



Informatica® Test Data Management
10.2.1

Installation Guide

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 names or trademarks of their respective owners.

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

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

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

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

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

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

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

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

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

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

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

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

This product includes software licensed under the terms at <http://www.tcl.tk/software/tcltk/license.html>, <http://www.bosrup.com/web/overlib/?License>, <http://www.stlport.org/doc/license.html>, <http://asm.ow2.org/license.html>, <http://www.cryptix.org/LICENSE.TXT>, <http://hsqldb.org/web/hsqLicense.html>, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, http://www.gzip.org/zlib/zlib_license.html, <http://www.openldap.org/software/release/license.html>, <http://www.libssh2.org>, <http://slf4j.org/license.html>, <http://www.sente.ch/software/OpenSourceLicense.html>, <http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3-license-agreement>, <http://antlr.org/license.html>, <http://aopalliance.sourceforge.net/>, <http://www.bouncycastle.org/license.html>, <http://www.jgraph.com/jgraphdownload.html>, <http://www.jcraft.com/jsch/LICENSE.txt>, http://jotm.objectweb.org/bsd_license.html, <http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>, <http://www.slf4j.org/license.html>, <http://nanoxml.sourceforge.net/org/copyright.html>, <http://www.json.org/license.html>, <http://forge.ow2.org/about/license.html>, <http://www.postgresql.org/about/license.html>, <http://www.sqlite.org/copyright.html>, <http://www.tcl.tk/software/tcltk/license.html>, <http://www.jaxen.org/faq.html>, <http://www.jdom.org/docs/faq.html>, <http://www.slf4j.org/license.html>, <http://www.iodbc.org/dataspace/iodbc/wiki/IODBC/License>, <http://www.keplerproject.org/md5/license.html>, <http://www.toedter.com/en/jcalendar/license.html>, <http://www.edankert.com/bounce/index.html>, <http://www.net-snmp.org/about/license.html>, <http://www.openmdx.org/#FAQ>, http://www.php.net/license/3_01.txt, <http://www.srp.stanford.edu/license.txt>, <http://www.schneider.com/blowfish.html>, <http://www.jmock.org/license.html>, <http://xsom.java.net>, <http://benalman.com/about/license/>, <https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js>, <http://www.h2database.com/html/license.html#summary>, <http://jsoncpp.sourceforge.net/LICENSE>, <http://jdbc.postgresql.org/license.html>, <http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto>, <https://github.com/rantav/hector/blob/master/LICENSE>, <http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html>, <http://jibx.sourceforge.net/jibx-license.html>, <https://github.com/lyokato/libgeohash/blob/master/LICENSE>, <https://github.com/hjiang/jsonxx/blob/master/LICENSE>, <https://code.google.com/p/lz4/>, <https://github.com/jedisct1/libsodium/blob/master/>

LICENSE; <http://one-jar.sourceforge.net/index.php?page=documents&file=license>; <https://github.com/EsotericSoftware/kryo/blob/master/license.txt>; <http://www.scala-lang.org/license.html>; <https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt>; <http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html>; <https://aws.amazon.com/asl/>; <https://github.com/twbs/bootstrap/blob/master/LICENSE>; <https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt>; <https://github.com/documentcloud/underscore-contrib/blob/master/LICENSE>, and <https://github.com/apache/hbase/blob/master/LICENSE.txt>.

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

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

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

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

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

NOTICES

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

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

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at info_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA 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 AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2018-06-09

Table of Contents

Preface	7
Informatica Resources.	7
Informatica Network.	7
Informatica Knowledge Base.	7
Informatica Documentation.	7
Informatica Product Availability Matrixes.	8
Informatica Velocity.	8
Informatica Marketplace.	8
Informatica Global Customer Support.	8
 Chapter 1: Test Data Management Installation Overview.....	9
Installation Overview.	9
Test Data Management Installation.	9
 Chapter 2: Before You Install TDM.....	10
Before You Install TDM on UNIX.	10
Read the Release Notes.	10
Verify the License Key.	11
Verify the Minimum System Requirements.	11
Verify the Status of the Informatica Domain.	12
Set the Environment Variables.	12
Determine Port Availability	12
Set Up a Keystore File.	13
Set Up the X Window Server.	13
Extract the Installer Files on UNIX.	14
Repository Database Requirements.	14
Verify the Database Requirements for the TDM Repository.	15
Set Up the TDM Repository Database.	15
 Chapter 3: Create the Application Services.....	18
Create the Application Services Overview.	18
Prepare Databases for the Informatica Domain.	18
Model Repository Database Requirements.	19
Profiling Warehouse Requirements.	20
Create and Configure the Model Repository Service.	22
Create the Model Repository Service.	22
Create and Configure the Data Integration Service.	25
Create the Data Integration Service.	25
Create and Configure the Content Management Service.	28
Create the Content Management Service.	28

Client Installation.	29
Verify Installation Requirements.	30
Verify Third-Party Software Requirements.	30
Installing in Silent Mode.	30
Install Languages.	31
Configure the Client for a Secure Domain.	32
Configure the Developer Tool Workspace Directory.	32
Starting the Developer Tool.	33
Chapter 4: TDM Installation.	35
TDM Installation Overview.	35
Installing in Graphical Mode.	35
Installing in Console Mode.	36
Installing in Silent Mode.	37
Creating the Properties File.	37
Running the Silent Installer.	38
Chapter 5: After You Install TDM.	39
After You Install TDM Overview.	39
Verify File Permissions.	39
Verify the Services and Objects in the Informatica Domain.	40
Create and Configure the Test Data Manager Service.	40
Test Data Manager Service Dependencies.	41
Creating the Test Data Manager Service.	41
Editing the Test Data Manager Service.	44
Test Data Manager Service Logs.	45
Third-Party JAR Files.	46
Storage Tables for Repeatable Masking.	46
Creating the Storage Tables.	47
Configuring a Non-English Locale Properties File.	47
Chapter 6: Infacmd.	49
infacmd Overview.	49
infacmd tdm Command Reference.	49
CreateService.	49
CreateContents.	55
EnableService.	56
DisableService.	57
removeService.	58
Chapter 7: Starting and Stopping Informatica and TDM.	60
Starting and Stopping Informatica and TDM Overview.	60
Starting Informatica Services.	60

Starting and Stopping Informatica Services Overview	61
Starting and Stopping the Informatica Services.	61
Stopping Informatica in Informatica Administrator.	61
Rules and Guidelines for Starting or Stopping Informatica.	61
Log In to Informatica Administrator.	62
Starting and Stopping the TDM Server.	62
Logging in to Test Data Manager.	63
Chapter 8: Uninstallation.	64
Uninstallation Overview.	64
Rules and Guidelines for Uninstallation.	64
Before You Uninstall.	64
Uninstalling TDM.	64
Appendix A: Updating the DynamicSections Parameter of a DB2 Database... 66	
DynamicSections Parameter Overview.	66
Setting the DynamicSections Parameter.	66
Downloading and Installing the DDconnect JDBC Utility	66
Running the Test for JDBC Tool	67
Appendix B: Locale Codes.	68
Index.	72

Preface

The Informatica *Test Data Management Installation Guide* is written for the system administrator who is responsible for installing Test Data Management. This guide assumes that you have knowledge of relational database concepts and are familiar with the relational database systems and other file systems in your environment. This guide also assumes that you are familiar with the operating systems in your environment.

Informatica Resources

Informatica Network

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

As a member, you can:

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

Informatica Knowledge Base

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

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

Informatica Documentation

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

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

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access PAMs at

<https://network.informatica.com/community/informatica-network/product-availability-matrices>.

Informatica Velocity

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

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

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

Informatica Marketplace

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

Informatica Global Customer Support

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

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:

<http://www.informatica.com/us/services-and-training/support-services/global-support-centers>.

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

CHAPTER 1

Test Data Management Installation Overview

This chapter includes the following topics:

- [Installation Overview, 9](#)
- [Test Data Management Installation, 9](#)

Installation Overview

Use the TDM installer to install Test Data Management.

You must have installed Informatica before you install Test Data Management. Run the installer to install Test Data Management on an existing Informatica domain and node. When you run the Test Data Management installer, you can choose to install in graphical or console mode.

Test Data Management Installation

You can install Test Data Management on a machine that hosts an Informatica node.

Test Data Management runs on the node within the Informatica domain.

The Informatica domain must have Informatica services that you can use to run Test Data Management processes.

Note: If no instance of Informatica exists, you must install Informatica before you install Test Data Management. See the Informatica *Installation and Configuration Guide* for information.

RELATED TOPICS:

- [“Before You Install TDM” on page 10](#)
- [“TDM Installation” on page 35](#)
- [“After You Install TDM” on page 39](#)

CHAPTER 2

Before You Install TDM

This chapter includes the following topics:

- [Before You Install TDM on UNIX, 10](#)
- [Repository Database Requirements, 14](#)

Before You Install TDM on UNIX

You can install TDM on UNIX.

Before you start the installation, set up the machine to meet the requirements to install and run TDM. If the machine where you install TDM is not configured correctly, the installation can fail.

Before you install on UNIX, complete the following tasks:

- Read the Release Notes.
- Verify the license key.
- Verify the system requirements.
- Set up the required environment variables.
- Verify the status of the Informatica Domain.
- Determine the availability of ports for TDM.
- Optionally, set up a keystore file for a secure connection.
- Set up the X Window server.
- Extract the installer files.

Read the Release Notes

Before you install or upgrade, read the product Release Notes. The Release Notes contain important information about the product installation and upgrade process. The Release Notes also contain information about known and fixed limitations.

Verify the License Key

The TDM installation requires a license key.

Before you install TDM to work with an existing instance of Informatica, verify that you have a license key for TDM available. The license key allows you to create the Test Data Manager Service to run the TDM Server and Test Data Manager and create repositories within an Informatica domain.

You can get the license key in one of the following ways:

- Installation DVD. If you receive the Informatica installation files in a DVD, the license key file is included in the Informatica License Key CD.
- FTP download. If you download the Informatica installation files from the Informatica Electronic Software Download (ESD) site, the license key is in an email message from Informatica. Copy the license key file to a directory accessible to the user account that installs the product.

Contact Informatica Global Customer Support if you do not have the required license key.

Verify the Minimum System Requirements

TDM works with Informatica services and repositories in the Informatica domain. The machine where you install TDM must contain an Informatica node and must meet minimum system requirements.

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

<https://network.informatica.com/community/informatica-network/product-availability-matrices>

Minimum System Requirements for TDM

You install TDM on a machine that hosts an Informatica node. The machine must meet the memory and disk space requirements for TDM.

