Novell Identity Manager

3.6

www.novell.com

NULL AND LOOPBACK SERVICES

June 30, 2008

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the International Trade Services (http://www.novell.com/company/policies/trade_services) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide provides information about the Identity Manager Loopback Service and Null Service drivers. Service drivers are used only for Metadirectory engine functions, not for connecting with external systems. They are automatically installed when you install Identity Manager.

The guide is organized as follows:

Audience

This guide is intended for administrators, consultants, and network engineers who require a high-level introduction to Identity Manager business solutions, technologies, and tools.

Documentation Updates

For the most recent version of this document, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36/index.html).

Additional Documentation

For documentation on other Identity Manager drivers, see the Identity Manager Drivers Web site (http://www.novell.com/documentation/idm36drivers/index.html).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Overview

1

Novell® Identity Manager includes two utility drivers, Null Service and Loopback Service, whose purpose is to implement custom behavior through policies established on the drivers' Subscriber and Publisher channels. Like other service drivers such as Entitlement and Workflow, the Null Service and Loopback Service drivers do not connect to external applications or systems.

The Null Services driver performs any tasks that are implemented through policies on the Subscriber channel. The Publisher channel is not used; the driver does not connect the Subscriber channel to the Publisher channel, but rather acts as a sink for most operations, simulates doing something with operations, and then returning success. Typical uses for the Null Service driver include the following:

- Adding the classes and attributes that you want to monitor for change in the Subscriber Filter as *Synchronize* for the class and *Notify* for the attribute.
- Adding Subscriber Event Transformation policies that react to specific object or attribute changes, and performing actions such as:
  - Making modifications back into the Identity Vault (using actions that manipulate source attributes and objects).
  - Sending e-mail.
  - Generating custom Audit Events.
  - Calling extension functions to communicate the change outside of Identity Manager.
- Adding a final Subscriber Event Transformation policy that vetoes all events.

The Null Service driver should be sufficient for the majority of the tasks you'll want to perform. However, if you need to process policies on both the Subscriber and Publisher channels, you can use the Loopback Service instead. The only difference between the two drivers is that the Loopback driver's Subscriber channel connects to the Publisher channel so that events can also be processed on the Publisher channel.

Installing and Activating the Drivers

2

The Loopback Services and Null Services drivers are automatically installed when you install the Metadirectory server. The drivers run on the platforms supported by Identity Manager and the Remote Loader service. The drivers do not require separate activation. When you activate Identity Manager, the drivers are also activated. For more information, see the *Identity Manager 3.6 Installation Guide*.

Creating a New Loopback Service Driver

3

A base configuration of the driver does not contain much information:

- No policies.
- An empty filter.
- Publisher heartbeat configuration option is available, but it is set to Disabled.
- No prompts for information when importing the driver.

The following steps provide information for using iManager to create a new Loopback Service driver. For information about using Designer to configure the driver, see "Importing into Designer" in the *Designer 3.0 for Identity Manager 3.6 Administration Guide*.

To configure the Loopback driver:

1. In iManager, click  to display the Identity Manager Administration page.
2. In the *Administration* list, select *Import Configurations*.
3. Select a driver set, then click *Next*.

   If you place this driver in a new driver set, you must specify a driver set name, context, and associated server.
4. Select how you want the driver configurations sorted:
   - All configurations
   - Identity Manager 3.5 configurations
   - Identity Manager 3.0 configurations
   - Configurations not associated with an IDM version
5. Select *Loopback Service Driver*, then click *Next*.
6. Specify a name for the driver, then click *Next*.
7. Define security equivalences for the driver and exclude administrative roles from replication, then click *Next*.
8. Read the summary, then click *Finish*.

3.0.1 Importing the Driver Configuration File

Importing the Loopback Service driver's configuration file creates the driver in the Identity Vault and adds the policies needed to make the driver work properly.

1. In iManager, click  to display the Identity Manager Administration page.
2. In the Administration list, click *New Driver* to launch the New Driver wizard.
3. Use the following table to supply the information required by the wizard

Prompt	Description
Where do you want to place the new driver?	You can add the driver to an existing driver set, or you can create a new driver set and add the driver to the new set. If you choose to create a new driver set, you'll be prompted to specify the name, context, and server for the driver set.
Import a configuration into this driver set	Use the default option, *Import a configuration from the server (.XML file)*. In the Show field, select *Identity Manager 3.6 configurations*. In the Configurations field, select the Generic Loopback file.
Driver name	Type a name for the driver. The name must be unique within the driver set.
Enter the authentication password	Skip this field.
Enter the driver password	Skip this field
Define Security Equivalences	The driver requires rights to objects within the Identity Vault and to the input and output directories on the server. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.
Exclude Administrative Roles	You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

4 On the Summary page, click the driver's link to display the list of mandatory parameters that must be configured for the driver to run properly.

