

Novell Identity Manager Fan- Out Driver

3.5

www.novell.com

March 19, 2007

QUICK START

Platform Services Quick Start Guide for AIX*

Before installing Identity Manager Fan-Out driver components, obtain the latest support pack and product updates, and review the Release Notes and Readme files. For the latest support information, see the [Novell Support Web site \(http://support.novell.com\)](http://support.novell.com).

REQUIRED KNOWLEDGE AND SKILLS

Successful installation of Platform Services for AIX requires administrative expertise with the Identity Manager Fan-Out driver and AIX. If you are new to the driver, you should first read and understand the information presented in the *Concepts and Facilities Guide*, the *Platform Services Planning Guide and Reference*, and the *Platform Services Administration Guide for Linux and UNIX*.

For Identity Manager Fan-Out driver documentation, see the [Identity Manager Driver Web site \(http://www.novell.com/documentation/dirxmldrivers\)](http://www.novell.com/documentation/dirxmldrivers).

PREREQUISITES

- 1 Ensure that your version of AIX is compatible with the Identity Manager Fan-Out driver.

- ♦ AIX 4.3.3 ML 9 or later with APAR IY37249
- ♦ AIX 5.1 with APAR IY37250
- ♦ AIX 5.2 or later with current maintenance.

- 2 Platform Services uses Secure Sockets Layer (SSL) for communications. SSL requires a source of entropy. AIX 5.2 and later includes a `/dev/random` device for entropy.

If your AIX version does not have a `/dev/random` device, you must install and configure an entropy daemon prior to installing Platform Services.

For your convenience, the Pseudo Random Number Generator Daemon PRNGD is included in the `/prngd` directory of the distribution.

Novell®

INSTALLING PLATFORM SERVICES FOR AIX

- 1 If you do not have an appropriately configured Platform Set object, use the Identity Manager Fan-Out driver Web interface to create a Platform Set object.

Associate users and groups with your Platform Set using the appropriate Search object configuration.

Platform Sets are established for platforms that share a common population of users and groups. Multiple types of platforms can reside in a single Platform Set, and individual users and groups can appear on multiple Platform Sets.

Whenever you modify Search objects, start a Trawl to populate the platforms.

- 2 Use the Web interface to create a Platform object for your platform in an appropriate Platform Set.

You must define all of the IP addresses for the platform so that mutually authenticated SSL can function properly.

- 3 Log in as root to the server where you are installing Platform Services.

- 4 Retrieve the Platform Services distribution package and place it in a temporary location on the target server.

- 5 Extract the distribution package to the temporary location.

This creates and populates an ASAM directory in the temporary location.

- 6 Run ASAM/setup/install and respond to the prompts.

This prepares the /usr/local/ASAM directory.

You can now remove all of the files from the temporary location.

- 7 Run /usr/local/ASAM/bin/PlatformServices/plat-config and respond to the prompts. You will be asked to choose one of these provisioning models for your platform:

- ◆ Local Provisioning, Redirected Authentication
- ◆ Local Provisioning, Local Authentication
- ◆ ASCAUTH LAM Module (Account Redirection)

For details about these provisioning models, see the *Platform Services Administration Guide For Linux And UNIX*. For Local Authentication and Account Redirection models, make sure you have your Universal Password policies configured to enable administrators to retrieve Universal Passwords.

- 8 Review the contents of the Platform Configuration file /usr/local/ASAM/data/asamplat.conf.

You must have at least one AUTHENTICATION statement and at least one PROVISIONING statement.

If your AIX version does not have a `/dev/random` device, you must include an `ENTROPY` statement to specify a source of entropy.

For an example `asamplat.conf` file, see `/usr/local/ASAM/data/sampleplat.conf`.

- 9 Review the file permissions of `/usr/local/ASAM/data` to ensure that they are appropriate for your installation.

Access should usually be restricted to the driver system itself, and to its administrators.

- 10 If you are using the Local Provisioning, Redirected Authentication provisioning model, edit `/etc/security/user` and change the default stanzas. The file `user.sample` in `ASAM/bin/PlatformServices` demonstrates the required changes. The required stanzas for the Identity Manager Fan-Out driver have the following entries: `AUTH1 = SYSTEM AUTH2 = NONE SYSTEM = DCE registry = DCE`

If you have AIX 5.3 or later and wish to use the PAM framework instead of the default AIX LAM framework, see the *Platform Services Administration Guide For Linux and UNIX* for details.

- 11 If you are not using the `ASCAUTH` LAM module for account redirection, set up the Receiver scripts.

The Platform Receiver responds to events by running corresponding Receiver scripts. The Platform Receiver runs Receiver scripts from `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts`. The base set of Receiver scripts is delivered in the `aix-passwd` subdirectory of `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts`. The `install` script offers to install the base scripts for you. If you accept, then the `plat-config` script copies all of the scripts in `aix-passwd` up one level to `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts`.

If you have developed your own set of custom scripts, copy your custom scripts to `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts`.

For information about developing your own custom scripts, see `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts/scriptwriters.README`.

- 12 If you are not using the `ASCAUTH` LAM module for account redirection, add the Platform Services Process (`asampsp`) and Platform Receiver (`asamrcvr`) operation into routine system startup, shutdown, and scheduling procedures as appropriate.

Optional startup and shutdown scripts are provided in the `ASAM/data/UnixStartupScripts` directory.

The first time a Platform Receiver is run for a new platform, it automatically receives provisioning events for all users and groups for the platform.

- 13 If you are using the `ASCAUTH` LAM module for account redirection, add the Platform Services Cache Daemon (`asamps`) into routine system startup and shutdown procedures as appropriate.

A startup/shutdown script for the Platform Services Cache Daemon is provided in the ASAM/data/UnixStartupScripts directory.

Edit /etc/security/user and change the default settings for SYSTEM and registry as follows:

```
SYSTEM = ASCAUTH
registry = ASCAUTH
```

Edit /usr/lib/security/methods.cfg and include a stanza for the ASCAUTH LAM module:

```
ASCAUTH:
program = /usr/lib/security/ASCAUTH
```

When you try to copy a newer version of the libascauth.a library file or the DCE file, you might get the error message `Cannot Open or Remove a File Containing a Running Program`. This occurs when the kernel or a user program has the library open. When this situation occurs, you can do one of the following to install the newer version.

- ◆ Remove /usr/lib/libascauth.a, then copy the newer version into /usr/lib.
- ◆ Remove /usr/lib/security/DCE, then copy the newer version into /usr/lib/security.
- ◆ Boot into single-user mode, then copy newer version into /usr/lib.

Legal Notice

Copyright © 2004 Omnibond Systems, LLC. All rights reserved. Licensed to Novell®, Inc. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher. Novell is a registered trademark of Novell, Inc. in the United States and other countries. All third-party products are the property of their respective owners. A trademark symbol (®, TM, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark.