Novell Identity Manager Fan-Out Driver

3.5.1

www.novell.com

September 28, 2007

PLATFORM SERVICES
ADMINISTRATION GUIDE
FOR OS/400*

Novell®

Legal Notices

Novell, Inc. and Omnibond Systems LLC. make no representations or warranties with respect to the contents or use of this documentation, and specifically disclaim any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. and Omnibond Systems LLC. reserve 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. and Omnibond Systems LLC. make no representations or warranties with respect to any software, and specifically disclaim any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. and Omnibond Systems LLC. reserve the right to make changes to any and all parts of the 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 the 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. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) 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 Woman Street, Suite 500
Lithium, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, 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.

The Solaris* standard IO library has kernel limitations that interfere with the operation of the Provisioning Manager. Therefore, components for Solaris use the AT&T* SFIO library. Use of this library requires the following notice:

The authors of this software are Glenn Fowler, David Born and Kim-Phone Do.

Contents

About This Guide

This guide provides you with the information you need to install, configure, administer, and troubleshoot Platform Services for IBM* OS400* as part of the Novell® Identity Manager Fan-Out driver.

This guide includes the following sections:

Audience

This guide is for system administrators and others who plan, install, configure, and use the Identity Manager Fan-Out driver. It assumes you are familiar with Identity Manager, Novell eDirectory™, and the administration of systems and platforms you connect to Identity Manager.

It also assumes you have read the *Platform Services Planning Guide and Reference* and have completed the planning phase it describes.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

For the most recent version of this guide, visit the Identity Manager 3.5.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm35drivers).

Additional Documentation

For additional documentation about Identity Manager drivers, see the Identity Manager 3.5.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm35drivers).

For documentation about Identity Manager, see the Identity Manager 3.5.1 Documentation Web site (http://www.novell.com/documentation/idm35).

For documentation about other related Novell products, such as eDirectory and iManager, see the Documentation Web site’s product index (http://www.novell.com/documentation).

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.

Installing Platform Services

1

The installation and setup of Novell® Identity Manager Fan-Out driver Platform Services includes tasks performed on the platform and the core driver. This section describes the installation tasks that are performed on the platform system. For details about platform configuration and administration tasks, see Chapter 2, “Configuring and Administering Platform Services,” on page 13.

The core driver tasks include defining UID/GID Sets, defining Platform Sets, and defining Platform objects. These tasks must be completed before you can use Platform Services. For more information about these tasks, see the *Core Driver Administration Guide*.

After the planning process has been completed, installation of Platform Services for OS/400 by experienced system programmers familiar with the local environment and the Identity Manager Fan-Out driver should take about half an hour.

Topics in this section include

1.1 About Platform Services for OS/400

Platform Services for OS/400 consists of two major components.

- **System Intercept:** The System Intercept provides password change information to the core driver. The System Intercept is implemented through the Password Validation Program Exit specified with the QPWDVLDPGM system value.
- **Platform Receiver:** The Platform Receiver requests provisioning events from Event Journal Services and runs a Receiver script to carry out the appropriate action for each event as it is received.

1.1.1 The System Intercept

The driver must be informed of changes made to passwords in order to support password replication. The System Intercept for OS/400 provides information to the core driver about password changes made on the platform. (Information about password changes to a user in eDirectory™ are received by the OS/400 platform as provisioning events and are processed by the Platform Receiver.)

The System Intercept must be configured to connect directly to core drivers using the `DIRECTTOAUTHENTICATION` statement in the platform configuration file. For details about the platform configuration file, see the *Platform Services Planning Guide and Reference*.

1.1.2 The Platform Receiver

The Platform Receiver processes provisioning events received from the Event Journal Services component of the core driver.

The Platform Receiver communicates with Event Journal Services using Secure Sockets Layer (SSL). Data is encoded using UTF-8, which is converted to EBCDIC.

Run the Platform Receiver on a schedule that is appropriate for your requirements. For details about Platform Receiver operation, see the *Platform Services Planning Guide and Reference*.

