of the following rules to determine the value of the property in the new resource:

- If the property is required, rmu assigns the model-provided default value to the property.
- If the property is optional and the model provides a default value, rmu assigns the model-provided default value to the property.
- If the property is optional and the model provides no default value, rmu assigns a null value to the property.

**Renamed Properties**

If the property has a different name, rmu copies the property value from the original resource to the corresponding property in the new resource.

**Properties with Value Set Changes**

If the property has a different set of values, rmu maps the original set of values to the new set of values.

**Deleted Properties**

If a property exists in the original resource but not in the new resource, rmu omits the resource property from the new resource.

To view the renamed properties, properties with value set changes, and deleted properties for different resource types, see the *Informatica Release Guide*. 
Running rmu

You invoke rmu from the command line. You can issue commands directly or from a script, batch file, or other program. On Windows, rmu is a batch file with a .bat extension. On UNIX, rmu is a script file with a .sh extension.

rmu is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities\rcfmuUtil`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\MM\rcfmuUtil`
- `<Informatica utilities installation directory>\MetadataManager\utilities\rcfmuUtil`

1. At a command prompt, navigate to the directory where rmu is located.
2. Enter `rmu` on Windows or `rmu.sh` on UNIX followed by the required arguments.

rmu Syntax

rmu uses the following syntax:

```
rmu.bat
[<<mr> newMigratedResourceName]
<<-r> oldResourceName|ALL>
<<-cf> configurationFile>
<<-connection_assignment> Retain|Discard>
```

rmu Options

rmu uses the following options:

[<<mr>]

Name of the new resource. rmu appends the metadata source file name to Embarcadero ERStudio, MicroStrategy, and SAP PowerDesigner resources.

If you do not enter a value for this option, rmu generates the new resource name as follows:

- Embarcadero ERStudio, MicroStrategy, and SAP PowerDesigner resources. rmu names each new resource `<original name>_new_<file name>`, where `<file name>` is the first 15 characters of the metadata source file name. If the source file names exceed 15 characters, rmu uses sequential numbers for the last character in each resource name.
- Other resources. rmu names the new resource `<original name>_new`.

<<-r>

Name of the resource that you want to migrate. To migrate all resources in a repository, enter `-r all`.

<<-cf>

Name of the XML configuration file.
Specifies whether to retain connection assignments in the new resource.

Enter one of the following arguments:

- **Retain**: rmu migrates connection assignments to the new resource. If a connection name changed, you must reassign the connection in the new resource.

- **Discard**: rmu does not migrate any connection assignment. However, Metadata Manager automatically configures connection assignments for the new resource when you load it.

## rmu Configuration File Format

rmu requires an XML configuration file that specifies connection information for the original Metadata Manager repository and authentication information for the original and new resources. Use a text editor to create and update the rmu configuration file.

The rmu configuration file contains the following elements:

- **configurations**: Root element for the configuration file.
- **sourceService**: Defines the original resource.
- **targetService**: Defines the new resource.
- **MMService**: Defines authentication information for the Metadata Manager service.
- **database**: Defines database information for the original Metadata Manager repository database.
- **user**: In the MMService element, defines the Metadata Manager user name. In the database element, defines the database user name for the original Metadata Manager repository database.
- **password**: Defines the password for the Metadata Manager user. If the domain uses Kerberos authentication, specify either the password or the keytab file.
- **encryptFlag**: Defines whether the password for the Metadata Manager user is encrypted.
- **url**: In the MMService element, defines the Metadata Manager URL. In the database element, defines the URL for the original Metadata Manager repository database.
The rmu resource migration utility takes an XML configuration file that specifies connection information and authentication information.

The following example shows a typical rmu configuration file:

```xml
<configurations>
  <sourceService>
    <MMService>
      <user>Administrator</user>
      <password>Ev+EEmdYj13PeGK1R9Ez+kJIamUMRTZnGHx6bvpC</password>
    </MMService>
    <DBUser01/>
  </sourceService>
  <sinkService>
    <MMService>
      <password>Ev+EEmdYj13PeGK1R9Ez+kJIamUMRTZnGHx6bvpC</password>
    </MMService>
    <DBUser01/>
  </sinkService>
</configurations>
```

**namespace**

If the domain uses Kerberos authentication or LDAP authentication, defines the name of the security domain to which the Metadata Manager user belongs. If the domain uses native authentication, leave this element empty or set the value to **Native**.