The following table lists the minimum requirements for TDM:

Component	RAM	Disk Space
TDM Server	4 GB	7 GB

Temporary Disk Space Requirements for Installation

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

The following table lists the temporary disk space requirements during installation:

Product	Disk Space
Installer	1 GB
Test Data Management	2 GB

Verify the Status of the Informatica Domain

When you install TDM, you must join an Informatica domain. TDM uses the services, databases, and connections that you configure in the Informatica domain. The domain must have the required application services and repositories to support TDM.

Verify the status of the Informatica domain and the application services in the domain that you plan to join.

Before you start the TDM installation, perform the following tasks:

- Verify the Informatica version installed on the machine where you plan to install TDM. The TDM version that you install must work with the Informatica version installed. For information about installing Informatica, see the Informatica *Installation and Configuration Guide*.
- Install required domain patches and libraries. For information about the required domain patches and libraries, see the *Informatica Release Notes*.
- Verify that the Informatica domain has the following application services:
 - Model Repository Service.
 - Data Integration Service. If you want to perform data discovery, verify that the Data Integration Service is configured to connect to a profiling warehouse.
 - Content Management Service. Required if you perform data masking operations on Hadoop source connections.

Set the Environment Variables

Set the required environment variables to work with the TDM installation.

The following table describes the environment variables to review or set on UNIX:

Variable	Description
IATEMPDIR	Location of the temporary files created during installation. Configure the environment variable if you do not want to create temporary files in the /tmp directory.
JRE_HOME	If you install Informatica services on a machine with 32-bit or 64-bit SUSE Linux or Linux EMT64 operating system, set the JRE_HOME environment variable before you start the installation.
JAVA_HOME	Set the JAVA_HOME environment variable to the root of the JDK directory.
INFA_HOME	Set the INFA_HOME environment variable to the root of the Informatica installation directory.
LANG and LC_ALL	Change the locale to set the appropriate character encoding for the terminal session. For example, set the encoding to <code>Latin1</code> or <code>ISO-8859-1</code> for French, <code>EUC-JP</code> or <code>Shift JIS</code> for Japanese, or <code>UTF-8</code> for Chinese or Korean. The character encoding determines the types of characters that appear in the UNIX terminal.

Determine Port Availability

The installer sets up the ports for the TDM connections.

You can specify the port numbers to use or you can use the default port numbers assigned by the installer. Verify that the port numbers are available on the machine where you install TDM.

The following table describes the ports that are used by TDM:

Port Type	Description
Startup port	Port number that controls the server startup for TDM. The TDM Server listens for startup commands on this port. Default is 6605.
Shutdown port	Port number that controls the server shutdown for TDM. The TDM Server listens for shutdown commands on this port. Default is 6607.
JMX port	Port number for the JMX/RMI connections to TDM. Default is 6675.
HTTPS port	Port number to use when secure connection is enabled for TDM. Default is 6643.

Set Up a Keystore File

You can optionally set up a secure connection to the TDM Server.

When you configure the Test Data Manager Service, you can configure secure communication between the Test Data Manager and the TDM Server. Set up a keystore file and provide the location of the file when you create the Test Data Manager Service to create a secure connection.

Keytool Utility

You can use the keytool utility to generate a keystore file to store the SSL keys and certificates for a secure connection.

Keytool is a key and certificate management utility to generate and administer SSL keys and certificates. The keys and certificates are stored in a keystore file. You can use a self-signed certificate or one signed by a certification authority (CA). To use a certificate signed by a CA, use keytool to generate a Certificate Signing Request (CSR) and apply for a digital identity certificate from a CA.

The keytool utility is shipped with Java. You can find the keytool utility in the /bin directory of the JDK or the JRE directory.

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

<http://java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html>

Set Up the X Window Server

To run the installer in graphical mode, use a graphics display server. If you are logged in remotely to a UNIX machine, you can use an X Window server to redirect the graphics display to your local host.

If you do not have a display device installed on the machine where you want to install the product, you can run the installer by using an X Window server installed on another machine. Use the DISPLAY variable to redirect output of the X Window to another machine that has X Window and xterm installed.

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

Shell	Command
C	setenv DISPLAY <host name>:0
Bash/Korn	export DISPLAY=<host name>:0
Bourne	DISPLAY=<host name>:0 export display

If you do not know the host name of the machine that has the X Window server that you want to use, ask your network administrator. You can also use the IP address of the machine. For more information about redirecting the DISPLAY variable, see the documentation from the UNIX or X Window vendor.

If the X Window server does not support the font that the installer uses, the installer displays the labels on the buttons incorrectly.

Extract the Installer Files on UNIX

Before you perform the installation, extract the installer files on the UNIX machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on install.sh.

The installer files are compressed and distributed as a tar file. Use a native tar or GNU tar utility to extract the installer files to a directory on the UNIX machine. For example,

```
tar -xvf <filename.tar>
```

You can extract the installer files in the following ways:

- Installation DVD. Download the Informatica tar file from the installation DVD to a directory on your machine and then extract the installer files, or extract the installer files directly from the DVD to a directory on your machine.
- FTP download. Download the Informatica installation tar file from the Informatica Electronic Software Download site to a directory on your machine and then extract the installer files.

Note: If you extract the tar file on Windows and then copy the installer files to UNIX, the installation can fail.

Repository Database Requirements

The TDM Server stores configuration and process information in the TDM repository. You must set up the database for the TDM repository before installation. You specify the database connection when you create the Test Data Manager Service.

Before you install TDM, complete the following database setup tasks:

- Verify the database requirements.
- Set up the database.

Verify the Database Requirements for the TDM Repository

Before you start the installation process, verify that the database server has adequate disk space for the TDM repository.

The following table describes the database requirement for the TDM repository:

Informatica Component	Database Type	Disk Space	Comments
TDM repository	IBM DB2 UDB Microsoft SQL Server Oracle Note: On a Microsoft SQL Server database, you must set the collation to case insensitive on the database.	35 MB	Set up the database before you create the Test Data Manager Service. Allocate more space based on the number of objects you plan to store.

After you install TDM, verify that the Informatica domain contains the repositories required to use TDM. If the domain does not contain a Model repository, you must create the repository in the Informatica domain. You must set up the databases before you create the Model Repository Service and Data Integration Service.

The following table describes the requirements for the repository databases:

Informatica Component	Database Type	Disk Space	Comments
Model repository	IBM DB2 UDB Microsoft SQL Server Oracle	200 MB	Set up the database before you create the Model Repository Service. Allocate more space based on the number of repository objects you plan to store.
Profiling warehouse	IBM DB2 UDB Microsoft SQL Server Oracle	35 MB	Set up the database before you create the Data Integration Service.

Set Up the TDM Repository Database

Before you start the installation process, set up a database and user account for the TDM repository.

When you create the Test Data Manager Service, you provide the database and user account information to create the TDM repository. The service uses JDBC to connect to the database and create the repository.

You can create the TDM repository in one of the following databases:

- Oracle
- IBM DB2
- Microsoft SQL Server

Use the following rules and guidelines when you set up the database and user account for the TDM repository:

- The database must be accessible to the gateway nodes in the Informatica domain.
- To prevent database errors from affecting other repositories, create the TDM repository in a separate database schema and with a separate database user account.

See the required Database Requirements sections for information on specific database requirements. For more information about configuring the database, see the documentation for your database system.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:
CREATE SESSION
CREATE TABLE
CREATE VIEW
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Set the system temporary tablespace to 32k bytes.
- If the repository is in an IBM DB2 9.7 database, verify that IBM DB2 Version 9.7 Fix Pack 7 or a later fix pack is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- On the database, set the configuration parameters.

The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

Parameter	Value
applheapsz	8192
appl_ctl_heap_sz	8192
logfilsiz	8000
maxlocks	98

Parameter	Value
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

For more information about updating the DynamicSections parameter, see [Appendix A, "Updating the DynamicSections Parameter of a DB2 Database" on page 66](#).

Microsoft SQL Server Database Requirements (TDM)

You must set the collation to *case insensitive* on the database.

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the allow snapshot isolation and read committed isolation level to ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT to minimize locking contention.
To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

CHAPTER 3

Create the Application Services

This chapter includes the following topics:

- [Create the Application Services Overview, 18](#)
- [Prepare Databases for the Informatica Domain, 18](#)
- [Create and Configure the Model Repository Service, 22](#)
- [Create and Configure the Data Integration Service, 25](#)
- [Create and Configure the Content Management Service, 28](#)
- [Client Installation, 29](#)

Create the Application Services Overview

Use the Administrator tool to create the application services in the required order.

Before you create the application services, you must prepare the following databases:

- Model repository database
- Profiling warehouse

You must create the following application services:

- Model Repository Service
- Data Integration Service
- Content Management Service

Prepare Databases for the Informatica Domain

Informatica stores data and metadata in repositories in the domain. Before you create the application services, set up the databases and database user accounts for the repositories.

Set up a database and user account for the following repositories:

- Model repository
- Profiling warehouse

To prepare the databases, verify the database requirements and set up the database. The database requirements depend on the application services that you create in the domain and the number of data integration objects that you build and store in the repositories.

Model Repository Database Requirements

Informatica services and clients store data and metadata in the Model repository. Configure a separate Model repository to store monitoring statistics. Before you create the Model Repository Service, set up a database and database user account for the Model repository.

The Model repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Allow 3 GB of disk space for DB2. Allow 200 MB of disk space for all other database types.

For more information about configuring the database, see the documentation for your database system.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- If the repository is in an IBM DB2 9.7 database, verify that IBM DB2 Version 9.7 Fix Pack 7 or a later fix pack is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- On the database, set the configuration parameters.

The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

For more information about updating the DynamicSections parameter, see [Appendix A, “Updating the DynamicSections Parameter of a DB2 Database” on page 66](#).

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the allow snapshot isolation and read committed isolation level to ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT to minimize locking contention.
To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the open_cursors parameter to 2000 or higher.
- Verify that the database user has the following privileges:

```
CREATE SEQUENCE
```

```
CREATE SESSION
```

```
CREATE SYNONYM
```

```
CREATE TABLE
```

```
CREATE VIEW
```

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

Profiling Warehouse Requirements

The profiling warehouse database stores profiling and scorecard results. You specify the profiling warehouse connection when you create the Data Integration Service.

The profiling warehouse supports the following database types:

- IBM DB2 UDB

- Microsoft SQL Server
- Oracle

Allow 10 GB of disk space for the database.

Note: Ensure that you install the database client on the machine on which you want to run the Data Integration Service. You can specify a JDBC connection or Hive connection as a profiling warehouse connection for IBM DB2 UDB, Microsoft SQL Server, and Oracle database types.

