

# Novell Identity Manager Fan- Out Driver

3.5.1

www.novell.com

September 28, 2007

QUICK START

## Platform Services Quick Start for z/OS\* RACF\*

This *Quick Start* provides basic steps to installing the Platform Services for z/OS RACF as part of the Novell Identity Manager Driver. It condenses information from other documentation that includes more details and additional tasks required to install, configure, and deploy the driver.

Before installing 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

This *Quick Start* assumes you are familiar with concepts and facilities of the Fan-Out driver, Novell eDirectory™, and the administration of z/OS and RACF.

For more information about installing the driver, as well as other suggested documentation, see the *Platform Services Planning Guide and Reference* and the *Platform Services Administration Guide for z/OS* at the [Identity Manager 3.5.1 Drivers Documentation Web site \(http://www.novell.com/documentation/idm35drivers\)](http://www.novell.com/documentation/idm35drivers).

### SOFTWARE REQUIREMENTS

Verify you are running Identity Manager 3.5.1, or later, as well as the required versions of eDirectory, iManager, z/OS and RACF. For more about these requirements, see the associated readme files on the [Identity Manager Documentation Web site \(http://www.novell.com/documentation/idm35drivers\)](http://www.novell.com/documentation/idm35drivers).

### INSTALLING PLATFORM SERVICES FOR Z/OS

- 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.

**Novell**®

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 FTP the z/OS installation files from the distribution media `mvspatformservices` directory to the target z/OS system.

You must specify the `BINARY` and `QUOTE SITE LRECL=80 RECFM=FB ftp` commands.

- 4 Use the TSO `RECEIVE` command to extract the samples library, load library, and scripts library to places appropriate for your site.

- 5 APF authorize the load library.

- 6 Add `ASCTEST` as an APF-authorized TSO command.

Add `ASCTEST` to the `AUTHCMD` section of your `PARMLIB(IKJTSOxx)` member, then use the TSO `PARMLIB` command to activate your changes.

- 7 Install the Platform Services Process. For the procedure, see [“Installing the Platform Services Process” on page 3](#).

You must run the Platform Services Process on each system that shares the security database. For initial testing, you can install the Platform Services Process to a single system.

- 8 Install and configure the RACF exits. For the procedure, see [“Installing the RACF Exits” on page 3](#).

You must install the RACF exits on each system that runs the z/OS Platform Services Process.

- 9 Install the Platform Receiver. For the procedure, see [“Installing the Platform Receiver” on page 4](#).

You must run only one instance of the Platform Receiver in your complex that shares the security database.

- 10 Integrate Platform Services into your routine operation.

- 10a Install Platform Services on all remaining systems that share the security database.

- 10b Add `ASCLIENT` and `PLATRCVR` operation into your routine system startup and shutdown scheduling procedures.

`ASCLIENT` must be active on every z/OS image in your complex. `PLATRCVR` must be active on only one system in the complex that shares the security database.

- 10c Change the Include/Exclude lists to match your production environment.

## INSTALLING THE PLATFORM SERVICES PROCESS

- 1 Copy the ASCLIENT member from the samples library to your started task procedure library, and customize it to use your own data set names.
- 2 Ensure that the ASCLIENT user ID is defined as a UNIX\* user.
- 3 Set up your ASCLIENT configuration member.

The ASCLIENT configuration member must belong to an LRECL=80 RECFM=FB PDS allocated to the ASCPARMS DD statement of the ASCLIENT JCL.

You can use member ASCPRMXX of the samples library as a model. For details about the configuration statements, see the *Platform Services Planning Guide and Reference*.

- 4 Assign a DES key for the platform.

Use the KEY statement of the configuration member to set the key for ASCLIENT.

Use the Web interface to set the identical key in the Platform object for the platform.

- 5 Assign ASCLIENT to a Service Class, such as SYSSTC, appropriate for its role in logon processing.
- 6 Start ASCLIENT.
- 7 Use ASCTEST to perform preliminary testing. For details, see the *Platform Services Administration Guide for z/OS*.
- 8 Establish Include/Exclude lists for initial testing of Authentication Services.

## INSTALLING THE RACF EXITS

- 1 Install ICHRIX01, the RACINIT pre-process exit.
  - ◆ If you do not have an existing ICHRIX01 exit, customize and run the job in the RACRIX0A member of the samples library.
  - ◆ If you already have an ICHRIX01 exit, customize and run the job in the RACRIX0B member of the samples library. RACRIX0B installs a router that calls the Platform Services RACINIT exit and your existing exit.
- 2 Install ICHPWX01, the RACF new password exit.
  - ◆ If you do not have an existing ICHPWX01 exit, customize and run the job in the RACPWX0A member of the samples library.
  - ◆ If you already have an ICHPWX01 exit, customize and run the job in the RACPWX0B member of the samples library. RACPWX0B installs a router that calls the Platform Services new password exit and your existing exit.
- 3 IPL with the CLPA option.
- 4 Update RACF options.

To avoid user confusion while phasing in your conversion to the driver, ensure that your RACF and eDirectory password rules are the same.

After your migration is complete, turn off the RACF password rules. Enter:

```
setropts password( nohistory interval(254) norevoke  
norules )
```

## INSTALLING THE PLATFORM RECEIVER

- 1 Customize and run job PAXRST0A from the samples library.

This job creates and populates the `ASAM` directory in HFS.

- 2 Copy the `PLATRCVR` member from the samples library to your started task procedure library, and customize it to use your own data set names.
- 3 Ensure that the `PLATRCVR` user ID is defined as a UNIX user.
- 4 Assign `PLATRCVR` the appropriate security system authority to manage users and groups.
- 5 Set up the platform configuration file for `PLATRCVR`.

Configuration statements must be placed in a sequential file allocated to ddname `ASAMCONF` in the `PLATRCVR` JCL.

You can use member `ASAMCONF` of the samples library as a model. For details about configuration statements, see the *Platform Services Planning Guide and Reference*.

- 6 Obtain a security certificate for the platform by customizing and running the `SETCERT` member of the script library, and responding to the prompts.
- 7 Establish Include/Exclude lists for initial testing of Identity Provisioning.
- 8 Customize and extend the Receiver scripts as appropriate for your management plan.

### Legal Notice

Copyright © 2004, 2007 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. For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html). 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.