**domainName**

Defines the name of the Informatica domain. If the domain uses Kerberos authentication, specify either the domain name or the gateway host name and port number. If the domain does not use Kerberos authentication, leave this element empty or omit it.

**gateway**

Defines the host name and port number of the gateway node in the Informatica domain in the format `<host>:<port>`. If the domain uses Kerberos authentication, specify either the domain name or the gateway host name and port number. If the domain contains multiple gateway nodes, specify the domain name. If the domain does not use Kerberos authentication, leave this element empty or omit it.

**keyTab**

Defines the path and file name of the keytab file for the Metadata Manager user. If the domain uses Kerberos authentication, specify either the password or the keytab file. If the domain does not use Kerberos authentication, leave this element empty or omit it.

**type**

Defines the database type for the original Metadata Manager repository database.

Specify one of the following types:

- DB2
- Oracle
- Microsoft SQL Server

**mmcmdDirPath**

Defines the file path for the mmcmd.bat file. Required for both the original and new resources. rmu uses mmcmd to determine the version of the original resource.

**filesDirPath**

Defines the file path for the original resource configuration file and the metadata source files for the original resource.

### rmu Sample Configuration File

The rmu resource migration utility takes an XML configuration file that specifies connection information and authentication information.

The following example shows a typical rmu configuration file:
<url>jdbc:informatica:oracle://10.65.40.60:1521;SID=goldwing</url>
<type>Oracle</type>
</database>
<mmcmdDirPath>C:\Informatica\9.1.0\mmcmd\mmcmdDirPath</mmcmdDirPath>
<sourceService>
<targetService>
<User>
<user>Administrator</user>
<password>QoZG30qekSjdr97ceGB4f5PJ3ofiF5ZQTtWOf0V8s</password>
<url>http://mminst02r10250</url>
<encryptFlag>true</encryptFlag>
</targetService>
<filesDirPath>C:\users\jsmith\desktop\RCF</filesDirPath>
</configurations>
INDEX

A
assignConnection
  mmcmd command 16
assigning connections
  with mmcmd 16
assignParameterFile
  mmcmd command 18

B
backing up
  Metadata Manager repository 97
backup configuration
  with mmcmd 20
backupConfiguration
  mmcmd command 20
backupRepository
  mmRepoCmd command 97
business terms
  searching with mmcmd 78

cancel
  mmcmd command 22
canceling resources
  with mmcmd 22
categories
  searching with mmcmd 78
connect
  mmcmd command 23
createLinkRuleSet
  mmcmd command 25
createLoadTemplate
  mmcmd command 27
createRepository
  mmRepoCmd command 99
createResource
  mmcmd command 28
creating
  Metadata Manager repository 99
creating load template
  with mmcmd 27
creating resources
  with mmcmd 28
custom resources
  exporting with mmcmd 36
  importing with mmcmd 58

D
data lineage graph database
  creation 90
deleteLinkRuleSet
  mmcmd command 30
deleteLoadTemplate
  mmcmd command 32
deleteRepository
  mmRepoCmd command 100
deleteResource
  mmcmd command 34
deleting
  Metadata Manager repository 100
deleting load template
  with mmcmd 32
deleting resources
  with mmcmd 34

E
encrypt
  mmcmd command 35
exit
  mmcmd command 36
export
  mmcmd command 36
exporting custom resources
  using mmcmd 36
exporting load template
  with mmcmd 51
exporting metadata objects
  using mmcmd 45
exporting models
  using mmcmd 43
exportLinkRuleSetDefs
  mmcmd command 38
exportLinkRuleSets
  mmcmd command 39
exportLoadLog
  mmcmd command 39
exportModel
  mmcmd command 41
exportObject
  mmcmd command 43

