Novell Nsure Identity Manager Driver for Linux and UNIX 2.0.1

September 29, 2004

Overview

The Novell® Nsure™ Identity Manager driver for Linux* and UNIX* is a solution to synchronize user data between Novell eDirectory 8.7.1 and later, and UNIX data stores that contain information in Files, NIS(YP), and NIS+ (NIS Plus).

In mixed networks, Novell eDirectory communicates with a variety of data stores spread across complex and heterogeneous computer systems in order to maintain network-wide information. On UNIX systems, this information is maintained in three different types of data stores: Files, NIS, and NIS+.

The Nsure Identity Manager driver for Linux and UNIX is used to synchronize information between these data stores and eDirectory. It uses DirXML 2.0 to communicate with eDirectory.

In this document, the term NIS is used to refer to Files, NIS, and NIS+.

1.0 Installing the Nsure Identity Manager Driver for Linux and UNIX

1.1 Before You Start

Before you install and configure the driver, keep in mind the following constraints:

- The driver can be run only on the application platform; that is, the machine where the Files, NIS, or NIS+ databases exist. If Novell® eDirectory™ and the DirXML Engine 2.0 are not installed on the application platform, you must use the Remote Loader to run the driver. For more information, refer the Configuring the Remote Loader section of the Nsure Identity Manager driver for Linux and UNIX Implementation Guide.

  NOTE: Nsure Identity Manager driver for Linux and UNIX needs to be installed on the Remote Loader platform.

- The driver application shim utility tries to locate the dependent utilities at the paths /usr/bin/, /bin/, /usr/sbin/, /usr/local/bin/, and /usr/lib/yp/.

  - Ensure that the awk, make, and makedbm utilities are available at any one of the paths mentioned above.

  - On Solaris, nawk utility must be available in any one of the paths mentioned above.

  - On HP-UX, nawk utility must be available, if not, create a soft link to "gawk" as "nawk" at any of the paths mentioned above.

- NIS or NIS+ should be configured before running drivers on the application platform.

- If the application platform hosts either NIS or NIS+, you must run the driver on the NIS(YP) and NIS+ master servers only.

- The makedbm utility should be available on the application platform.

  This is required for the Files and NIS(YP) drivers only. This utility is available when you install the ypserv package.

- For remote installation of NIS 2.0 PAM module, SSH must be set up between the source machine and the target machine.

1.2 Supported Platforms

- Solaris Sparc 2.7 or 2.8

- Linux Red Hat AS 2.1

- SuSE Linux 8.1

- IBM AIX 5.2

- HP-UX 11i

1.3 System Requirements

- Novell eDirectory 8.7.1

- Novell DirXML 2.0

- iManager 2.0.1

- eDirectory Administration Utilities (for extending the schema). For more information, refer to the Novell eDirectory Administration Guide at Novell eDirectory Administration Guide (http://www.novell.com/documentation/lg/edir87/index.html)

- For remote installation of NIS 2.0 PAM module, SSH must be set up between the source machine and target machine. For information, see the Nsure Identity Manager driver for Linux and UNIX Implementation Guide at http://www.novell.com/documentation.

2.0 Installation

To install the Nsure Identity Manager driver for Linux and UNIX:

1 Log in with the Root account on the machine where you want to install the Nsure Identity Manager driver for Linux and UNIX.

2 Change the directory to DirXML-NIS-Driver/*platform*/Setup.

  Replace *platform* with the platform for which you extracted the install package.

3 Execute the following command:

```
./nis-drv-install
```

4 Specify the choice of the desired language to read the License agreement.

5 Press Enter to read the License agreement.

6 Enter y to accept the License agreement.

  The following package is now installed on your machine.

  novell-DXMLnis on all platforms except Solaris. On Solaris, DXMLnis is installed.

3.0 Post-Installation

Before executing the nis-drv-config script, ensure that the Require TLS for Simple Binds with Password option is disabled in eDirectory version 8.7.x. For more information, refer to the Novell eDirectory 8.7 Administration Guide at http://www.novell.com/documentation/lg/edir87/index.html.

3.1 Extending the Schema

To run the script, use the following command:

```
nis-drv-config [-h hostname] [-D adminContext] [-w adminPassword]
```

This utility invokes the ldapsearch/ldapmodify tools in the current PATH. Please check the usage of the LDAP tools in the current PATH to specify any additional parameters required for the appropriate LDAP tools.

If you are using native LDAP tools on a Linux machine, extend the schema by using:

```
nis-drv-config [-h hostname] [-D adminContext] [-w adminPassword] [-x]
```

The adminContext must be specified in the LDAP format cn=admin,o=context.

3.2 Installing and Configuring PAM

The PAM module for NIS 2.0 is used to synchronize the UNIX user passwords with the universal password in eDirectory.

If PAM is not installed, the UNIX user password will not synchronize with universal password. However, the unidirection password set from eDirectory to UNIX will still function.

To run the script, use the following command:

```
nis-drv-config -pam
```

This will install the PAM module for NIS 2.0 and create appropriate entries in the PAM configuration file. Also, there is an option to install the PAM module on a remote machine, which requires SSH to be configured between the source and target machines.

4.0 Activating the Driver

DirXML and DirXML drivers must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can choose to activate DirXML products to a fully licensed state.

To activate your driver, you should:

- Purchase DirXML licenses
- Generate a Product Activation Request
- Submit the Product Activation Request
- Install the Product Activation Credential received from Novell

For more information about completing these tasks, refer to DirXML Documentation Web site (http://www.novell.com/documentation/beta/dirxml20/index.html)

5.0 Important Notes

NIS+

- All existing entries are overwritten in NIS+ when you run the nispopulate command. Doing so will cause the entries added by the driver's Subscriber channel to be lost. Therefore, We strongly recommend that you use the nistbladm command for any updates to NIS+.

- When modifying indexed attributes such as the name and GID for groups, and the name and UID for users, you must use the nistbladm command. Using the nisaddent or nispopulate commands to modify these indexed attributes results in the deletion of the entry in eDirectory, because of the order in which these events are stored in the NIS+ log.

6.0 Known Issues

- On AIX, PAM module for NIS 2.0 is not supported. Hence, PAM need not be installed on AIX machines during post-installation. Password synchronization from UNIX to eDirectory will not work if PAM module is not available. Since password set is supported on AIX, you can use iManager to change/set the user password in eDirectory so that the UNIX password can get synchronized.

- Removal of home directory from UNIX during a delete for user operation in eDirectory is not supported.

- On AIX, When a user is added in eDirectory with an associated group, the group information does not get updated with the user name.

- After installing and configuring PAM, verify that the PAM configuration file contains the correct entries. For more information, see the Nsure Identity Manager driver for Linux and UNIX Implementation Guide at http://www.novell.com/documentation.

- On AIX, the Authpassword attribute does not synchronize with user password.

- In NIS(YP), the default files will not be present during the creation of home directory.

- Password synchronization is not supported for groups. The group password will be reset if a group is modified in the eDirectory.

- You cannot specify the asterisk character (*) in the gecos field. If you do so, the character will remove the existing value.

- Renaming a user or group in the NIS database on the Publisher channel is not supported for Files and NIS(YP). Doing so will delete the existing user or group and create a new user or group in eDirectory.

- Users or Groups added to eDirectory using the ICE Forward Referencing feature will not be synchronized by the driver. You can use Migrate from eDirectory in iManager to synchronize such users or groups.

- On Linux, if a NIS(YP) driver is configured it might retry synchronizing some events on the Subscriber channel for a long time. This issue does not occur if you are using ypserv version 1.x.

  Ensure that you upgrade the ypserv version to 2.6.1 or higher if you are using ypserv version 2.x.

  Execute the following command to check the ypserv version:

  ```
  rpm -qa | grep ypserv
  ```

For more information, refer to TID NOVL83989 at http://support.novell.com

- ◆ During bulk migration of users and groups on Solaris with eDirectory 8.7.3, eDirectory might dump core. The fix for this issue will be available with eDirectory 8.7.3 FP1.

7.0 Legal Information

7.1 Disclaimer, Patents, Export Notice, and Copyright

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.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Patents pending.

7.2 Novell Trademarks

Novell, DirXML, and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

eDirectory is a trademark of Novell, Inc.

7.3 Third-Party Trademarks

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