For more information about configuring the database, see the documentation for your database system.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- The database user account must have the CREATETAB, CONNECT, CREATE VIEW, and CREATE FUNCTION privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

Note: Informatica does not support the partitioned database environment for IBM DB2 databases when you use a JDBC connection as the profiling warehouse connection.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- The database user account must have the CONNECT, CREATE TABLE, CREATE VIEW, and CREATE FUNCTION privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:
 ALTER TABLE
 CREATE ANY INDEX
 CREATE PROCEDURE
 CREATE SESSION
 CREATE TABLE
 CREATE VIEW
 DROP TABLE
 UPDATE TABLE
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- Set the tablespace parameter. Use the following formula to determine the value: 2 MB x (number of tables in each scan x number of concurrent scans)

For example, you have 1,000 tables in each scan and you plan to run 10 scans concurrently. Calculate the tablespace parameter value as follows: 2 MB x (100 x 10) = 20 GB

Note: Tablespace must be distributed across multiple disks.

- Set the following parameters to the Informatica recommended values:

Parameter	Recommended Value
open_cursors	3000
Sessions	1000
Processes	1000

Create and Configure the Model Repository Service

The Model Repository Service is an application service that manages the Model repository. The Model repository stores metadata created by Informatica clients and application services in a relational database to enable collaboration among the clients and services.

When you access a Model repository object from the Developer tool, the Analyst tool, the Administrator tool, or the Data Integration Service, the client or service sends a request to the Model Repository Service. The Model Repository Service process fetches, inserts, and updates the metadata in the Model repository database tables.

Create the Model Repository Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Model Repository Service**.
The **New Model Repository Service** dialog box appears.
3. On the **New Model Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.

Property	Description
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

- Click **Next**.

The **New Model Repository Service - Step 2 of 2** page appears.

- Enter the following properties for the Model repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository.
Password	Repository database password for the database user.
Database Schema	Available for Microsoft SQL Server. Name of the schema that will contain Model repository tables.
Database Tablespace	Available for IBM DB2. Name of the tablespace in which to create the tables. For a multi-partition IBM DB2 database, the tablespace must span a single node and a single partition.

- Enter the JDBC connection string that the service uses to connect to the Model repository database. Use the following syntax for the connection string for the selected database type:

Database Type	Connection String Syntax
IBM DB2	<code>jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server that uses the default instance <code>jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true</code> - Microsoft SQL Server that uses a named instance <code>jdbc:informatica:sqlserver://<host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <host_name>:<port_number>;SID=<database_name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

- If the Model repository database is secured with the SSL protocol, you must enter the secure database parameters in the **Secure JDBC Parameters** field.

Enter the parameters as `name=value` pairs separated by semicolon characters (;). For example:

```
param1=value1;param2=value2
```

Enter the following secure database parameters:

Secure Database Parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to <code>SSL</code> .
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends. If this parameter is set to <code>True</code> , Informatica validates the certificate that the database server sends. If you specify the <code>HostNameInCertificate</code> parameter, Informatica also validates the host name in the certificate. If this parameter is set to <code>False</code> , Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify.
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to <code>cryptoProtocolVersion=TLSv1.1</code> or <code>cryptoProtocolVersion=TLSv1.2</code> based on the cryptographic protocol used by the database server.
TrustStore	Required. Path and file name of the truststore file that contains the SSL certificate for the database. If you do not include the path for the truststore file, Informatica looks for the file in the following default directory: <code><Informatica installation directory>/tomcat/bin</code>
TrustStorePassword	Required. Password for the truststore file for the secure database.

Note: Informatica appends the secure JDBC parameters to the JDBC connection string. If you include the secure JDBC parameters directly in the connection string, do not enter any parameter in the **Secure JDBC Parameters** field.

8. Click **Test Connection** to verify that you can connect to the database.
9. Select **No content exists under specified connection string. Create new content.**
10. Click **Finish**.

The domain creates the Model Repository Service, creates content for the Model repository in the specified database, and enables the service.

Note: When you update the Model Repository Service properties, you must restart the Model Repository Service and the Catalog Service for the modifications to take effect.

After you create the service through the wizard, you can edit the properties or configure other properties.

Create and Configure the Data Integration Service

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

When you preview or run data profiles, SQL data services, and mappings in the Analyst tool or the Developer tool, the client tool sends requests to the Data Integration Service to perform the data integration jobs. When you run SQL data services, mappings, and workflows from the command line program or an external client, the command sends the request to the Data Integration Service.

Create the Data Integration Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Data Integration Service, verify that you have created and enabled the Model Repository Service. If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Data Integration Service can use to access the Model Repository Service.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. In the Domain Navigator, select the domain.
4. Click **Actions > New > Data Integration Service**.

The **New Data Integration Service** wizard appears.

5. On the **New Data Integration Service - Step 1 of 14** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Assign	Select Node to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.
Model Repository Service	Model Repository Service to associate with the service.

Property	Description
Username	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

6. Click **Next**.
The **New Data Integration Service - Step 2 of 14** page appears.
7. Enter the HTTP port number to use for the Data Integration Service.
8. Accept the default values for the remaining security properties. You can configure the security properties after you create the Data Integration Service.
9. Select **Enable Service**.
The Model Repository Service must be running to enable the Data Integration Service.
10. Verify that the **Move to plugin configuration page** is not selected.
11. Click **Next**.
The **New Data Integration Service - Step 3 of 14** page appears.
12. Set the **Launch Job Options** property to one of the following values:
 - In the service process. Configure when you run SQL data service and web service jobs. SQL data service and web service jobs typically achieve better performance when the Data Integration Service runs jobs in the service process.
 - In separate local processes. Configure when you run mapping, profile, and workflow jobs. When the Data Integration Service runs jobs in separate local processes, stability increases because an unexpected interruption to one job does not affect all other jobs.

If you configure the Data Integration Service to run on a grid after you create the service, you can configure the service to run jobs in separate remote processes.
13. Accept the default values for the remaining execution options and click **Next**.
The **New Data Integration Service - Step 4 of 14** page appears.
14. If you created the data object cache database for the Data Integration Service, click **Select** to select the cache connection. Select the data object cache connection that you created for the service to access the database.
15. Accept the default values for the remaining properties on this page and click **Next**.
The **New Data Integration Service - Step 5 of 14** page appears.
16. For optimal performance, enable the Data Integration Service modules that you plan to use.

The following table lists the Data Integration Service modules that you can enable:

Module	Description
Web Service Module	Runs web service operation mappings.
Mapping Service Module	Runs mappings and previews.
Profiling Service Module	Runs profiles and scorecards.
SQL Service Module	Runs SQL queries from a third-party client tool to an SQL data service.
Workflow Orchestration Service Module	Runs workflows.

17. Click **Next**.

The **New Data Integration Service - Step 6 of 14** page appears.

You can configure the HTTP proxy server properties to redirect HTTP requests to the Data Integration Service. You can configure the HTTP configuration properties to filter the web services client machines that can send requests to the Data Integration Service. You can configure these properties after you create the service.

18. Accept the default values for the HTTP proxy server and HTTP configuration properties and click **Next**.

The **New Data Integration Service - Step 7 of 14** page appears.

The Data Integration Service uses the result set cache properties to use cached results for SQL data service queries and web service requests. You can configure the properties after you create the service.

19. Accept the default values for the result set cache properties and click **Next**.

The **New Data Integration Service - Step 8 of 14** page appears.

20. If you created the profiling warehouse database for the Data Integration Service, select the Profiling Service module.

21. If you created the workflow database for the Data Integration Service, select the Workflow Orchestration Service module.

22. Verify that the remaining modules are not selected.

You can configure properties for the remaining modules after you create the service.

23. Click **Next**.

The **New Data Integration Service - Step 11 of 14** page appears.

24. If you created the profiling warehouse database for the Data Integration Service, click **Select** to select the database connection. Select the profiling warehouse connection that you created for the service to access the database.

25. Select whether or not content exists in the profiling warehouse database.

If you created a new profiling warehouse database, select **No content exists under specified connection string**.

26. Click **Next**.

The **New Data Integration Service - Step 12 of 14** page appears.

27. Accept the default values for the advanced profiling properties and click **Next**.

The **New Data Integration Service - Step 14 of 14** page appears.

28. If you created the workflow database for the Data Integration Service, click **Select** to select the database connection. Select the workflow database connection that you created for the service to access the database.

29. Click **Finish**.

The domain creates and enables the Data Integration Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

Create and Configure the Content Management Service

The Content Management Service is an application service that manages reference data. A reference data object contains a set of data values that you can search while performing data quality operations on source data. The Content Management Service also compiles rule specifications into mapplets. A rule specification object describes the data requirements of a business rule in logical terms.

The Content Management Service uses the Data Integration Service to run mappings to transfer data between reference tables and external data sources. The Content Management Service also provides transformations, mapping specifications, and rule specifications with the following types of reference data:

- Address reference data
- Identity populations
- Probabilistic models and classifier models
- Reference tables

Create the Content Management Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Content Management Service, verify that you have created and enabled the following services:

- Model Repository Service

If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Content Management Service can use to access the Model Repository Service.

- Data Integration Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Content Management Service**.

The **New Content Management Service** dialog box appears.

- On the **New Content Management Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
HTTP Port	HTTP port number to use for the Content Management Service.
Data Integration Service	Data Integration Service to associate with the service. The Data Integration Service and the Content Management Service must run on the same node.
Model Repository Service	Model Repository Service to associate with the service.
Username	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.
Reference Data Location	Reference data warehouse connection that you created for the Content Management Service to access the reference data warehouse. Click Select to select the connection.

- Click **Next**.
The **New Content Management Service - Step 2 of 2** page appears.
 - Accept the default values for the security properties.
 - Select **Enable Service**.
The Model Repository Service and Data Integration Service must be running to enable the Content Management Service.
 - Click **Finish**.
The domain creates and enables the Content Management Service.
- After you create the service through the wizard, you can edit the properties or configure other properties.

Client Installation

Verify Installation Requirements

Before you install the Developer tool, verify the installation requirements to run the Developer tool are met.

You can install all the Developer tool on the same machine or on separate machines. You can also install the Developer tool on multiple machines.

Before you install the Developer tool, verify the following installation requirements:

Disk space for the temporary files

The installer writes temporary files to the hard disk. Verify that you have 1 GB disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

Permissions to install the Developer tool

Verify that the user account that you use to install the Developer tool has write permission on the installation directory and Windows registry.

Minimum system requirements to run the Developer tool

The following table lists the minimum system requirements to run the Developer tool:

Client	Processor	RAM	Disk Space
Informatica Developer	1 CPU	1GB	6 GB

Verify Third-Party Software Requirements

Before you install the Informatica clients, verify that you installed the third-party software required by the clients.

Installing in Silent Mode

To install the Informatica clients without user interaction, install in silent mode.

Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install the Informatica clients on multiple machines on the network or to standardize the installation across machines.

To install in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the installer with the installation properties file.

