Novell Identity Manager Roles Based Provisioning Module 3.6 Readme

January 18, 2008

Novell®

This document contains the known issues for the Identity Manager Roles Based Provisioning Module, Version 3.6. Please see the Identity Manager 3.5.1 Readme (http://www.novell.com/documentation/idm35/) for issues that might affect the User Application, but that do not relate to the Role subsystem. See Section 8, "Issues Fixed in IDM 3.6," on page 7 for a list of the IDM 3.5.1 issues that were fixed in the Roles Based Provisioning Module version 3.6.

The documentation resources are refreshed regularly. Corrections and enhancements are made as needed. Please check Novell Identity Manager 3.6 Product Documentation Web site (http://www.novell.com/documentation/idmrbpm36/index.html) for updates.

1 Documentation

The following sections list issues related to the documentation.

1.1 Identity Manager Roles Based Provisioning Module 3.6 User Application: Installation Guide

- "Error in Section 1.3 System Requirements" on page 1
- "Error in Section 2.6, Security Prerequisites" on page 2
- "Update for Section 2.7.1, Extending the eDirectory Schema for Roles Based Provisioning Module Version 3.6" on page 2
- "Error in Section 2.8.3, Copying the Role Service Driver Configuration File" on page 2
- "Error in Section 2.8.4, Copying the User Application Driver Configuration File" on page 2

1.1.1 Error in Section 1.3 System Requirements

Table 1-1, System Requirements incorrectly lists Metadirectory 3.5 as a supported system component. You must use Metadirectory 3.5.1. You cannot use Metadirectory 3.5.

1.1.2 Error in Section 2.6, Security Prerequisites

Section 2.6, "Security Prerequisites" lists the feature Simultaneous Logout. It is a feature, not a prerequisite.

1.1.3 Update for Section 2.7.1, Extending the eDirectory Schema for Roles Based Provisioning Module Version 3.6

If you are on NetWare, you must rename the `nrf-extensions.sch` file before using the nwconfig utility. The nwconfig utility only supports 8.3 file names so it cannot use the `nrf-extensions.sch` file with the default name. Rename `nrf-extensions.sch` to a supported format, such as `nrfext.sch`.

1.1.4 Error in Section 2.8.3, Copying the Role Service Driver Configuration File

The path specified for NetWare is incorrect. The correct path is:

`SYS:\tomcat\5.0\webapps\nps\Dirxml.Drivers`

1.1.5 Error in Section 2.8.4, Copying the User Application Driver Configuration File

The path specified for NetWare is incorrect. The correct path is:

`SYS:\tomcat\5.0\webapps\nps\Dirxml.Drivers`

2 User Application: Roles

The following sections describe known issues for the Roles tab of the User Application.

2.1 Search Issues

2.1.1 Roles Search Dialog Always Wildcards Entries by Adding * to the End of the Search

The Object Selector that you use to find or filter a search always adds a wildcard (*) to the end of the search criteria.

2.1.2 Searching and Case Sensitivity

Role search is case-sensitive in the Object Selector.

Role name filtering is NOT case-sensitive in the following pages:

- My Roles
- Role Assignments
- View Request Status
- Browse Role Catalog
- Manage Role Relationships

2.2 Supported Characters for Role Name and SoD Name

The Role Name and the SoD Constraint Name can contain only the following characters:

- Alphanumeric characters.
- A - (dash) or _ (underscore) within the string (but not at the beginning or end of the string).

The following characters can NOT be used and will cause errors:

! # % & , " ' ; \ / +

The Display Name is limited to this same character set when you first create it. After you save the Role or SoD constraint the first time, you can then modify the Display Name to use other characters.

If the Role Name includes unsupported characters, users will encounter an error if they try to perform any actions on that role. The error is:

```
796 WARN [Parameters] Parameters: Character decoding failed. Parameter
skipped.
```

2.3 Assigning an Organizational Unit (OU) to a Role But the Role is Not Applied

If you assign a role to an OU, but none of the users in that OU are provisioned for that role, you must check the Role Service driver error log for an error. The User Application user interface does not indicate this type of error, and it appears that the role was provisioned in the View Requests page.