The Platform Receiver reads its configuration information from `ASAM/data/asamplat.conf`, the platform configuration file. For details about the platform configuration file, see the *Platform Services Planning Guide and Reference*.

The OS/400 Platform Receiver uses the Attribute Name Mapping file, `/usr/local/ASAM/data/attrmap.conf`, to convert attribute names obtained from Event Journal Services to the Profile and System Distribution Directory field names for use by the Receiver scripts. For more information about the Attribute Name Mapping file, see "The Attribute Name Mapping File" on page 14.

The OS/400 Platform Receiver logs messages to the standard joblog facility.

1.1.3 Receiver Scripts

Receiver scripts for OS/400 platforms are implemented as Control Language (CL) programs. The Platform Receiver runs the programs from the ASAM library.

Provisioning events are received as groupings of name-value pairs as shown in the following example:

```
enterpriseUserName  bob
```

The Platform Receiver calls a Receiver script whenever it is necessary to obtain information about users or groups on the platform and whenever it is appropriate to take an action for a user or group on the platform.

Processing Summary

1. When the Platform Receiver calls a Receiver script, it maps the name-value pairs and stores them in a user space. Procedures are provided for setting and retrieving these values.

   User names and group names are checked for validity before they are mapped. A utility Receiver script is called to perform the validity checking.
2. Receiver scripts are called as appropriate to determine group affiliations for user events and group membership for group events.
3. Receiver scripts are called to take the necessary actions.

For more information about Receiver scripts, see the *Platform Services Planning Guide and Reference* and the scripts themselves.

1.1.4 Authentication Services

Authentication Services for OS/400 does not redirect authentication requests to eDirectory, but instead replicates passwords between the OS/400 system and eDirectory.

When a password is changed on the OS/400 system, the System Intercept sends a change password notification to a core driver for processing.

When a password for a user associated with an OS/400 system is changed in eDirectory, a provisioning event is generated by the core driver and given to the Platform Receiver for processing. By default, the core driver converts passwords to lowercase before sending them to the Platform Receiver. For more information about password case, see the Maintain Password Case configuration parameter in the *Core Driver Administration Guide*.

Because password replication information travels in both directions, it is affected by the Include/Exclude lists of both Authentication Services and Identity Provisioning. It is important therefore, to configure both sets of Include/Exclude lists symmetrically.

1.2 Platform Services Installation Procedure

For detailed step-by-step instructions about installing Platform Services, see the *Platform Services Quick Start Guide for OS/400*.

1.3 Uninstalling Platform Services

To remove Platform Services from an OS/400 system:

1. Stop the Platform Receiver.

   For details, see "Starting and Stopping the Platform Receiver" on page 13.
2. Remove the Platform Receiver from any system startup, shutdown, and scheduling procedures as appropriate.
3. In the Web interface, remove the Platform object for the OS/400 system.
4. Remove ASAMPWD from the QPWDVLDPGM system value.
5. Remove the ASAM library from your library list.
6. Remove the ASAM library and `/usr/local/ASAM` directory created by Platform Services installation.

Configuring and Administering Platform Services

2

After you have installed Novell® Identity Manager Fan-Out driver Platform Services, use the information in this section for configuration and administration.

2.1 Platform Certificate Management

Connections between Platform Services and core drivers use Secure Sockets Layer (SSL). SSL connections are authenticated through the use of certificates.

The certificates used by the Identity Manager Fan-Out driver are minted by the Certificate Services component of the core driver. When you install and configure Platform Services, you obtain a certificate.

To obtain a new certificate for your platform, run the Platform Receiver with the MODE(*SECURE) command line parameter.

Platform certificates are stored in the `ASAM/data/platformservices/certs` directory. Ensure that access to the certs directory is limited to the appropriate users.

2.2 Administering Platform Services

The Platform Receiver obtains provisioning events from Event Journal Services and calls the appropriate Receiver script to process the given type of event. For more information about Receiver scripts, see “Receiver Scripts” on page 10.