Configuring the Properties File

Informatica provides a sample properties file that includes the properties required by the installer. Customize the sample properties file to create a properties file and specify the options for your installation. Then run the silent installation.

The sample SilentInput.properties file is stored in the root directory of the DVD or the installer download location.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput.properties` file.
3. Create a backup copy of the `SilentInput.properties` file.

4. Use a text editor to open and modify the values of the properties in the file.

The following table describes the installation properties that you can modify:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade the Informatica clients. If the value is 0, the Informatica clients are installed in the directory you specify. If the value is 1, the Informatica clients are upgraded. Default is 0.
UPGRADE_WITHOUT_BIGDATA	Informatica does not support big data products for version 10.1.1 HotFix 2. If you want to install or upgrade to this version, the big data functionality will not be available. Set the value to 1, to continue with the installation. Set the value to 0, to quit the installer.
UPG_BACKUP_DIR	Directory of the previous version of the Informatica client that you want to upgrade.
USER_INSTALL_DIR	Informatica client installation directory.
DXT_COMP	Indicates whether to install Informatica Developer. If the value is 1, the Developer tool will be installed. If the value is 0, the Developer tool will not be installed. Default is 1.

5. Save the properties file.

Running the Silent Installer

After you configure the properties file, open a command prompt to start the silent installation.

1. Open a command prompt.
2. Go to the root of the directory that contains the installation files.
3. Verify that the directory contains the file SilentInput.properties that you edited and resaved.
4. To run the silent installation, run silentInstall.bat.

The silent installer runs in the background. The process can take a while. The silent installation is complete when the Informatica_<Version>_Client_InstallLog<timestamp>.log file is created in the installation directory.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

Install Languages

To view languages other than the system locale and to work with repositories that use a UTF-8 code page, install additional languages on Windows for use with the Informatica clients.

You also must install languages to use the Windows Input Method Editor (IME).

1. Click **Start > Settings > Control Panel**.

2. Click **Regional Options**.
3. Under Language settings for the system, select the languages you want to install.
4. Click **Apply**.

If you change the system locale when you install the language, restart the Windows machine.

Configure the Client for a Secure Domain

When you enable secure communication within the domain, you also secure connections between the domain and Informatica client applications, such as the Developer tool. Based on the truststore files used, you might need to specify the location and password for the truststore files in environment variables on each client host.

You might need to set the following environment variables on each client host:

INFA_TRUSTSTORE

Set this variable to the directory that contains the truststore files for the SSL certificates. The directory must contain truststore files named `infa_truststore.jks` and `infa_truststore.pem`.

INFA_TRUSTSTORE_PASSWORD

Set this variable to the password for the `infa_truststore.jks` file. The password must be encrypted. Use the command line program `pmpasswd` to encrypt the password.

Informatica provides an SSL certificate that you can use to secure the domain. When you install the Informatica clients, the installer sets the environment variables and installs the truststore files in the following directory by default: `<Informatica installation directory>\clients\shared\security`

If you use the default Informatica SSL certificate, and the `infa_truststore.jks` and `infa_truststore.pem` are in the default directory, you do not need to set the `INFA_TRUSTSTORE` or `INFA_TRUSTSTORE_PASSWORD` environment variables.

You must set the `INFA_TRUSTSTORE` and `INFA_TRUSTSTORE_PASSWORD` environment variables on each client host in the following scenarios:

You use a custom SSL certificate to secure the domain.

If you provide an SSL certificate to use to secure the domain, copy the `infa_truststore.jks` and `infa_truststore.pem` truststore files to each client host. You must specify the location of the files and the truststore password.

You use the default Informatica SSL certificate, but the truststore files are not in the default Informatica directory.

If you use the default Informatica SSL certificate, but the `infa_truststore.jks` and `infa_truststore.pem` truststore files are not in the default Informatica directory, you must specify the location of the files and the truststore password.

Configure the Developer Tool Workspace Directory

Configure Informatica Developer to write the workspace metadata to the machine where the user is logged in.

1. Go to the following directory: `<Informatica installation directory>\clients\DeveloperClient\configuration\`
2. Locate the `config.ini` file.
3. Create a backup copy of the `config.ini` file.
4. Use a text editor to open the `config.ini` file.

5. Add the `osgi.instance.area.default` variable to the end of the `config.ini` file and set the variable to the directory location where you want to save the workspace metadata. The file path cannot contain non-ANSI characters. Folder names in the workspace directory cannot contain the number sign (#) character. If folder names in the workspace directory contain spaces, enclose the full directory in double quotes.

- If you run Informatica Developer from the local machine, set the variable to the absolute path of the workspace directory:

```
osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
```

or

```
osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
```

- If you run Informatica Developer from a remote machine, set the variable to the directory location on the local machine:

```
osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
```

or

```
osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
```

The user must have write permission to the local workspace directory.

Informatica Developer writes the workspace metadata to the workspace directory. If you log into Informatica Developer from a local machine, Informatica Developer writes the workspace metadata to the local machine. If the workspace directory does not exist on the machine from which you logged in, Informatica Developer creates the directory when it writes the files.

You can override the workspace directory when you start Informatica Developer.

Starting the Developer Tool

When you start the Developer tool, you connect to a Model repository. The Model repository stores metadata created in the Developer tool. The Model Repository Service manages the Model repository. Connect to the repository before you create a project.

1. From the Windows Start menu, click **Programs > Informatica[Version] > Client > Developer Client > Launch Informatica Developer**.

The first time you run the Developer tool, the Welcome page displays several icons. The Welcome page does not appear when you run the Developer tool subsequently.

2. Click **Workbench**.

The first time you start the Developer tool, you must select the repository in which to save the objects you create.

3. Click **File > Connect to Repository**.

The **Connect to Repository** dialog box appears.

4. If you have not configured a domain in the Developer tool, click **Configure Domains** to configure a domain.

You must configure a domain to access a Model Repository Service.

5. Click **Add** to add a domain.

The **New Domain** dialog box appears.

6. Enter the domain name, host name, and port number.

7. Click **Finish**.

8. Click **OK**.

9. In the **Connect to Repository** dialog box, click **Browse** and select the Model Repository Service.

10. Click **OK**.

11. Click **Next**.
12. Enter a user name and password.
13. Click **Finish**.

The Developer tool adds the Model repository to the Object Explorer view. When you run the Developer tool the next time, you can connect to the same repository.

CHAPTER 4

TDM Installation

This chapter includes the following topics:

- [TDM Installation Overview, 35](#)
- [Installing in Graphical Mode, 35](#)
- [Installing in Console Mode, 36](#)
- [Installing in Silent Mode, 37](#)

TDM Installation Overview

On UNIX, you can run the installer in graphical, console, or silent mode.

When you install TDM, you must join an Informatica domain. The Informatica domain is the fundamental administrative unit for services, users, and resources. The gateway node is the entry point to the domain.

When you run the TDM installer, the installer copies the TDM files to the Informatica home location.

After installation, log in to Informatica Administrator and create a Test Data Manager Service and configure the application services for TDM.

Complete the pre-installation tasks to prepare for the installation.

Installing in Graphical Mode

On the SUSE Linux Enterprise 11 operating system, install TDM in console mode or silent mode.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. Begin the installation.
 - On UNIX, perform the following steps:
 1. Use a shell command line to run `install.sh` from the installer root directory.
 2. Press `g` for graphical mode installation.
4. Verify the prerequisites and then click **Next**.
5. Select the option to install Test Data Management and then click **Next**.
6. Enter the installation directory. The installation directory must be the Informatica home location.

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

7. Click **Next**.

8. Verify the TDM installation settings and disk space requirements and click **Install**.

The installer copies the TDM files to the installation directory. The **Post-Installation Summary** page appears indicating the installation status and the installation directory.

9. Click **Done** to close the installer.

View the installation log files for more information about the tasks performed by the installer and for the configuration properties of the installed components.

10. Restart the Informatica domain.

After installation, log in to Informatica Administrator. You must create a Test Data Manager Service and configure the application services for TDM before you can log in to Test Data Manager.

RELATED TOPICS:

- [Starting and Stopping Informatica](#)
- [“After You Install TDM” on page 39](#)

Installing in Console Mode

You can install TDM in console mode on UNIX.

When you run the installer in console mode, the words quit and back are reserved words. Do not use these words as input text.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. On a shell command line, run the install.sh file from the installer root directory.
4. Press **c** to install in console mode.
5. Verify the prerequisites and then press **Enter** to continue.
6. Press **1** to install Test Data Management.
7. Enter the installation directory. The installation directory must be the Informatica home location.

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

8. Press **Enter** to continue.

9. Review the installation information and press **Enter** to continue.

The installer copies the TDM files to the installation directory.

10. Press **Enter** to exit the installer.

View the installation log files for information about the tasks performed by the installer and for the configuration properties of the installed components.

11. Restart the Informatica domain.

After installation, log in to Informatica Administrator. You must create a Test Data Manager Service and configure the application services for TDM before you can log in to Test Data Manager.

RELATED TOPICS:

- [Starting and Stopping Informatica](#)
- [“After You Install TDM” on page 39](#)

Installing in Silent Mode

To install TDM without user interaction, install in silent mode. Use a properties file to specify the installation parameters. The installer reads the file to determine the installation options.

Copy the installation files to the hard disk on the machine where you plan to install TDM. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on the install.bat and install.sh files. If you install on a remote machine, verify that you can access and create files on the remote machine.

To install in silent mode, complete the following tasks:

1. Create the installation properties file and specify the installation parameters.
2. Run the installer with the installation properties file.

Creating the Properties File

Informatica provides a sample properties file that includes the parameters that the installer requires. You can customize the sample properties file to specify the options for your installation.

The name of the sample properties file is `SilentInput.properties`. The file is located in the installer root directory of the installation DVD or the installer download location. After you customize the file, save the file with the same name in the same directory. Then run the installer in silent mode.

1. Browse to the installer root directory.
2. Find the sample `SilentInput.properties` file.
3. Create a backup copy of the `SilentInput.properties` file.
4. Use a text editor to open the file and enter the values of the installation parameters:

The following table describes the installation parameters:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade TDM. If the value is 0 the installer performs an installation. If the value is 1 the installer performs an upgrade.
TDM_USER_INSTALL_DIR	Absolute path for the directory in which to install TDM. You must install TDM in the Informatica installation location. The directory names in the path must not contain spaces or the following special characters: @ * \$ # ! % () { } [] , ; ' .
PC_OLD_USER_INSTALL_DIR	Absolute path of the installation directory of the previous installed version of Informatica services. Enter this value if you have upgraded Informatica services and INSTALL_TYPE=1.

5. Verify that the values you set are correct. Then save the properties file with the name `SilentInput.properties` in the same directory.

