Configuring
Enhance Provisioning Module

Marcel Thibault
Lead Consulting Engineer
Novell, Inc.

Eric Kuprel
Sr. Software Engineer
Novell, Inc.

Novell

Enhanced Provisioning Module
Overview

What is the Enhanced Provisioning Module?

Formerly Charles River

An interim release of Clearwater (Not the real product name...)

A Consultant Toolkit for Identity Driven application solutions

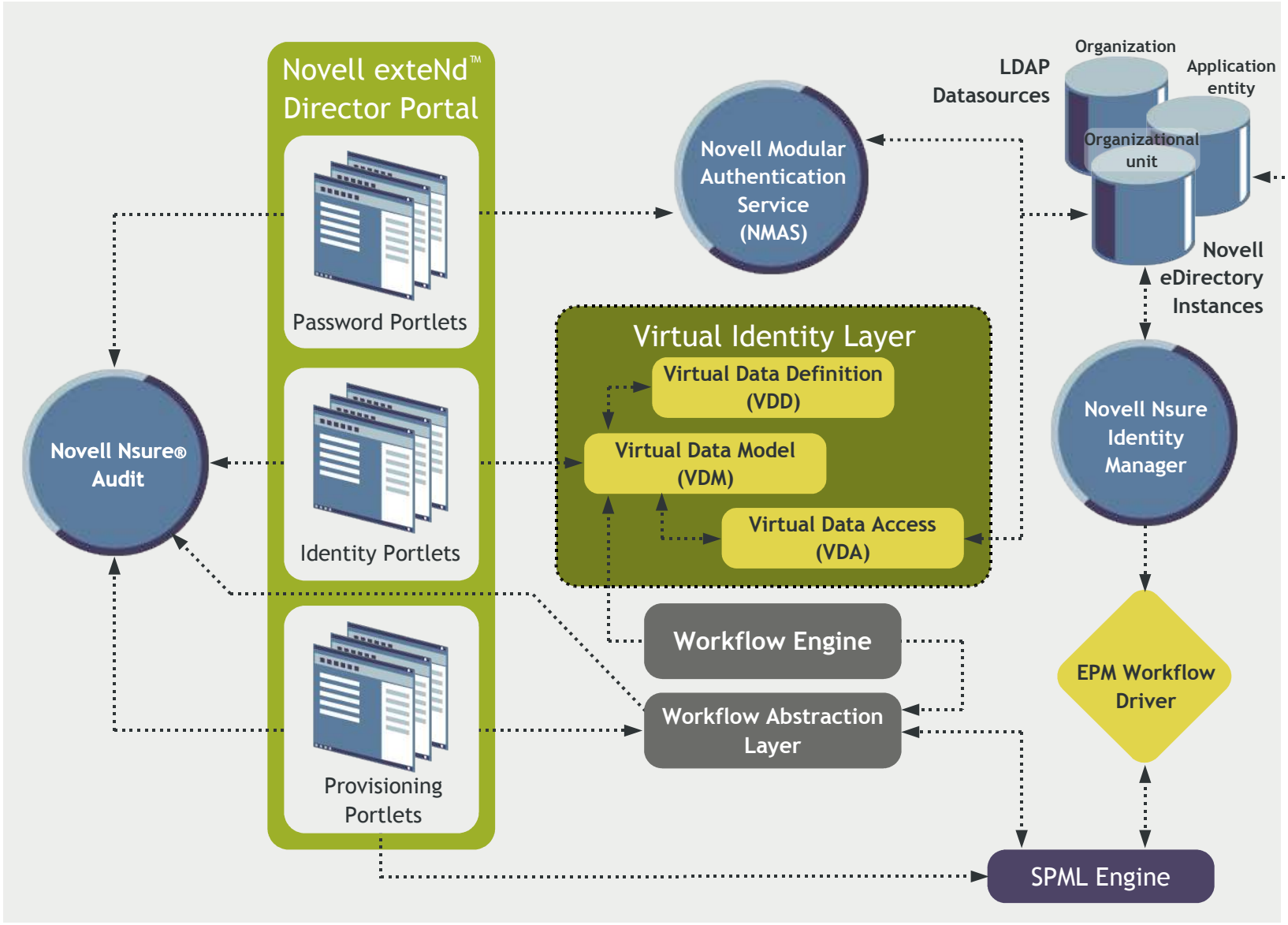
Enhanced Provisioning Module Includes

- Identity Driven Portlet Suite
- Password Management Portlets
- Service Provisioning Development Tools
- SPML Provisioning Target
- Workflow and Pageflow Enhancements
- Workflow Abstraction Layer
- Identity Abstraction Layer
- IDM Workflow Driver

© April 25, 2005 Novell Inc.

