AUTHORIZED DOCUMENTATION

Business Solutions Reference Guide

Novell®
Identity Manager Resource Kit

1.2

August 29, 2008

www.novell.com

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.

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.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide explains the different business solutions that the Resource Kit contains. It explains what the solutions are and how to implement them.

Audience

This guide is intended for Identity Manager administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Business Solution Guide*, visit the Novell Compliance Management Platform Documentation Web site (http://www.novell.com/documentation/ncmp10/).

Additional Documentation

For documentation on Identity Manager, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36/index.html).

Documentation Conventions

In Novell 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.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

Password Expiration Notification Solution

1

This section contains the technical information on how the Password Expiration Notification solution works. It explains the business problem that occurs, the solution, and the technical aspects of the solution.

1.1 The Business Problem

The IT department wants to use e-mail to notify all employees whose passwords are about to expire. This reduces the number of help desk calls when users are locked out. The employees browse to a specified Web page or use their client application to change their passwords.

If it is not automated, the process can take a lot of time for the user and for the IT person. It is time wasted that could be spend on more productive tasks.

1.2 The Resource Kit Solution

The solution is to automatically notify users when their passwords are about to expire. By automating the process, the IT department is free to do other tasks, and users are aware that they should change their passwords before they expire.

1.3 The Technical Explanation

The Resource Kit accomplishes password expiration notification by using a job and an e-mail template.

1.3.1 Password Expiration Notification Job

The purpose of an Identity Manager job is to complete a task that occurs many times. For more information about jobs, see the *Identity Manager 3.6 Jobs Guide*. In this case, the default job runs daily at 12:01 a.m. The job searches all user objects and checks the attribute that stores the password expiration date. When the password is about to expire, the job uses the e-mail template to create a message that informations the user that the password is going to expire.

A job consists of a JAR file (`pwdexpjob.jar`) and an XML file (`PwdExpNotifyJobDef.xml`).

The JAR file is placed in the `/opt/novell/eDirectory/lib/dirxml/classes` directory during the installation of Identity Manager. Every time eDirectory™ starts, the JAR file is loaded. The JAR file is executed when all of the criteria set in the job parameters are met. For the Resource Kit, that means every night at 12:01 a.m. the job performs a search of the Identity Vault to find all users whose passwords are scheduled to expire in 30 days, 15 days, 5 days, and 1 day. The job sends an e-mail to each user who meets the criteria, informing them that the password is about to expire.

For configuration information, see "Configuring the Password Expiration Notification Job" in the *Identity Manager 3.6 Jobs Guide*.

1.3.2 Password Expiration Notification E-Mail Template

The job calls the Password Expiration Notification e-mail template to create the e-mail that the users receive to notify them that their passwords are going to expire. You can modify the text in the e-mail to customize the e-mail message for each deployment of the Resource Kit.

You select the Password Expiration Notification e-mail template during the configuration of the Password Expiration Notification job.

Single Sign-On Solution Using Credential Provision Policies

2

This section contains the technical information of how the Credential Provisioning policies work to enable Single Sign-On. It explains the business problem that occurs, the solution, and the technical aspects of the solution.

2.1 The Business Problem

For most users, it is easier to have one password for multiple applications that require a username and password. The users don’t forget the passwords as often if they only have one password to remember.

Security is increased for the company by requiring a more complex password, and if users only need to remember one password, they are less likely to write that password on a piece of paper and store it by the computer.

If a user has multiple passwords, the calls to the help desk increase because the users forget their passwords more often. The help desk must spend more time resetting users’ passwords.

2.2 The Resource Kit Solution

The Resource Kit has implemented the Credential Provisioning policies to help manage passwords, instead of relying only on Password Synchronization. Credential Provisioning policies help overcome the following common issues:

- Users don’t know or forget the passwords for each separate application they log into.
- Users remember only the main password that is synchronized to the connected systems.
- Secure passwords that are randomly generated for the connected application are randomly generated are much more secure than passwords created by users.

The Resource Kit contains a solution that:

- Allows users to access their workstations and connected enterprise applications with a single login process.
- Uses only the primary login directory to prompt users to change their passwords.
- Never prompts users to change their password in a connected application like e-mail or HR.
- Requires the user’s password to match the primary login directory’s password policy.