Running the Silent Installer

After you create the properties file, open a command window to start the silent installation.

1. Open a command window.
2. Go to the TDM installer files directory.
3. Verify that the directory contains the `SilentInput.properties` file that you created.
4. Run the silent installer.
On UNIX, run the file `silentinstall.sh`.

The silent installer runs in the background. The process can take a while. View the TDM installation log file in the `<Informatica installation directory>\TDM` location for more information about the tasks performed by the installer and configuration properties for the installed components. If the silent installation fails, the installer creates the `silentErrorLog.log` file.

On UNIX, the installer creates the log file in the `$HOME` directory.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. If the installation fails, view the installation log files and correct the errors. Then run the silent installer again.

CHAPTER 5

After You Install TDM

This chapter includes the following topics:

- [After You Install TDM Overview, 39](#)
- [Verify File Permissions, 39](#)
- [Verify the Services and Objects in the Informatica Domain, 40](#)
- [Create and Configure the Test Data Manager Service, 40](#)
- [Third-Party JAR Files, 46](#)
- [Storage Tables for Repeatable Masking, 46](#)
- [Configuring a Non-English Locale Properties File, 47](#)

After You Install TDM Overview

After you install TDM, create a Test Data Manager Service. Verify that the Informatica domain contains the services and repositories required for TDM operations before you create the Test Data Manager Service. If the domain does not contain the required services and repositories, you must create them before you can create the Test Data Manager Service.

TDM creates a default connection for substitution masking with repeatable values and creates the storage tables for the connection. To use a different storage connection, you must assign the connection as the default storage connection and create storage tables for the substitution values. You can assign the connection as the default connection and create storage tables from the **Administrator | Preferences** view of Test Data Manager.

Verify File Permissions

Verify that users have access to the following files:

- TDM users must have permission and access to all files and folders that TDM uses in plans and workflows.

Verify the Services and Objects in the Informatica Domain

Use the Administrator tool to verify that the Informatica domain contains the services and objects required by TDM.

Log in to the Administrator tool and verify that the domain contains the following services:

Log in to the Administrator tool and verify that the domain contains the following services

Model Repository Service

You must associate the Data Integration Service with a Model repository. The Model Repository Service manages the profiling objects in the Model repository.

Profiling warehouse

To create and run profiles, you must associate the Data Integration Service with a profiling warehouse. The profiling warehouse stores profiling data.

Connection to the profiling warehouse

The Data Integration Service uses the connection when you run a profile.

Data Integration Service

Runs the profiles that you create to perform data discovery.

Content Management Service

Manages reference data and compiles rule specifications into mapplets.

Test Data Manager Service

The Test Data Manager Service creates and manages the TDM repository. You must create a Test Data Manager Service from the Administrator tool before you can access Test Data Manager.

For more information about the Informatica services and repositories, see the *Informatica Application Service Guide*.

Create and Configure the Test Data Manager Service

Before you can use TDM, you must create and configure a Test Data Manager Service from Informatica Administrator.

The Test Data Manager Service manages the TDM repository. When you access a TDM repository object or a test data warehouse object from Test Data Manager, it sends a request to the Test Data Manager Service. The Test Data Manager Service accesses the database content from the TDM repository or connects to the Test Data Warehouse Service associated with it.

Work with the Informatica domain Administrator to create a Test Data Manager Service from Informatica Administrator.

Test Data Manager Service Dependencies

The Test Data Manager Service depends on other application services to perform tasks. Before you create the Test Data Manager Service, you must create the services that it depends on.

Create the application services that the Test Data Manager Service depends on in the following order:

1. **Model Repository Service**
Test Data Manager requires this service to perform data discovery.
2. **Data Integration Service**
Test Data Manager requires this service to perform data discovery.

Create the services before you create the Test Data Manager Service.

Creating the Test Data Manager Service

Log in to the Administrator tool to create the Test Data Manager Service. You can also create the Test Data Manager Service using the TDM command line program.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. Click **Actions > New > Test Data Manager Service**.
The **New Test Data Manager Service** dialog box appears.
4. On the **New Test Data Manager Service - Step 1 of 5** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () [] You cannot change the name of the service after you create it.
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

5. Click **Next**.

6. On the **New Test Data Manager Service - Step 2 of 5** page, enter the following properties:

Property	Description
Model Repository Service	The Model Repository Service associated with the Test Data Manager Service.
User Name	The user name that the Test Data Manager Service uses to connect to the Model Repository Service.
Password	The password that the Test Data Manager Service uses to connect to the Model Repository Service.
Data Integration Service	The Data Integration Service associated with the Test Data Manager Service. The Data Integration Service runs the workflows that you generate when you perform data discovery operations in Test Data Manager. If you have enabled profiling, or if you use Hadoop connections, you must select the Data Integration Service in the domain.

7. Enable data profiling to perform data discovery tasks in TDM, and click **Next**.
8. On the **New Test Data Manager Service - Step 3 of 5** page, enter the following properties:
- The repository connection information must be valid for the service to work.

Property	Description
Database Type	Type of database for the TDM repository. <ul style="list-style-type: none">- Oracle- Microsoft SQL Server- DB2 Note: If you use a Microsoft SQL Server database, you must set the collation to <i>case insensitive</i> on the database.
Username	User account for the TDM repository database. Set up this account using the appropriate database client tools. To apply changes, restart the Test Data Manager Service.
Password	Password for the TDM repository database. Must be in 7-bit ASCII. To apply changes, restart the Test Data Manager Service.
JDBC URL	JDBC connection URL used to access the TDM repository database. Enter the JDBC URL in the following format: <ul style="list-style-type: none">- Oracle: jdbc:informatica:oracle://<host name>:<port>;ServiceName=<service name>- IBM DB2: jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>- Microsoft SQL Server: jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name>
Connection String	Native connect string to the TDM repository database. The Test Data Manager Service uses the connect string to create a connection object to the TDM repository and the PowerCenter repository or Model repository. To apply changes, restart the Test Data Manager Service.

Property	Description
Schema Name	Available for Microsoft SQL Server. Name of the schema for the database. If not selected, the service creates the tables in the default schema.
Creation options for the New Test Data Manager Service	<p>Options to create content, or use existing content, and upgrade existing content.</p> <ul style="list-style-type: none"> - Do not create new content. Creates the repository without creating content. Select this option if the database content exists. If the content is of a previous version, the service prompts you to upgrade the content to the current version. - Previous Test Data Manager Service Name: Enter the name of the previous Test Data Manager Service. Required if you create the service with a different name. <p>Note: If you create the Test Data Manager Service with a different name, the source and target connections do not appear in Test Data Manager. Import the connections again if the connections do not appear in Test Data Manager.</p> <ul style="list-style-type: none"> - Upgrade TDM Repository Contents. Upgrades the content to the current version. - Create new content. Creates repository content.

9. Select the required content creation option.
 - If no content exists, select **Create new content**. You cannot select this option if the database has content.
 - If the database content exists, select **Do not create new content**. If you entered a different name for the Test Data Manager Service, you are prompted to enter the name of the previous Test Data Manager Service. The application checks the version of the content. If the content is of a previous version, an option to upgrade the repository content appears. Upgrade the repository content. Creating the service without upgrading the content to the current version generates a warning.
10. Enable the Test Data Manager Service, and click **Next**.
11. On the **New Test Data Manager Service - Step 4 of 5** page, enter the following properties:

Property	Description
HTTP Port	Port number that TDM runs on. The default is 6605.
Enable Transport Layer Security (TLS)	Secures communication between the Test Data Manager Service and the domain.
HTTPS Port	Port number for the HTTPS connection. The default is 6643.
Keystore File	Path and file name of the keystore file. The keystore file contains the keys and certificates required if you use the SSL security protocol with the Test Data Manager application. Required if you select Enable Transport Layer Security.
Keystore Password	Password for the keystore file. Required if you select Enable Secured Socket Layer.
SSL Protocol	Secure Sockets Layer protocol to use. Default is TLS.

12. Click **Next**.

13. On the **New Test Data Manager Service - Step 5 of 5** page, enter the following properties:

Property	Description
JVM Params	The heap size allocated for Test Data Manager. - Xms512m - Xmx1024m -XX:MaxPermSize=512m The time after which database connections are renewed if the Test Data Manager remains idle. Required if you modified the database configuration settings to values less than the TDM defaults. Configure the following values in TDM to be less than the database values. - IDLE_TIME. -DIDLE_TIME=<seconds>. Default is 300 seconds. - CONNECT_TIME. -DCONNECT_TIME=<seconds>. Default is 5000 seconds.
Connection Pool Size	The JDBC connection pool size.
JMX Port	Port number for the JMX/RMI connections to TDM. Default is 6675.
Shutdown Port	Port number that controls the server shutdown for TDM. The TDM Server listens for shutdown commands on this port. Default is 6607.

RELATED TOPICS:

- [“infacmd tdm Command Reference” on page 49](#)

Editing the Test Data Manager Service

You can edit the Test Data Manager Service from the Administrator tool or using the tdm command line program.

Edit the Test Data Manager Service to create or upgrade content and to edit or update the service properties.

Enabling and Disabling the Test Data Manager Service

You can enable, disable, and recycle the Test Data Manager Service from the service **Actions** menu in the Administrator tool. You can also use the tdm command line program to enable and disable the service.

Disable a Test Data Manager Service to perform maintenance or to temporarily restrict users from accessing Test Data Manager. When you disable the Test Data Manager Service, you also stop Test Data Manager. You might recycle the service if you update a property. When you recycle the service, the Service Manager disables and enables the service.

When you enable the Test Data Manager Service, the Service Manager starts TDM on the node where the service runs.

Assigning a New License to the Test Data Manager Service

If you buy additional licenses, you can assign a different license to the Test Data Manager Service. Unassign the Test Data Manager Service from the existing license and then assign the service to the new license. You must add the license to the domain before you can assign it to the Test Data Manager Service.

Add the new license to the domain from the Domain **Actions** > **New** > **License** option.

To assign a new license to the Test Data Manager Service, perform the following steps in the Administrator tool:

1. Disable the Test Data Manager Service.

2. Select the assigned license in the Domain Navigator.
3. Click **Assigned Services**.
4. Click **Edit Assigned Services**.
5. Select the Test Data Manager Service from the **Assigned Services** list and click **Remove** to unassign it.
6. Select the new license in the Domain Navigator.
7. Click **Assigned Services**.
8. Click **Edit Assigned Services**.
9. Select the Test Data Manager Service from the **Unassigned Services** list and click **Add** to assign it.
10. Click **OK**.
11. Enable the Test Data Manager Service.

Assigning the Test Data Manager Service to a Different Node

You can assign the Test Data Manager Service to a different node in the domain. The new node that uses the Test Data Manager Service must have TDM installed.