The Platform Receiver must be running if you plan to use Identity Provisioning on the platform.

2.2.1 Starting and Stopping the Platform Receiver

Set up routine operation of the OS/400 Platform Receiver using Persistent Mode or Polling Mode, in a subsystem as an autostart entry. For information about choosing a mode of operation, see the *Platform Services Planning Guide and Reference*.

To start and stop the Platform Receiver, execute `GO ASAM` to load the ASAM menu, and select the desired option. The ASAM library must be in your library list.

To start the Platform Receiver at the command line, enter `ASAMRCVR`, specifying command line parameters as appropriate. The ASAM library must be in your library list.

2.2.2 Platform Receiver Command Line Parameters

Table 2-1 *Platform Receiver Command Line Parameters*

Option	Argument	Explanation
CONFIG	Configuration File Path	Specifies the platform configuration file to use. If you do not specify this option, the default is /usr/local/ASAM/data/asamplat.conf.
MODE	*POLL	The Platform Receiver uses Polling Mode.
	*PERSIST	The Platform Receiver uses Persistent Mode.
	*FULL	The Platform Receiver uses Full Sync Mode.
	*SCHED	The Platform Receiver uses Scheduled Mode.
	*SECURE	Obtain a security certificate for the Platform and end. This is needed only during the initial configuration process.
CHECK	*ON	The Platform Receiver uses Check Mode.

The MODE option determines the mode of operation for the Platform Receiver. If this option is not specified, the mode of operation specified by the `RUNMODE` statement in the platform configuration file is used. If there is no `RUNMODE` statement, the Platform Receiver uses Persistent Mode.

For details about the Platform Receiver modes of operation, see the *Platform Services Planning Guide and Reference*.

2.2.3 Maintaining Files Used by the Platform Receiver

Maintenance involves four types of files.

- “The Attribute Name Mapping File” on page 14
- “The Platform Configuration File” on page 15
- “Receiver Scripts” on page 15
- “Log Files” on page 15

The Attribute Name Mapping File

The OS/400 Platform Receiver uses the Attribute Name Mapping file to convert attribute names obtained from Event Journal Services to Profile and System Distribution Directory field names for use by the Receiver scripts. The attribute names used by Event Journal Services are the names that appear in the Identity Manager Subscriber filter.

The Attribute Name Mapping file is `/usr/local/ASAM/data/attrmap.conf`.

Each line of the file contains the name of an attribute received from Event Journal Services, a comma, and the name to which the attribute is to be mapped for use by Receiver scripts.

Any line in the file beginning with an octothorpe (#) is a comment. Blank lines are ignored.

For more information about provisioning attributes to your platform, see Appendix A, “OS/400 Provisioning Tips,” on page 19.

The Platform Configuration File

The Platform Receiver reads the platform configuration file to locate the core driver, to determine which users and groups are managed using provisioning events, and to find other configuration information. For details about the platform configuration file, see the *Platform Services Planning Guide and Reference*.

Receiver Scripts

Receiver scripts for OS/400 platforms are implemented as Control Language (CL) programs. The Platform Receiver runs the Receiver scripts from the ASAM library. The source code for the Receiver scripts is stored in the `SCRIPTS` file in the ASAM library. Several varieties of Receiver scripts are placed in subdirectories of `asam/bin/platformservices/platformreceiver/scripts` by the installation process.

Log Files

The OS/400 Platform Receiver writes messages to standard OS/400 joblogs. Use DSPJOBLOG or iSeries* Navigator to view these logs. Log messages are documented in the *Messages Reference*.

Troubleshooting Platform Services

3

Novell® Identity Manager Fan-Out driver components record messages to their Audit Log, Operational Log, and their host system log. Examining these should be foremost in your troubleshooting efforts.

The Audit and Operational logs of core driver components are maintained in their logs directory.

The OS/400 Platform Receiver writes log messages to the standard OS/400 joblog facilities.