5 Leave the Driver Set Overview page open and continue with the next section, Configuring the Driver.

3.0.2 Configuring the Driver

The following steps help you configure only the parameters that are required for the driver to run properly. For information about the parameters not mentioned in this section, see Appendix A, "Driver Properties," on page 35.

1 Click the Delimited Text driver's status icon (upper-right corner of the driver icon), then click *Edit Properites* to display the driver's property pages.

2 On the Identity Manager tab, make sure that *Driver Configuration* is selected, then fill in the following fields:

Field Delimiter: Specify the character that is used to delimit field values in the input files. It must be one character. The default is a comma.

If the values of any of the input fields contain this character, enclose the entire input field value in quotes to prevent it from being seen as a delimiter.

Changing this delimiter parameter to something other than a comma does not automatically change the delimiter character used in the output files when a Subscriber is used. To change the

delimiter character in the output files, edit the Output Transform style sheet. The delimiter character is assigned to a variable near the top of that style sheet.

Field Names: Specify a comma-separated list of attribute names that can be referred to in the Schema Mapping rule. In the input files, the fields of the records must correspond to the order and positioning of the names in this list.

Object Class Name: Specify the eDirectory class name that should be used when creating new objects to correspond to input files.

Output File Path: Specify the platform-specific path to the local directory where the driver will create output files. This directory must already exist (see Section 4.1, "Preparing Data Locations," on page 17).

Output File Extension: Specify the file extension to be used for output files. This should match the extension required by the application that will consume the files. If the output files are used as input files for another Delimited Text driver, the destination file extension must match the input file extension parameter of the second driver.

Input File Path: Specify the platform-specific path to the local directory where input files are placed. This directory must already exist (see Section 4.1, "Preparing Data Locations," on page 17).

Input File Extension: Specify the extension used to designate input files.

Rename File Extension: Specify the extension that an input file will be renamed with after the file has been processed. If you want the file deleted, leave this field blank.

3 (Conditional) If the driver is using the Remote Loader, fill in the following fields on the Driver Configuration tab:

Driver Module: Select *Connect to Remote Loader*.

Driver Object Password: The driver object password is used by the Remote Loader to authenticate itself to the Metadirectory server. This password must match the password for the driver object defined on the Remote Loader.

Remote Loader Connection Parameters: Specify the information required to connect to the Remote Loader. The parameter format is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, where `hostname` is the IP address of the Remote Loader server and `port` is the port the Remote Loader is listening on (the default is 8090). The `kmo` parameter is used only when an SSL connection exists between the Remote Loader and the Metadirectory engine; tt defines the Key Name of the Key Material Object containing the keys and certificate used for SSL.

Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`

Remote Loader Password: Specify the password required for the Metadirectory engine (or Remote Loader shim) to authenticate to the Remote Loader.

4 On the Identity Manager tab, click *Global Config Values* to display the Global Config Values page, then fill in the following fields:

Container for User Publication: Select the Identity Vault container where any new users created from delimited text file information will be placed.

5 Click *OK* to save your changes.

Configuring the Null Service Driver

4

A base configuration of the driver does not contain much information:

- No policies.
- An empty filter.
- Publisher heartbeat configuration option is available, but it is set to Disabled.
- No prompts for information when importing the driver.

The following steps provide information for using iManager to configure the driver. For information about using Designer to configure the driver, see "Importing into Designer" in the *Designer 3.0 for Identity Manager 3.6 Administration Guide*.

To configure the Null Services driver :

1. In iManager, click  to display the Identity Manager Administration page.
2. In the *Administration* list, select *Import Configurations*.
3. Select a driver set, then click *Next*.

   If you place this driver in a new driver set, you must specify a driver set name, context, and associated server.
4. Select how you want the driver configurations sorted:
   - All configurations
   - Identity Manager 3.5 configurations
   - Identity Manager 3.0 configurations
   - Configurations not associated with an IDM version
5. Select *Null Service Driver*, then click *Next*.
6. Specify a name for the driver, then click *Next*.
7. Define security equivalences for the driver and exclude administrative roles from replication, then click *Next*.
8. Read the summary, then click *Finish*.