2.3 The Technical Explanation

The solution is implemented by enabling Credential Provisioning policies that create and enable the user's Single Sign-On accounts. A user can have one or more accounts, depending upon how many drivers and applications you have configured to use Single Sign-On.

The Resource Kit contains the policies and resource objects required for the solution to work. The additional products required for this solution must be installed and configured for the solution to work.

1. Install and configure SecureLogin. For more information, see the *Novell SecureLogin 6.1 Installation Guide* (http://www.novell.com/documentation/securelogin61/nsl61_installation_guide/data/bookinfo.html).
2. (Optional) Install and configure Novell® SecretStore®. For more information, see the *Novell SecretStore 3.4 Installation Guide* (http://www.novell.com/documentation/secretstore34/nssadm/data/admu1ef.html).
3. Choose one of the following methods to enable the Credential Provisioning policies:
   - To enable policies globally, continue with Step 4.
   - To enable the policies for each connected system, skip to Step 5.
4. Enable the Credential Provisioning policies globally by specifying the Credential Provisioning GCV on the driver set:
   - **4a** In the Designer project, right-click the driver set.
   - **4b** Select *GCVs*, then use the information in Table 2-1 to configure the settings under *Credential Provisioning*.
   - **4c** Click *OK* to save the changes.
5. Enable the Credential Provisioning policies for each connected system:
   - **5a** In the Designer project, right-click the connected system driver (Active Directory* or Lotus Notes* icon or the driver line in the Modeler), then click *Properties*.
   - **5b** Select *GCVs*, then use the information in Table 2-1 to configure the settings under *Credential Provisioning*.
   - **5c** Click *OK* to save the changes.
   - **5d** Repeat Step 5a through Step 5c for each application driver.
6. (Conditional) If the SecretStore or SecureLogin servers are on a separate machine from the Resource Kit image, you must change the server information on the repository objects:
   - **6a** In Designer, click the *Outline* tab, then expand the library object.
   - **6b** Right-click the lib-CredProv-NSSRepository object, then select *Edit*.
   - **6c** Change the server-specific information, then click *OK* to save the changes.
   - **6d** Right-click the lib-CredProv-NSLRepository object, then select *Edit*.
   - **6e** Change the server-specific information, then click *OK* to save the changes.
7. Click *Save* in the toolbar to save the Designer project.
8. Deploy the changed project to the Identity Vault. For more information, see "Deploying a Project to an Identity Vault" in the *Designer 3.0 for Identity Manager 3.6 Administration Guide*.

Table 2-1 *Credential Provisioning GCV options*

Option	Value
Enable Credential Provisioning Policies	Set this option to true. By default it is set to false.
On user creation	If this is set to true, credentials are provisioned when a user is created. By default, it is set to true.
On user enable/disable	If this is set to true, credentials are provisioned when user accounts are enabled and credentials are de-provisioned from user accounts that are disabled. To enhance security new credentials are provisioned every time an enable/disable cycle completes.
On password changes	If this is set to true, the credentials are re-provisioned on every password change.
Application Credential ID	Specify the ID that SecureLogin uses to identify the provisioned login. This login is linked with an application on the SecureLogin client.
Application User ID Attribute	Specify the attribute name used to retrieve the application userid. This is an attribute in the application's namespace.
Provision to Novell SecretStore	Set this to true if the SecretStore is used by the credential provisioning policies. Set it to false if a SecretStore is not used by the credential provisioning policies. By default, it is set to false.
Provision to Novell SecretStore > SecretStore Shared Secret Type	If the credential is provisioned to SecretStore, select the SecretStore Shared Secret Type to be used. It is either Credential Set or Application Set.
Provision to Novell SecretStore > Use Enhanced Protection Password	Select true if the SecretStore Enhanced Protection Password is to be used. If true is selected, then the named password secretstore-enhanced-protection-password must be properly set. The named password is stored on the driver object. By default, it this is set to false.
Provision to Novell SecureLogin Repository	Select true if a SecureLogin repository is used by the Credential Provisioning policies. Select false if a SecureLogin repository is not to be used by the Credential Provisioning policies. By default, it is set to true.
Provision to Novell SecureLogin Repository > Set Novell SecureLogin Passphrase	Select true to set a passphrase question and answer for SecureLogin. Select false if a passphrase question and answer should not be set by the Credential Provisioning policies.
Provision to Novell SecureLogin Repository > SecureLogin Passphrase Question	Specify the passphrase question that is set for each user.
Provision to Novell SecureLogin Repository > SecureLogin Passphrase Answer Value Attribute	Specify the attribute name that contains the value of the passphrase answer.