By its very nature, the Fan-Out driver is highly dependent upon the proper operation of your network and eDirectory™. If you are having problems with the driver, ensure that the various driver components are able to communicate with one another and that eDirectory is functioning properly.

For information pertaining to Fan-Out driver performance issues, see the planning section in the *Core Driver Administration Guide*.

IMPORTANT: Make sure you upgrade the driver, including all of your platforms, when new versions or support packs become available.

3.1 Obtaining Debugging Output

Identity Manager Fan-Out driver components support the option to produce extensive debugging output. Although this output is intended primarily for use by Novell Technical Support, you might find it useful for your own troubleshooting efforts.

Because debugging mode adversely affects performance, it should not be used for routine operations.

To obtain debugging output for the Platform Receiver on OS/400:

1. Add a `DEBUGLOGFILE` statement or `DEBUGTOSTDOUT` statement to the platform configuration file.

   For information about the platform configuration file, see the *Platform Services Planning Guide and Reference*.
2. Specify the debugging command line parameter when you start the Platform Receiver.

   To obtain full debugging output, specify `DEBUG(*)` on the command line.

   To obtain debugging output limited to messages exchanged with core drivers, specify `DEBUG(dom)`.

3.2 Troubleshooting Identity Provisioning

Ensure that user and group names conform to the character set and length restrictions imposed by the platform operating system.

Identity Provisioning information for platforms that use password replication is not normally available unless password information is available. For example, if you have just installed and configured the Identity Manager Fan-Out driver for the first time, and you run the Platform Receiver in Full Sync Mode on a system whose Platform object specifies Permit Password Replication, no accounts are created there. You must install the password intercepts, and users must authenticate through the driver or change their passwords so that password replication information is available. Then that account information becomes available to the platform.

3.3 Troubleshooting Network Issues

Although the details of network troubleshooting are beyond the scope of this document and depend on a number of factors particular to your environment, the purpose of this section is to determine if the various Identity Manager Fan-Out driver components can communicate with one another.

To verify IP connections between driver platforms and core drivers using the ping command:

1. From a command prompt on z/OS*, OS/400, UNIX, or Windows*, enter `ping ipaddr` , where *ipaddr* is the IP address of the remote computer.
2. From a NetWare® console, enter `LOAD TPING ipaddr` , where *ipaddr* is the IP address of the remote computer.

If your installation uses router filters to prevent the use of ping, consult with those responsible for managing your network for information on how to verify connectivity.

You can use other NetWare utilities, such as MONITOR, CONFIG, INETCFG, and TCPCON to examine and change other aspects of server status that pertain to networking. Refer to your NetWare documentation for further details. The *Utilities Reference*, *Basic Protocol Configuration Guide*, and *Advanced Protocol Configuration and Management Guide* provide detailed information on using these and other NetWare utilities.

OS/400 Provisioning Tips

A

You can add additional attributes to your Novell® Identity Manager Fan-Out driver configuration for your own purposes.

A.1 Provisioning Attributes

Certain attributes are configured to be made available to platforms by default. You can add additional attributes to be provisioned to platforms if necessary. For a list of the attributes configured by default, see the *Core Driver Administration Guide.*

To configure additional attributes, you must add them to the Identity Manager Subscriber filter. For details about adding attributes to the Subscriber filter, see the *Novell Identity Manager Administration Guide*. The attribute names that you use in the Subscriber filter must be the eDirectory™ names. The attribute names presented to the Platform Receiver are the eDirectory names.

If you are using attributes on an OS/400 platform, you may need to map attribute names to their Profile and System Distribution Directory field names. This is done using the Attribute Name Mapping file. For more information about the Attribute Name Mapping file, see “The Attribute Name Mapping File” on page 14.

A.2 Synchronizing Password Expiration

To ensure that passwords expire on your OS/400 platform at the same time as they expire in eDirectory, you must make two additional attributes available to the platform.

Add the following two attribute names to the Subscriber filter:

Password Expiration Interval
Password Expiration Time