G
generateDefaultLoadTemplate
  mmcmd command 47
generateImageMapping
  mmXConPluginUtil command 108
generatePlugin
  mmXConPluginUtil command 109
generating default load template with mmcmd 47
getLinkReport
  mmcmd command 49
getLoadTemplate
  mmcmd command 51
getResource
  mmcmd command 52
getResourceFiles
  mmcmd command 54
getServiceLog
  mmcmd command 56
help
  mmcmd command 58
import
  mmcmd command 58
importing custom resources using mmcmd 58
importing models using mmcmd 62
importing rule sets with mmcmd 60
importLinkRuleSets
  mmcmd command 60
importModel
  mmcmd command 62
load templates (continued)
  listing with mmcmd 65
  updating with mmcmd 85
  loading resources
  getting status with mmcmd 80
  with mmcmd 70
load templates (continued)
  listing with mmcmd 65
  updating with mmcmd 85
  loading resources
  getting status with mmcmd 80
  with mmcmd 70
metadata
  purging with mmcmd 73
Metadata Manager repository
  back-up file location 97
  backing up with mmRepoCmd 97
  backup and restore guidelines 96
  creating with mmRepoCmd 99
  deleting with mmRepoCmd 100
  restoring with mmRepoCmd 104
metadata objects
  searching with mmcmd 78
migrateBGLinks
  mmcmd 72
mmcmd
  certificate validation 13
  commands 14
  connecting in interactive mode 23
  connection timeout period 13
  encrypting text 35
  exiting interactive mode 36
  exporting link summary 49
  exporting load details 41
  exporting service log 56
  interactive mode 12
  migrating business glossary links 72
  MMCmdConfig.properties file 13
    overview 12
    running 14
    server polling interval 13
    truststore path 13
mmLineageMigrator
  options 91
  overview 90
  running 90
  syntax 91
mmRepoCmd
  certificate validation 95
  commands 96
  connection timeout period 95
  MMCmdConfig.properties file 95
  overview 94
  rules and guidelines 96
  server polling interval 95
  truststore path 95
  truststore path 95
mmXConPluginUtil
  commands 108
  overview 107
  running 108
models
  listing with mmcmd 67

parameter files
  assigning with mmcmd 18
PowerCenter repository
  restoring with mmRepoCmd 102

Index 123
purgeMetadata
  mmcmd command 73
purging metadata
  with mmcmd 73

R
rcfmu
  options 112
  overview 110
  resource properties migration rules 110, 117
  running 111
  syntax 112
resource configuration files
  writing 52
resource migration utilities
  rcfmu 110
  rcfmu options 112
  rcfmu syntax 112
  resource properties migration rules 110, 117
  rmu 116
  rmu configuration file format 119
  rmu options 118
  rmu syntax 118
  sample rmu configuration file 120
resources
  assigning connections with mmcmd 16
  backup configuration with mmcmd 20
  canceling load with mmcmd 22
  creating with mmcmd 28
  deleting with mmcmd 34
  get source files with mmcmd 54
  getting properties with mmcmd 52
  linking with mmcmd 63
  listing with mmcmd 58
  loading with mmcmd 70
  purging metadata with mmcmd 73
  restore configuration with mmcmd 75
  restoring
    Metadata Manager repository 104
    PowerCenter repository 102
  resume
    mmcmd command 77
    rmu
      configuration file format 119
rmu (continued)
  options 118
  overview 116
  resource properties migration rules 117
  running 118
  sample configuration file 120
  syntax 118
rule-based inks
  creating rule sets with mmcmd 25
  updating rule sets with mmcmd 83
rule-based links
  deleting rule sets with mmcmd 30
  exporting rule set definitions with mmcmd 38
  exporting rule sets with mmcmd 39
  exporting with a model 43
  exporting with a resource 52
S
search
  mmcmd command 78
service log file
  exporting through mmcmd 56
status
  mmcmd command 80
T
testing connections
  with mmcmd 82
testSourceConnection
  mmcmd command 82
U
updateLinkRuleSet
  mmcmd command 83
updateLoadTemplate
  mmcmd command 85
updateResource
  mmcmd command 86
upating load templates
  with mmcmd 85
upating resources
  with mmcmd 86
V
version
  mmcmd command 89