1. Disable the Test Data Manager Service.
2. Click **Edit** in the **General Properties** section.
3. Select a different node for the Node property, and then click **OK**.
4. If the Test Data Manager Service is running in HTTPS security mode, change the Keystore File Location to the path on the new node. Click **Edit** in the **Server Configuration Properties** section and update the Keystore File location, and click **OK**.
5. Enable the Test Data Manager Service.

Test Data Manager Service Logs

The Test Data Manager Service logs contain detailed information about all Test Data Manager Service actions. View the Test Data Manager Service logs from the **Logs | Services** view in the Administrator tool.

View detailed information about Test Data Manager Service startup and shut down. You can also view console logs and error log messages in the Test Data Manager Service logs in the Administrator tool.

View information about content creation and content upgrade when you perform a service upgrade or create content for the service.

You can access all the Test Data Manager Service logs from the **Logs | Services** view of the Administrator tool.

Viewing Test Data Manager Service Logs

View the event logs for the Test Data Manager Service that you want to monitor.

You can view messages for events such as enablement, disablement, content creation, and content upgrade of the Test Data Manager Service.

1. In the Administrator tool, click the **Logs** tab.
2. Select the **Service** view.

The contents panel displays event logs for all services.
3. From the **Service Type** list, select Test Data Manager Service.

4. From the **Service Name** list, select the Test Data Manager Service that you want to monitor.
5. Click the **Filter** button.
The Log Manager retrieves the log events and displays the most recent log events first.
To narrow down the list of log events, select the severity and time period of the events that you want to view. Click the **Filter** button again to refresh the list.

Third-Party JAR Files

Ensure that you copy all required third-party JAR files to required locations.

- To use a Teradata or a Teradata Parallel Transporter connection as a staging connection, the Teradata JDBC JAR files `tdgssconfig.jar` and `terajdbc4.jar` must be present in the following location:
`<Informatica installation directory>\TDM\utilities\mapgen\thirdpartylib.`
Create a `thirdpartylib` folder and copy the JAR files before you configure the connection as a staging connection.
- Before you can test a Teradata or a Teradata Parallel Transporter connection, you must add the Teradata JDBC JAR files `tdgssconfig.jar` and `terajdbc4.jar` to the following location:
`<Informatica installation directory>\TDM\lib\thirdparty.`
Restart the Test Data Manager Service after you add the files.
- Before you can test a JDBC connection that you configure with a MySQL database, you must add the MySQL JDBC JAR file `mysql-connector-java-5.1.44-bin.jar` to the following location:
`<Informatica installation directory>\TDM\lib\thirdparty.`
Restart the Test Data Manager Service after you add the JAR file.
- Before you can test a Netezza connection, you must add the Netezza JDBC JAR file `nzjdbc.jar` to the following location:
`<Informatica installation directory>\TDM\lib\thirdparty.`
Restart the Test Data Manager Service after you add the JAR file.

Storage Tables for Repeatable Masking

To perform expression masking or substitution masking with repeatable values, you must assign a storage table for the repeatable values. You can create the table in the TDM repository database or in another database. TDM creates a default storage connection and creates storage tables for this connection.

If you choose to use a different storage connection, you must set this connection as the default connection and create the storage tables for the connection. Set the connection as the default storage and staging connections and create storage tables in Test Data Manager.

Staging connections and storage connections can be on Oracle, Sybase, IBM DB2, or Microsoft SQL Server databases. You can create a staging connection on Teradata and Teradata Parallel Transporter connections.

Note: To use a Teradata or a Teradata Parallel Transporter connection as a staging connection, the Teradata JDBC JAR files `tdgssconfig.jar` and `terajdbc4.jar` must be present in the following location:
`<Informatica installation directory>\TDM\utilities\mapgen\thirdpartylib.` Create a `thirdpartylib` folder and copy the JAR files before you configure the connection as a staging connection.

You can create the storage tables for the required staging and storage connection from the **Administrator** view in Test Data Manager.

You can also use the SQL scripts that Informatica provides to create the storage tables. Use your database client tool to run the SQL script and create the table in the database. For example, you can use the SQL*Plus client for Oracle to create the storage table in an Oracle database.

Run the storage table SQL script for your database. For example, to create the substitution storage table in a Microsoft SQL Server database, run the *Substitution_SQL_Server.sql* file. The SQL scripts to create the storage table for repeatable expression masking are installed in the following TDM directory:

```
<TDM Installation Directory>/TDM/storage_script/expression_storage
```

After you run the expression storage script, verify that the script created the IDM_EXPRESSION_STORAGE table in the database. The SQL scripts to create the storage table for repeatable substitution masking are installed in the following TDM directory:

```
<TDM Installation Directory>/TDM/storage_script/substitution_storage
```

After you run the substitution storage script, verify that the script created the IDM_SUBSTITUTION_STORAGE table in the database.

Important: The expression and substitution storage tables can contain original values from the source database and the corresponding masked values from the target database. Ensure that access to the storage table is secure. Alternatively, you can create the expression or substitution storage table in a database with limited user access.

Creating the Storage Tables

Create storage tables if you do not want to use the default staging and storage connection and storage tables that TDM creates.

1. In the **Administrator | Preferences** view, click **Edit** in the **Workflow Generation** section.
The **Edit Preferences** dialog box appears.
2. Select the required default storage connection from the list.
3. Click **Create Storage Tables** to create the storage tables for this connection.

Configuring a Non-English Locale Properties File

When you install TDM, the installer creates a locale properties file PC_en_US.properties. The installer creates the file for an English locale. Create a locale properties file with the correct name and entry if you install TDM with a different locale.

1. Browse to the following location: <Informatica installation directory>/TDM/lang.
2. Create a file with the following name format: PC_<locale code>.properties. For example, for a setup with a Brazilian Portuguese locale, the file name would be PC_pt_BR.properties.
3. Add an entry *PARTITION_LABEL=<Locale specific "Partition #">*.
For example, for a setup with a Brazilian Portuguese locale, the entry would be *PARTITION LABEL=Partição n°*.
4. Save the file in the same location.

RELATED TOPICS:

- [“Locale Codes” on page 68](#)

CHAPTER 6

Infacmd

This chapter includes the following topics:

- [infacmd Overview, 49](#)
- [infacmd tdm Command Reference, 49](#)

infacmd Overview

infacmd is a command line program that allows you to administer services in the domain. You can create the service, add content to the service, enable the service, and disable the service with the *infacmd* command.

Use the *infacmd* command line program to administer the Test Data Manager Service and the Test Data Warehouse Service.

Run the commands from the `<INFA_HOME>\isp\bin` path.

You do not need to add the `UserName` and `Password` options when you run the commands in Kerberos network authentication mode.

infacmd tdm Command Reference

The *infacmd* tdm program administers the Test Data Manager Service.

You can create the service, add content to the service, enable the service and disable the service with the *infacmd* tdm commands.

CreateService

Creates a Test Data Manager Service in a domain.

The *infacmd* tdm `CreateService` command uses the following syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
```

```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-LicenseName|-ln> license_name

<-MRSServiceName|-mrs> model_repo_service

<-MRSUserName|-rsun> model_repo_service_username

<-MRSPassword|-rspd> model_repo_service_password

[<-MRSSecurityDomain|-rsdn> model_repo_security_domain]

<-EnableProfiling|-ep> enable_profiling

<-DISServiceName|-dis> data_integration_service

<-db_type|-dt> database_type (ORACLE, DB2, SQLSERVER or CUSTOM)

<-DBUsername|-du> db_user

<-DBPassword|-dp> db_password

<-DBUrl|-dl> db_url

<-DBConnString|-dc> db_conn_string

[<-DbSchema|-ds> db_schema (used for SQL Server only)]

[<-DbTablespace|-db> db_tablespace (used for DB2 only)]

[<-HttpPort> http_port]

[<-HttpsPort> https_port]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

[<-SSLProtocol|-sp> ssl_protocol]

[<-jvmParams|-jp> jvmParameters]

[<-connPoolSize|-cp> conn_pool_size]

[<-jmxPort> jmx_port]

[<-shutdownPort> shutdown_port]

[<-hadoopDistDir> Hadoop Distribution Directory]

[<-hadoopKerbSPN> Hadoop Kerberos Service Principal Name]