2.4 Viewing Role Assignments

When viewing role assignments from My Roles or Role Assignments (by User), you will not see all of the containers or groups for the role. You will see just one. For example, if the role TestRole is in two containers, the user interface displays the role in only one container.

2.5 SoD Conflicts Are Reported at Request Time and Not at Effective Date

The User Application checks for SoD constraint exceptions when a user requests a role assignment, but they are not checked when a role assignment takes effect.This means that a role might be in violation, but no notice or approval is performed. Suppose that the nurse and pharmacist roles are in conflict. You might assign UserA to the nurse role with an effective date two weeks in the future. In the meantime, you assign UserA to the pharmacist role with an effective date of immediate. You will not be notified of this conflict because the exception is checked at request time, and the user is not in a conflicting role at request time.

2.6 Role Assignments Page Does Not Show Items With a Future Start Date

The Role Assignments page does not show assignments that have a status of "Pending Activation". To see assignments that will be activated in the future, go to the View Request Status page.

2.7 Roles User Interface Sometimes Shows Inconsistent Effective Dates

If the current date for the User Application server is different than the current date for the eDirectory server, the user may see different dates on different pages within the Roles tab. For example, suppose the User Application server's current date is 05Dec, but the eDirectory server's current date is 26Dec. In this case, on the My Roles and Role Assignments pages, the effective dates display the eDirectory server's date. However, in the View Request Status page, the effective date and request date display the User Application server's date.

If the effective date is not specified, the Role Assignments page uses the eDirectory server system time, but in the View Request Status page, the effective date is taken from the User Application server system time. This discrepancy may not exist in a production environment because time synchronization techniques may be used to correct these problems.

Furthermore, the assignment and assignment request data are maintained separately in different objects. One object represents the date provided at the time the user made the request, whereas the other object represents the state of the actual role assignment. If the user does not specify an effective date (meaning that the role assignment should go into effect immediately), the effective date shown on the View Request Status page is the date that the request was submitted to the Application Server. This is not the same as the date shown on the Role Assignment screen, which is based on the when the role assignment was actually processed.

2.8 Role Manager Rights to Browse Role Containers

In the Manage Roles page, the Role Manager is able to see all Role Containers, but they can create new roles and modify existing roles for which they have browse rights.

3 User Application: Role Reporting

The following sections describe known issues with role reports.

3.1 Adobe Reader Plug-in Required to View Reports

To view reports, your browser must have the Adobe Reader plug-in installed. If you do not have the plug-in installed, the reports do not display.

3.2 Mixed Language Support

If a PDF report contains content generated in Chinese, Japanese or Russian, the user's preferred locale must be set to the appropriate language. If the PDF contains a mix of these languages, the user's preferred locale must be set to one of them. Otherwise, the user will not be able to view the report correctly.

3.3 SoD Constraint Reports causing NullPointerExceptions

There is a known Sun JDK problem relating to NullPointerExceptions observed when running multiple reports simultaneously. If you encounter the NullPointerException you may need to rerun the report. See Sun's bug report (http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6367148) for more information.

3.4 Tips for Avoiding OutOfMemory Errors When Running Reports Concurrently

Generating reports is a memory-intensive operation. Here is some guidance to ensure best performance during report generation:

- Configure a large Java heap size for the application server.
- Avoid generating a large number of reports at the same time.
- Whenever possible, generate reports at a time when the server is idle to minimize impact on active users.
- In a cluster, dedicate an application server in the cluster for report generation to minimize impact on active users.

4 Localization

The following sections describe known localization issues.