Novell.

EPM Architecture



Demo User Interface

Virtual Identity Layer

Virtual Identity Layer

Implementation of abstraction layer

Aggregates and normalizes multiple identity stores

Provides real-time access to one or more eDirectory™ Instances

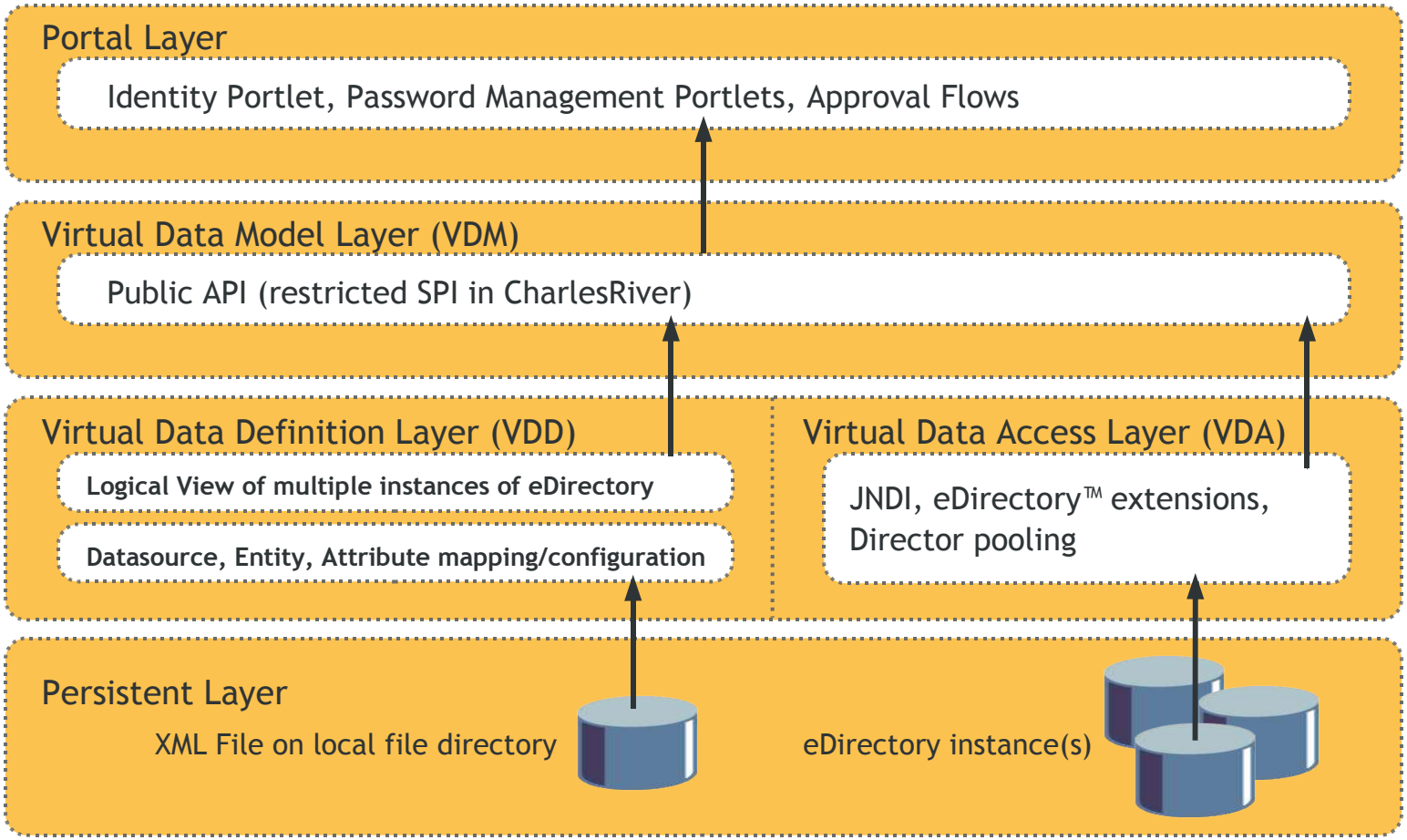
Registered as a Director subsystem

3 Layers

- Virtual Data Model Layer (VDM)—Portal Layer Interface
- Virtual Data Access Layer (VDA)—Access to persistent layer
- Virtual Data Definition Layer (VDD)—Defines logical view

© April 25, 2005 Novell Inc.