Business Logic Solution

3

The Resource Kit contains a business logic abstraction layer you can use to simplify the process of deploying an Identity Manager solution.

3.1 The Business Problem

Each company has its own business requirements and policies that must be followed. For example, a new employee must be granted access to applications, resources, and physical buildings. If the employee is a salesperson, he or she has a different set of requirements than a marketing person.

Developing a set of policies that work with Identity Manager takes time. If you need to deploy a new Identity Manager solution, you must go through the process of defining the business logic for each deployment. This is very time-consuming work.

In addition, you must validate that the business policies are being followed, and define and enable the action to take when a policy is violated.

3.2 The Resource Kit Solution

The Resource Kit contains an abstraction layer of architecture that defines common business policies. These business policies are defined in the driver policies, jobs, and workflow. By having the abstraction layer in place, it is very easy to deploy an Identity Manager solution once or more times.

3.3 The Technical Explanation

How the business process is implemented in the Resource Kit is documented in the “Business Logic” section of the *Identity Manager Resource Kit 1.2 Architecture Reference Guide*. The abstraction layer is defined in the “Business Processes” section of the *Identity Manager Resource Kit 1.2 Architecture Reference Guide*.

Solution for Making eDirectory Visible on the External IP Address

4

The Resource Kit VMware image is set for DHCP on the external IP address. eDirectory™ might not be visible to any other machine on the external IP address.

4.1 The Business Problem

By having the VMware image set to DHCP, the Resource Kit is not accessible to other machines. For example, no users can log in and access the User Application Web page. The Resource Kit is isolated.

4.2 The Resource Kit Solution

The setndsconf script makes eDirectory visible to other machines and the Resource Kit solution is no longer isolated. The setndsconf script is contained in the Designer project. For instructions on how to implement the script, see “Making eDirectory Visible on the External IP Address” in the *Identity Manager Resource Kit 1.2 Installation Guide for the Identity Manager Components*.

4.3 The Technical Explanation

The setndsconf script works as follows:

1. The script is not invoked until the network interfaces are started and assigned IP addresses. There can be multiple interfaces defined.
2. The script accesses the `root` user’s ID. In most cases it should be 0.
3. It checks for the default eDirectory configuration file location. Normally it is `/etc/opt/novell/eDirectory/conf/.edir/instances.`*`myuserid`* for eDirectory instances that the `root` user owns.
4. It parses the instance file and assumes that the first instance is the eDirectory instance installed on the VMware server.
5. It checks the `nds.conf` configuration file to see what ports have been defined for NCP™, HTTP, and HTTPS.
6. It accesses the server’s hostname.
7. It accesses the operating system name. (Linux).
8. It generates a list of interfaces. For example, eth0, eth1.
9. For each interface found, it parses the IP address and adds it to a list.
10. It backs up the `nds.conf` file found in the `/etc/opt/novell/eDirectory/conf/.edir/instances.<myuserid>`.

11. Changes are applied to the `nds.conf` file. The only changes made to the file are the list of https.server.interfaces, n4u.server.interfaces, and http.server.interfaces. These are changed to the list of IP addresses and ports found in Step 5 and Step 8. Everything else in the file remains the same.
12. It parses `/etc/hosts` file, looking for a domain name.
13. It backs up the `/etc/hosts` file.
14. It creates a new `/etc/hosts` file with the interfaces it found. They are listed as eth0 hostname.domain name hostname.
15. The script has finished executing, and ndsd starts after the new `nds.conf` file is in place. This allows eDirectory to start on any interface listed in the new `nds.conf` file.