Novell

Nsure™ Identity Manager Fan-Out Driver

3.1

October 27, 2004

QUICK START

www.novell.com

Platform Services Quick Start Guide for MVS* CA-Top Secret*

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).

This Quick Start summarizes the installation procedure for Platform Services on MVS, as a convenience for expert installers. For detailed information, see the *Platform Services Administration Guide for MVS.*

REQUIRED KNOWLEDGE AND SKILLS

Successful installation of Platform Services for MVS requires administrative expertise with the Identity Manager Fan-Out driver, and system programming skills with MVS. 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 MVS.*

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

- For information about MVS, see the IBM* z/OS* Internet Library Web Site (http://www.ibm.com/servers/eserver/zseries/zos/bkserv).

REQUIRED SOFTWARE ENVIRONMENT

- Any OS/390* or z/OS release supported by IBM

- IBM OS/390 eNetwork Communications Server V2R6 or later, or any 100% compatible TCP/IP product

- CA-Top Secret version 5.2 SP3 or later

Novell®

INSTALLING PLATFORM SERVICES FOR MVS

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   FTP the MVS installation files from the distribution media mvsplatformservices directory to the target MVS 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 libary, 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(IKJTSO*xx*) 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 CA-Top Secret exit. For the procedure, see "Installing the CA-Top Secret Exit" on page 3.

You must install the CA-Top Secret exit on each system that runs the MVS 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 MVS 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 Add a SECURITY TSS statement to the configuration member.

6 Assign ASCLIENT to a Service Class, such as SYSSTC, appropriate for its role in logon processing.

7 Start ASCLIENT.

8 Use ASCTEST to perform preliminary testing. For details, see the *Platform Services Administration Guide for MVS*.

9 Establish Include/Exclude lists for initial testing of Authentication Services.

INSTALLING THE CA-TOP SECRET EXIT

1 Review the section pertaining to the use of the CA-Top Secret Installation Exit TSSINSTX in the *CA-Top Secret User Guide*.

2 Modify TSSINSTX to use the driver PREINIT function.

    2a If you already use the PREINIT function, review the considerations for sites with a pre-existing PREINIT function in the *Platform Services Administration Guide for MVS*.

    2b Change the ##MATRIX byte for PREINIT to a value of #####YES.

    2c Insert the following instructions immediately after the PREINIT label:

```
LR    R1,R9           <AM> | Copy parmlist ptr to R1
LR    R11,R13         <AM> | Save TSS's savearea ptr
LA    R13,WORKAREA    <AM> | Use WORKAREA as savearea
L     R15,=V(ASCTSSPI) <AM> | Get addr of AM preinit exit
BALR  R14,R15         <AM> | Call it
LR    R13,R11         <AM> | Restore TSS's savearea ptr
B     EXIT            <AM> | Exit with exit's returncode
```

3 Place the modified TSSINSTX exit module in your TSS product library.

    3a Customize and run the job in the ASMINSTX member of the samples library.

    3b If your TSS product library is in the linklist, refresh LLA with the following operator command:
    F LLA,REFRESH

4 Activate the modified TSSINSTX exit.

    4a If TSSINSTX is already in use, issue the following operator command:
    F TSS,EXIT(OFF)

    4b Issue the following operator command:
    F TSS,EXIT(ON)

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.