Virtual Identity Layer



© April 25, 2005 Novell Inc.

Novell.

Virtual Data Definition Layer

- Used by VDM and VDD
- Definitions are XML files stored on file directory
- Datasource configuration
- Object and attribute mapping
- Attribute Filtering and Sub typing
- Lightweight Access Controls
- Manual Configuration – Schema validation

© April 25, 2005 Novell Inc.

Novell.

VDD – XML Files

Datasource definitions (required)

- vdd-datasource.xml

Entity definitions (required)

- vdd-entity.xml

General configuration parameters (required)

- vdd-configuration.xml

Entity Attribute definitions (required per entity)

- vdd-{entityname}-attributes.xml

Dynamic Choice List Selections (optional)

- vdd-{selection}-choices.xml

© April 25, 2005 Novell Inc.

Novell.

Datasource Definition - VDD

Connection parameters for one or more eDirectory Instances

Define host and container root

Multiple definitions to same host, different container

Authentication – Uses Director login credentials to bind

© April 25, 2005 Novell Inc.

Novell.

Entity Definition - VDD

Logical object called “Entity” (i.e. User, Device, Group)

Defines object classes, including auxiliary classes if applicable

Defines lightweight access controls (Viewable, Creatable, Editable, Removable)

Specify datasource key

Specify attribute configuration file

© April 25, 2005 Novell Inc.

Novell.

Entity Attribute Definition - VDD

Defines attributes associated with entity

Definitions include:

- LDAP attribute name
- Reference Key
- Display label – localization support in next release
- Access control (enabled, readable, editable, viewable, searchable)
- Type (Integer, String, Boolean and Binary)
- Filtering – global filter on attribute
- Advanced Subtype (DN Lookup, Dynamic List, Static List, Range)

Immediate access revocation

© April 25, 2005 Novell Inc.

Attribute Subtype

StaticList

- valid choices for attribute (i.e. Employee type)

DynamicList

- valid choices for attribute defined in external xml file
  - will be expanded in future release.

Range

- valid range of values

DNLookup

- Provide lookup of associated objects, rather than qualified context (i.e. Cn=...)
- Can provide synchronization on update for LDAP group associations. Used in sample for device/user associations

© April 25, 2005 Novell Inc.

VDD Definition Demo

SPML Advanced Configuration

SPML Advanced Configurations

SPML

- Service Provisioning Meta Language
- SPML Documents
  - Provide Identifier
  - Define Provisioning Services
    - Attributes
    - Type (Add, Modify, Delete)
  - Associate Workflow To Services

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations

Configurations

- UI
  - SPML Document, Pageflow, Xforms
- Processing Logic
  - Pageflow and Workflows
  - Java Activities, Scopedpath, XSL Transformation
- IDM EPM Driver
  - Provisioning Services, Supply Values For Attributes

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations

UI – SPML Document

- Add or Remove Attributes
  - List Screen
  - Edit/Display screens
- Create Input/Output Field
  - “required” attribute set to true/false
- Create check box fields (boolean)

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations

UI – SPML Document Structure

<schema

<providerIdentifier

<schemaIdentifier

<attributeDefinition – used for all services

<objectClassDefinition – provisioning services

<memberAttributes>

<attributeDefinitionReference

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations

UI – Add or Remove Attributes

- Example – Version

```
<attributeDefinition description="Version"
  multivalued="false" name="Version" type="xsd:string">
    <properties>
        <attr name="realmAttribute">
            <value>false</value>
```

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations

UI – Add or Remove Attributes

- Example – Email

```
<attributeDefinition description="EMail"
 multivalued="false" name="EMail" type="xsd:string">
    <properties>
        <attr name="listDisplay">
            <value>true</value>
        </attr>
        <attr name="realmObjectClass">
            <value>user</value>
```

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations

UI – Add or Remove Attributes

- Example

```
<objectClassDefinition
    <memberAttributes>
        <attributeDefinitionReference name="version"
          required="true"/>
        <attributeDefinitionReference name=”Email”
          required="false"/>
```

© April 25, 2005 Novell Inc.