[<-hadoopKerbKeytab> Hadoop Kerberos Keytab]

```

The following table describes infacmd tdm CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Test Data Manager Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > "
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.
-NodeName -nn	node_name	Required. Name of the node where the service will run.
-LicenseName -ln	license_name	Required. Name of the license. The name is not case sensitive and must be unique within the domain. The name cannot exceed 79 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > "
-MRSServiceName -mrs	model_repo_service	Name of the Model Repository Service to which TDM connects.
-MRSUserName -rsun	model_repo_service_username	Required. User name to connect to the Model repository.
-MRSPassword -rspd	model_repo_service_password	Required. Password for the user name to connect to the Model repository. The password is case sensitive.
-MRSSecurityDomain -rsdn	model_repo_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Security domain is case sensitive. Default is Native.
-EnableProfiling -ep	enable_profiling	Indicates data discovery settings. Set to true to enable data discovery. Set to false to disable data discovery.
-DISServiceName -dis	data_integration_service	Name of the Data Integration Service to which TDM connects.
-db_type -dt	database_type	Type of TDM repository database. Values are Oracle, SQL Server, DB2, or Custom.
-DBUsername -du	db_user	Required. Account for the repository database. Use the database client to set up this account.
-DBPassword -dp	db_password	Required. Repository database password for the database user.

Option	Argument	Description
-DBUrl -dl	db_url	<p>Required. JDBC connect string to the database for the TDM repository. Use one of the following syntaxes:</p> <p>Oracle:</p> <pre>jdbc:informatica:oracle: // <machineName>:<PortNo>;ServiceName= <DBName>; MaxPooledStatements=20; CatalogOptions=0; EnableServerResultCache=true</pre> <p>DB2:</p> <pre>jdbc:informatica:db2: //<host>:<port>; DatabaseName=<dbname>; BatchPerformanceWorkaround=true;Dynam icSections=1000</pre> <p>SQLServer:</p> <pre>jdbc:informatica:sqlserver: // <host>:<port>; DatabaseName=<dbname>; SnapshotSerializable=true</pre>
-DBConnString -dc	db_conn_string	Native connect string to the TDM repository database. The service uses the connect string to create a connection object to the Test Data Manager repository and the PowerCenter repository or Model repository.
-DbSchema -ds	db_schema	Optional. The schema name for a Microsoft SQL Server database.
-DbTablespace -db	db_tablespace	<p>Required for a DB2 database only. When you configure a tablespace name, the Test Data Manager Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name.</p> <p>The tablespace must be defined on a single node and the page size must be 32 KB. In a multipartition database, you must select this option. In a single-partition database, if you do not select this option, the installer creates the tables in the default tablespace.</p>
-HttpPort	http_port	Required. Port number for the service.
-HttpsPort	https_port	Optional. Port number to secure the connection to the Administrator tool. Set this port number if you want to configure HTTPS for a node.
-KeystoreFile -kf	keystore_file_location]	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol with PowerCenter.
-KeystorePassword -kp	keystore_password	Optional. If TLS is enabled, you must specify a password.

Option	Argument	Description
-SSLProtocol -pt	SSL Protocol	Optional. Secure Sockets Layer protocol to use. Editable if you enable Transport Layer Security (TLS).
-jvmParams -jp	jvmParameters	<p>JVM parameters to set:</p> <ul style="list-style-type: none"> - The heap size allocated for Test Data Manager. - The time after which database connections are renewed if the TDM UI remains idle. Required if you have modified the database configuration settings to values less than the TDM defaults. Edit the values in TDM such that the values are less than the database values. <p>Include the JVM parameters in single quotes and then in double quotes. For example, 'value' and then "value".</p> <p>The -Xms option is case sensitive. For example: "- Xms512m - Xmx1024m - XX:MaxPermSize=512m"</p> <ul style="list-style-type: none"> - IDLE_TIME. -DIDLE_TIME=<seconds>. Default is 300 seconds. - CONNECT_TIME. -DCONNECT_TIME=<seconds>. Default is 5000 seconds.
-connPoolSize -cp	conn_pool_size	Optional. The maximum number of idle connection instances that a pool maintains for a database connection before the maximum idle time is met. Set this value to be more than the minimum number of idle connection instances. Default is 15.
-jmxPort	jmx_port	Port number for the JMX/RMI connections to TDM. Default is 6675.
-shutdownPort	shutdown_port	Port number that controls shutdown for TDM.
-hadoopDistDir -hdd	Hadoop Distribution Directory	The Hadoop distribution directory on the Test Data Manager Service node.
-hadoopKerbSPN -hks	Hadoop Kerberos Service Principal Name	<p>Service Principal Name (SPN) of the Data Integration Service to connect to a Hadoop cluster that uses Kerberos authentication.</p> <p>Not required when you run the MapR Hadoop distribution. Required for other Hadoop distributions.</p>
-hadoopKerbKeytab -hkt	Hadoop Kerberos Keytab	<p>The file path to the Kerberos keytab file on the machine on which the Data Integration Service runs.</p> <p>Not required when you run the MapR Hadoop distribution. Required for other Hadoop distributions.</p>

CreateContents

Creates repository content for the Test Data Manager repository.

The infacmd tdm CreateContents command uses the following syntax:

```
<-DomainName|-dn> domain_name  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
<-ServiceName|-sn> service_name  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd tdm CreateContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. The Test Data Manager Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

EnableService

Enables the Test Data Manager Service.

The infacmd tdm EnableService command uses the following syntax:

```
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd tdm EnableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the service you want to run the command against. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

DisableService

Disables the Test Data Manager Service. When you disable the Test Data Manager Service, all the service processes stop.

The infacmd tdm DisableService command uses the following syntax:

```
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-DisableMode|-dm> disable_mode: COMPLETE|ABORT|STOP
```

The following table describes infacmd tdm DisableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the service you want to run the command against. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-DisableMode -dm	disable_mode	Required. Defines how the service is disabled: <ul style="list-style-type: none"> - Complete. Disables the service after all service processes stop. - Abort. Stops all processes immediately, and then disables the service. - Stop. Stops all running workflows, and then disables the service.

removeService

Removes the Test Data Manager Service from the domain. Before you remove a service, you must disable it.

The infacmd tdm removeService command uses the following syntax:

```
removeService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ServiceName|-sn> service_name
```

The following table describes infacmd tdm removeService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of service you want to remove. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

CHAPTER 7

Starting and Stopping Informatica and TDM

This chapter includes the following topics:

- [Starting and Stopping Informatica and TDM Overview, 60](#)
- [Starting Informatica Services, 60](#)
- [Log In to Informatica Administrator, 62](#)
- [Starting and Stopping the TDM Server, 62](#)
- [Logging in to Test Data Manager, 63](#)

Starting and Stopping Informatica and TDM Overview

When you install TDM and join an Informatica domain, the Informatica services must be running before you start the TDM Server.

On the node where you install Informatica and TDM, the installer creates a UNIX daemon to run Informatica.

On UNIX, you must start the Informatica daemon manually when the installation completes. Start or stop the Informatica daemon from the command line.

You use the Administrator tool to administer the Informatica domain objects and user accounts. Log in to the Administrator tool to create the user accounts for users of Informatica and TDM and to create and configure the Test Data Manager Service and other application services in the domain. You can also use the Administrator tool to shut down a node. When you shut down a node, you stop Informatica services on the node.

You can use Test Data Manager to configure and run TDM operations. You must create and enable the Test Data Manager Service before you can log in to Test Data Manager.

Starting Informatica Services

Starting and Stopping Informatica Services Overview

On each node where you install Informatica, the installer creates a Linux daemon to run Informatica. When the installation completes successfully, the installer starts the Informatica daemon on Linux.

The Informatica service runs the Service Manager on the node. The Service Manager manages all domain functions and starts application services configured to run on the node. The method you use to start or stop Informatica depends on the operating system. You can use Informatica Administrator to shut down a node. When you shut down a node, you stop Informatica on the node.

You can configure the behavior of the Informatica service.

The Informatica service also runs Informatica Administrator. You use Informatica Administrator to administer the Informatica domain objects and user accounts. Log in to Informatica Administrator to create the user accounts for users of Informatica and to create and configure the application services in the domain.

Starting and Stopping the Informatica Services

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

```
<Informatica installation directory>/tomcat/bin
```

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

```
infaservice.sh startup
```

Enter the following command to stop the daemon:

```
infaservice.sh shutdown
```

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

Stopping Informatica in Informatica Administrator

When you shut down a node using Informatica Administrator, you stop the Informatica service on that node.

You can abort the processes that are running or allow them to complete before the service shuts down. If you shut down a node and abort the repository service processes running on the node, you can lose changes that have not yet been written to the repository. If you abort a node running integration service processes, the workflows will abort.

1. Log in to Informatica Administrator.
2. In the Navigator, select the node to shut down.
3. On the Domain tab **Actions** menu, select **Shutdown Node**.

Rules and Guidelines for Starting or Stopping Informatica

Consider the following rules and guidelines when starting and stopping Informatica on a node:

- When you shut down a node, the node is unavailable to the domain. If you shut down a gateway node and do not have another gateway node in the domain, the domain is unavailable.
- When you start Informatica, verify that the port used by the service on the node is available. For example, if you stop Informatica on a node, verify that the port is not used by any other process on the machine before you restart Informatica. If the port is not available, Informatica will fail to start.

- If you do not use Informatica Administrator to shut down a node, any process running on the node will be aborted. If you want to wait for all processes to complete before shutting down a node, use Informatica Administrator.
- If you have two nodes in a domain with one node configured as a primary node for an application service and the other node configured as a backup node, start Informatica on the primary node before you start the backup node. Otherwise, the application service will run on the backup node and not the primary node.

Log In to Informatica Administrator

You must have a user account to log in to the Informatica Administrator web application.

If the Informatica domain runs on a network with Kerberos authentication, you must configure the browser to allow access to the Informatica web applications. In Microsoft Internet Explorer and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. If you are using Chrome version 41 or later, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

1. Start a Microsoft Internet Explorer or Google Chrome browser.
2. In the **Address** field, enter the URL for the Administrator tool:
 - If the Administrator tool is not configured to use a secure connection, enter the following URL:

`http://<fully qualified hostname>:<http port>/administrator/`

- If the Administrator tool is configured to use a secure connection, enter the following URL:

`https://<fully qualified hostname>:<http port>/administrator/`

Host name and port in the URL represent the host name and port number of the master gateway node. If you configured secure communication for the domain, you must use HTTPS in the URL to ensure that you can access the Administrator tool.

If you use Kerberos authentication, the network uses single sign on. You do not need to log in to the Administrator tool with a user name and password.

3. If you do not use Kerberos authentication, enter the user name, password, and security domain for your user account, and then click **Login**.

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

Note: If this is the first time you log in with the user name and password provided by the domain administrator, change your password to maintain security. Informatica Administrator and most application services take a long time to run on Microsoft Windows Server 2016.

Starting and Stopping the TDM Server

You must start the TDM Server before you can access Test Data Manager. The TDM Server is managed by the Test Data Manager Service.

Start the TDM Server by enabling the Test Data Manager Service from the Informatica Administrator. To stop the server, disable the Test Data Manager Service. You cannot use Test Data Manager to access the TDM Server contents when the Test Data Manager service is disabled.

Logging in to Test Data Manager

You must have an Informatica user account to log in to Test Data Manager. Use the Informatica Administrator to create an Informatica user account.

1. Start a Microsoft Internet Explorer or Google Chrome browser.
2. In the **Address** field, enter the URL for Test Data Manager:

`http://<HostName>:<PortNumber>/tdm`

HostName represents the host name of the machine where TDM is installed. *PortNumber* is the startup port number for TDM. The default port number is 6605.

If you configure TDM to use HTTPS, the URL opens the HTTPS site:

`https://<HostName>:<HTTPSPortNumber>/tdm`

3. On the login page, enter an Informatica user name and password.
When you initially log in after installation, you can use the Informatica administrator user account.
4. Click **Login**.

CHAPTER 8

Uninstallation

This chapter includes the following topic:

- [Uninstallation Overview, 64](#)

Uninstallation Overview

On UNIX, uninstall TDM from the command line.

The uninstallation process deletes the TDM files and clears all configuration. The process does not delete files that are not installed with TDM. For example, the installation process creates temporary directories. The uninstaller does not keep a record of these directories and therefore cannot delete them. You must manually delete these directories for a clean uninstallation.

Rules and Guidelines for Uninstallation

Use the following rules and guidelines when you uninstall TDM:

- The uninstallation mode depends on the mode that you use to install TDM. For example, you install TDM in console mode. When you run the uninstaller, it runs in console mode.
- Uninstalling TDM does not delete the TDM repository or the test data warehouse repository. The uninstaller removes the TDM files. It does not remove repositories from the database. If you need to move the repositories, you can back them up and restore them to another database.
- The uninstaller does not create a log of the uninstallation process. At the end of the uninstallation process, the uninstaller displays the names of the files and directories that could not be removed.

Before You Uninstall

Before you uninstall TDM, stop and disable the Test Data Manager Service. The uninstallation process cannot remove the files that are being used by a service that is running.

Uninstalling TDM

To uninstall TDM, use the uninstaller created during the installation. When you run the installation, the installer creates the following directory for the uninstaller:

```
<TDM installation directory>/Uninstaller_TDM
```


Running the Uninstaller on UNIX

To uninstall TDM on UNIX, run the uninstaller from the command line.

Go to the following directory:

```
<TDM installation directory>/Uninstaller_TDM
```

Run the uninstaller with the following command:

```
./uninstaller
```

APPENDIX A

Updating the DynamicSections Parameter of a DB2 Database

This appendix includes the following topics:

- [DynamicSections Parameter Overview, 66](#)
- [Setting the DynamicSections Parameter, 66](#)

DynamicSections Parameter Overview

IBM DB2 packages contain the SQL statements to be executed on the database server. The DynamicSections parameter of a DB2 database determines the maximum number of executable statements that the database driver can have in a package. You can raise the value of the DynamicSections parameter to allow a larger number of executable statements in a DB2 package. To modify the DynamicSections parameter, connect to the database using a system administrator user account with BINDADD authority.

Setting the DynamicSections Parameter

Use the DataDirect Connect for JDBC utility to raise the value of the DynamicSections parameter in the DB2 database.

To use the DataDirect Connect for JDBC utility to update the DynamicSections parameter, complete the following tasks:

- Download and install the DataDirect Connect for JDBC utility.
- Run the Test for JDBC tool.

Downloading and Installing the DDconnect JDBC Utility

Download the DataDirect Connect for JDBC utility from the DataDirect download web site to a machine that has access to the DB2 database server. Extract the contents of the utility file and run the installer.

1. Go to the DataDirect download site:
<http://www.datadirect.com/support/product-documentation/downloads>
2. Choose the Connect for JDBC driver for an IBM DB2 data source.

3. Register to download the DataDirect Connect for JDBC Utility.
4. Download the utility to a machine that has access to the DB2 database server.
5. Extract the contents of the utility file to a temporary directory.
6. In the directory where you extracted the file, run the installer.

The installation program creates a folder named testforjdbc in the installation directory.

Running the Test for JDBC Tool

After you install the DataDirect Connect for JDBC Utility, run the Test for JDBC tool to connect to the DB2 database. You must use a system administrator user account with the BINDADD authority to connect to the database.

1. In the DB2 database, set up a system administrator user account with the BINDADD authority.
2. In the directory where you installed the DataDirect Connect for JDBC Utility, run the Test for JDBC tool (testforjdbc).
3. On the Test for JDBC Tool window, click Press Here to Continue.
4. Click Connection > Connect to DB.
5. In the Database field, enter the following text:

```
jdbc:datadirect:db2://  
HostName:PortNumber;databaseName=DatabaseName;CreateDefaultPackage=TRUE;ReplacePackage=TRUE;DynamicSections=3000
```

HostName is the name of the machine hosting the DB2 database server.

PortNumber is the port number of the database.

DatabaseName is the name of the DB2 database.

6. In the User Name and Password fields, enter the system administrator user name and password you use to connect to the DB2 database.
7. Click Connect, and then close the window.

APPENDIX B

Locale Codes

When you install TDM, the installer creates a locale properties file for an English locale. If you install TDM with a different locale, you can use the correct locale code to create a locale properties file that you require.

The following table lists the locales and their corresponding locale codes:

Locale	Locale Code
Arabic (Algeria)	ar_DZ
Arabic (Bahrain)	ar_BH
Arabic (Egypt)	ar_EG
Arabic (Iraq)	ar_IQ
Arabic (Jordan)	ar_JO
Arabic (Kuwait)	ar_KW
Arabic (Lebanon)	ar_LB
Arabic (Libya)	ar_LY
Arabic (Morocco)	ar_MA
Arabic (Oman)	ar_OM
Arabic (Qatar)	ar_QA
Arabic (Saudi Arabia)	ar_SA
Arabic (Sudan)	ar_SD
Arabic (Tunisia)	ar_TN
Arabic (United Arab Emirates)	ar_AE
Arabic (Yemen)	ar_YE
Belarusian (Belarus)	be_BY
Bulgarian (Bulgaria)	bg_BG

Locale	Locale Code
Chinese (China)	zh_CN
Chinese (Hong Kong)	zh_HK
Chinese (Macao)	zh_MO
Chinese (Singapore)	zh_SG
Chinese (Taiwan)	zh_TW
Croatian (Croatia)	hr_HR
Dutch (Belgium)	nl_BE
Dutch (Netherlands)	nl_NL
English (Australia)	en_AU
English (Canada)	en_CA
English (India)	en_IN
English (Ireland)	en_IE
English (New Zealand)	en_NZ
English (South Africa)	en_ZA
English (United Kingdom)	en_GB
English (United States)	en_US
French (Belgium)	fr_BE
French (Canada)	fr_CA
French (France)	fr_FR
French (Luxembourg)	fr_LU
French (Switzerland)	fr_CH
German (Austria)	de_AT
German (Germany)	de_DE
German (Italy)	de_IT
German (Luxembourg)	de_LU
German (Switzerland)	de_CH
Greek (EL)	el_EL

Locale	Locale Code
Hebrew (Israel)	he_IL
Italian (Italy)	it_IT
Italian (Switzerland)	it_CH
Japanese (Japan)	ja_JP
Kazakh (Kazakhstan)	kk_KZ
Korean (South Korea)	ko_KR
Macedonian (Macedonia)	mk_MK
Portuguese (Brazil)	pt_BR
Portuguese (Portugal)	pt_PT
Russian (Russia)	ru_RU
Slovenian (Slovenia)	sl_SI
Spanish (Argentina)	es_AR
Spanish (Bolivia)	es_BO
Spanish (Chile)	es_CL
Spanish (Colombia)	es_CO
Spanish (Costa Rica)	es_CR
Spanish (Dominican Republic)	es_DO
Spanish (Ecuador)	es_EC
Spanish (El Salvador)	es_SV
Spanish (Guatemala)	es_GT
Spanish (Honduras)	es_HN
Spanish (Mexico)	es_MX
Spanish (Nicaragua)	es_NI
Spanish (Panama)	es_PA
Spanish (Paraguay)	es_PY
Spanish (Peru)	es_PE
Spanish (Puerto Rico)	es_PR

Locale	Locale Code
Spanish (Spain)	es_ES
Spanish (Uruguay)	es_UY
Spanish (Venezuela)	es_VE
Turkish (Turkey)	tr_TR
Ukrainian (Ukraine)	uk_UA
Vietnamese (Vietnam)	vi_VN

INDEX

A

applications services
enabling [56](#)

B

before installing the clients
verifying installation requirements [30](#)
verifying minimum system requirements [30](#)
verifying third-party software requirements [30](#)

C

clients
configuring for secure domains [32](#)
Content Management Service
configuring [28](#)
creating [28](#)
CreateContent (infacmd tdm) [55](#)
CreateService (infacmd tdm) [49](#)

D

Data Integration Service
configuring [25](#)
creating [25](#)
database preparations
repositories [18](#)
database requirements
installation requirements [15](#)
Model repository [19](#)
profiling warehouse [20](#)
DisableService (infacmd tdm) [57](#)
disk space requirements
installation requirements [11](#)
domain configuration repository
IBM DB2 database requirements [19](#)

E

EnableService (infacmd tdm) [56](#)
environment variables
configuring clients [32](#)
DISPLAY [13](#)
INFA_TRUSTSTORE [32](#)
INFA_TRUSTSTORE_PASSWORD [32](#)
installation [12](#)

G

graphical mode
installation requirements [13](#)

H

HTTPS
installation requirements [13](#)

I

IATEMPDIR
environment variables [12](#)
IBM DB2 database requirements
domain repository [19](#)
Model repository database [19](#)
profiling warehouse [21](#)
INFA_HOME
environment variables [12](#)
INFA_JDK_HOME
environment variables [12](#)
infacmd tdm
creating Test Data Manager Service Content in a domain [55](#)
creating Test Data Manager Service in a domain [49](#)
disabling the Test Data Manager Service [57](#)
enabling the Test Data Manager Service [56](#)
services, removing [58](#)
Informatica Administrator
logging in [62](#)
Informatica clients
installing in silent mode [30](#)
Informatica Developer
configuring local workspace directory [32](#)
installing languages [31](#)
local machines [32](#)
remote machines [32](#)
Informatica services
starting and stopping on UNIX [61](#)
installation
TDM
UNIX
console mode [36](#)
graphical mode [35](#)
Windows
graphical mode [35](#)
installation requirements
database requirements [15](#)
disk space [11](#)
environment variables [12](#)
keystore file [13](#)
minimum system requirements [11](#)
TDM repository database [15](#)
X Window Server [13](#)

ITDM
uninstallation [64](#)

J

JAVA_HOME
environment variables [12](#)
JRE_HOME
environment variables [12](#)

K

keystore file
installation requirements [13](#)

L

LANG
locale codes [68](#)
locale environment variables [12](#)
non-English locale [47](#)
languages
client tools [31](#)
installing on Windows [31](#)
LC_ALL
locale environment variables [12](#)
LD_PRELOAD
locale environment variables [12](#)
library path
environment variables [12](#)
license key
verifying [11](#)
logs
Test Data Manager Service [45](#)

M

Microsoft SQL Server database requirements
Model repository [20](#)
profiling warehouse [21](#)
TDM repository [17](#)
Model repository
database requirements [19](#)
IBM DB2 database requirements [19](#)
Microsoft SQL Server database requirements [20](#)
Oracle database requirements [20](#)
Model Repository Service
configuring [22](#)
creating [22](#)

O

Oracle database requirements
Model repository [20](#)
profiling warehouse [21](#)
TDM repository [16](#)

P

PATH
environment variables [12](#)

PowerCenter Client
installing languages [31](#)
profiling warehouse
database requirements [20](#)
IBM DB2 database requirements [21](#)
Microsoft SQL Server database requirements [21](#)
Oracle database requirements [21](#)

R

removeService (infacmd tdm)
description [58](#)
repositories
preparing databases [18](#)

S

secure domains
configuring clients [32](#)
silent mode
installing Informatica clients [30](#)
system requirements
minimum installation requirements [11](#)
TDM Server [11](#)

T

TDM repository
Microsoft SQL Server database requirements [17](#)
Oracle database requirements [16](#)
requirements [15](#)
TDM repository database
installation requirements [15](#)
TDM Server
system requirements [11](#)
TDM service
disabling [57](#)
Test Data Manager Service
assign a new license [45](#)
creating [41](#)
creating in a domain [49](#), [55](#)
removing using infacmd tdm [58](#)

U

uninstallation
process [64](#)
rules and guidelines [64](#)
UNIX
starting and stopping Informatica services [61](#)

X

X Window Server
installation requirements [13](#)