4.1 SessionWarning Text and Simplified Chinese

The SessionWarning text does not display for Simplified Chinese. After the timeout, the user is redirected to the session timeout page and can re-login successfully. However, any page the user goes to displays a JavaScript error onload of the page.

4.2 Problems with Role and SoD Constraint Name and Description in Chinese

If you run the User Application using one of the Chinese locales, you cannot use Designer to define localized Role or SoD constraint names or descriptions. They will display correctly in Designer, but will not display correctly once they are deployed. To work around this problem, you can localize the names and descriptions in the User Application Roles tab.

The System Roles that ship with the product will not display correctly by default on Chinese systems. They will display in English. Use the User Application Roles tab to update the names and descriptions to the correct translation.

5 iManager

The following sections list known issues for iManager.

5.1 Unable to Examine Roles Based Provisioning Request Definitions in iManager

You cannot use iManager to work with the Roles Based provisioning request definitions. If you try to open one, you see the following error.

```
The ''XmlData'' attribute on the Provisioning Request cannot be read or does
not contain valid XML data. This Provisioning Request cannot be configured or
used to create other Provisioning Requests.
```

5.2 Using the Driver Inspector on the Role Service Driver Crashes eDirectory

Do not use iManager's Driver Inspector (available through the Identity Manager link in the left navigation), or you might crash your eDirectory server. If you do use it, you see the message Reading associations followed by an error dialog with a message like the following:

```
The following SPI error has occurred...(-621)...
```

When you restart the eDirectory server, it displays a message that eDirectory was improperly shutdown.

6 Integration

The following sections describe known integration issues.

6.1 User Application Requires Version 1.0.809.102 of the MS SQL Server 2005 JDBC Driver

The User Application requires version 1.0.809.102 of the Microsoft SQL Server 2005 JDBC Driver. Note that only the Sun Solaris, Red Hat Linux, and Windows 2000 or later operating systems are officially supported with this JDBC driver.

6.2 Login.jsf and FormFill Policy Differences on JBoss and WebSphere

The JBoss and WebSphere containers handle JSF pages differently. This means that the Access Manager FormFill policy must use Form ID rather than Form Name.

6.3 NMAS Errors Prevent Role Service Driver from Starting

If you are using Novell Security Services 2.0.5 (which includes NMAS 3.2.0.2), and you have the environment variable `NDSD_TRY_NMASLOGIN_FIRST=true`, you will not be able to start the Role Service driver. You will get the following NMAS error when you try to start it:

```
locallogin -799 ERR_CANNOT_GO_REMOTE
```

To work around this problem, set the `NDSD_TRY_NMASLOGIN_FIRST` environment variable to false, or get the necessary NMAS patch.

On NetWare, the `NDSD_TRY_NMASLOGIN_FIRST` environment variable is set to true by default. For other platforms, it is set to false by default.

7 Performance

To improve performance in environments with a large number of roles with high user concurrency, consider creating a value-based index in eDirectory for the nrfRoles attribute.

8 Issues Fixed in IDM 3.6

This section includes the list of issues described in the IDM 3.5.1 User Application Readme that were fixed in the IDM 3.6 Roles Based Provisioning Module.

◆ 4.4 GUI install fails on Solaris 9 and 10 when using eDirectory 8.8.1.

◆ 4.5 Configupdate script fails after adding files to the WAR.

◆ 4.8 User Application and Access Manager simultaneous logout

◆ 6.9 Setting SSL configuration parameters

◆ 6.12 User Application driver requires activation

◆ 6.15 Sensitive data in a user session is not encrypted

◆ 6.18 A workflow fails to trigger from an eDirectory event

◆ 6.23 Service config.xml files contain outdated version numbers

- 6.25 Starting workflows with the SOAP Web Service sometimes causes errors.
- 6.30 Installing to a cluster does not prompt for the workflow engine ID.

9 Documentation Conventions

In this 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.

10 Legal Notices

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.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of 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.

Copyright © 2008 Novell, Inc. All rights reserved. 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, 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.

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

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