Novell.

Demo SPML

SPML Advanced Configurations

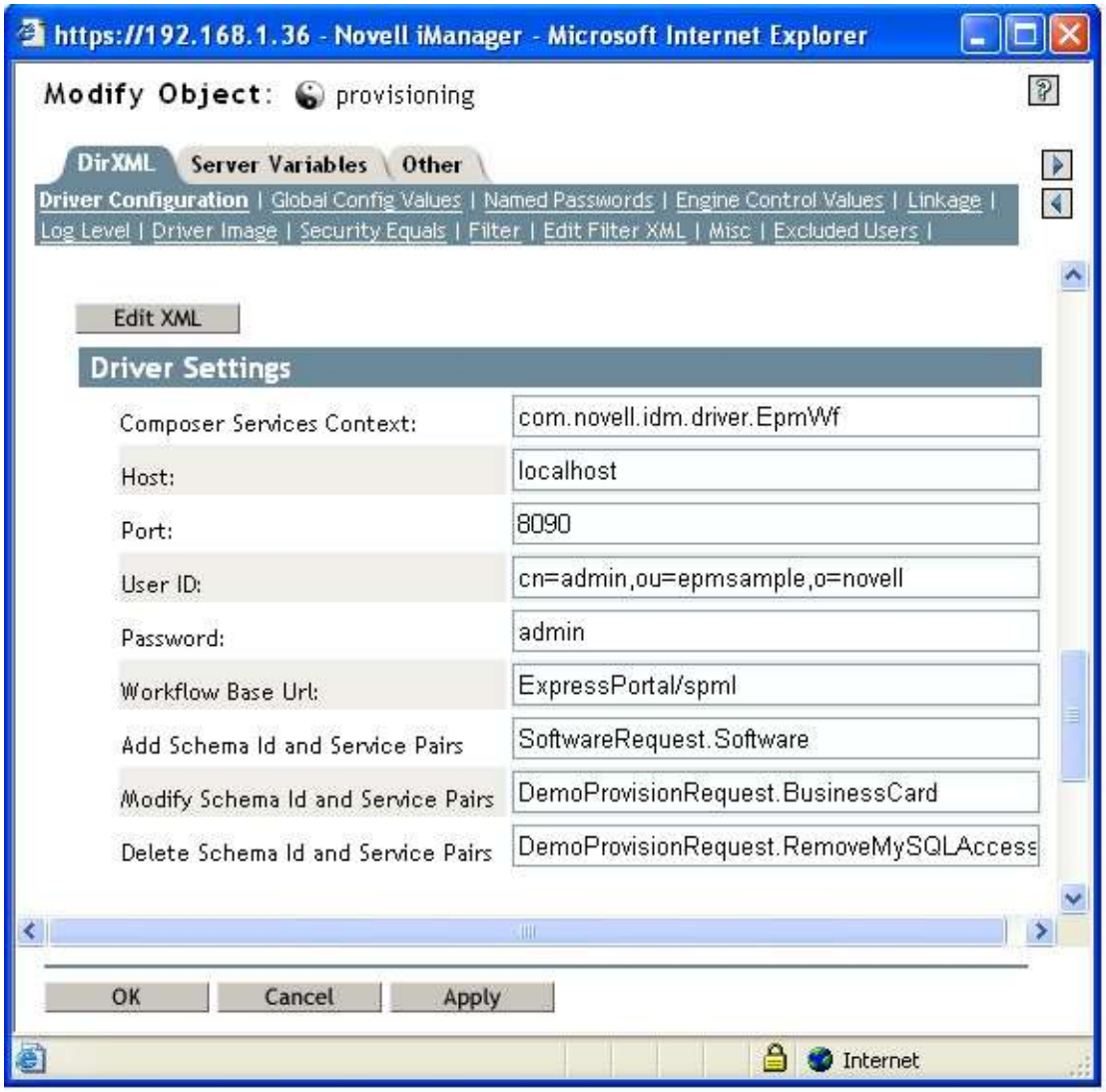
IDM EPM Driver - Provisioning Services

- Three IDM Events (Add, Modify, Delete)
- Start Multiple Provisioning Services
  - Comma Delimited [SPML Doc].[Service] Pair
  - Example:
    - SoftwareRequest.Software, DemoProvisioningRequest.BusinessCard
- Access To Transformation Processes
  - Schema Mappings
  - Policies
  - etc.

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations



SPML Advanced Configurations

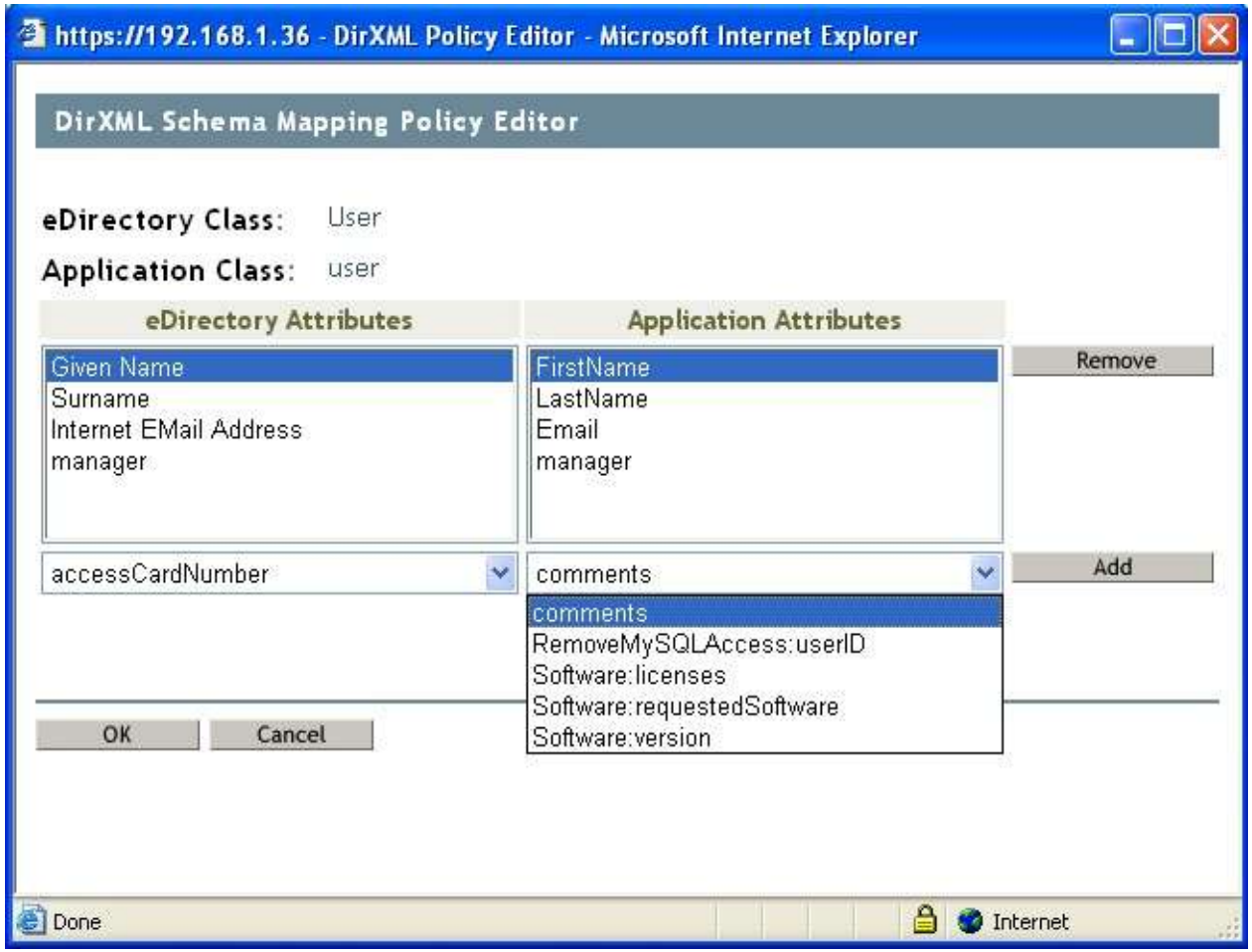
IDM EPM Driver - Schema Mappings

- Map IDM Attributes to EPM/SPML Attributes
- Refresh Application Schema
  - New SPML Documents
  - New Attributes
  - Remove Attributes

© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations



© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations

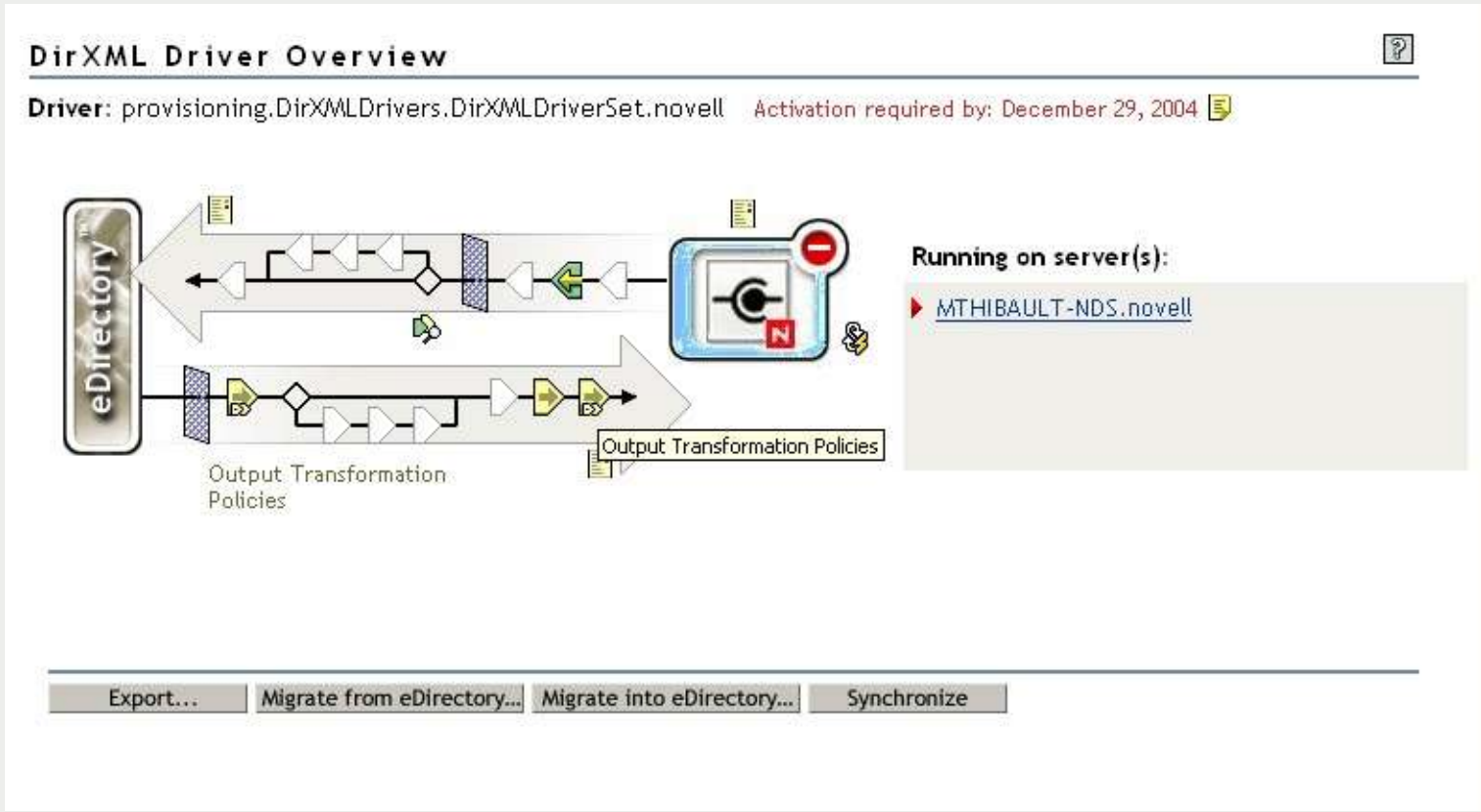
IDM EPM Driver – Transformation Policies

- Defined At Various Points During The Transformation Process
- Access To SPML Attributes
- Publisher/Subscriber Transformation Channels
  - Usually Use Subscriber Channel
  - Output Transformation Policies

© April 25, 2005 Novell Inc.

Novell.

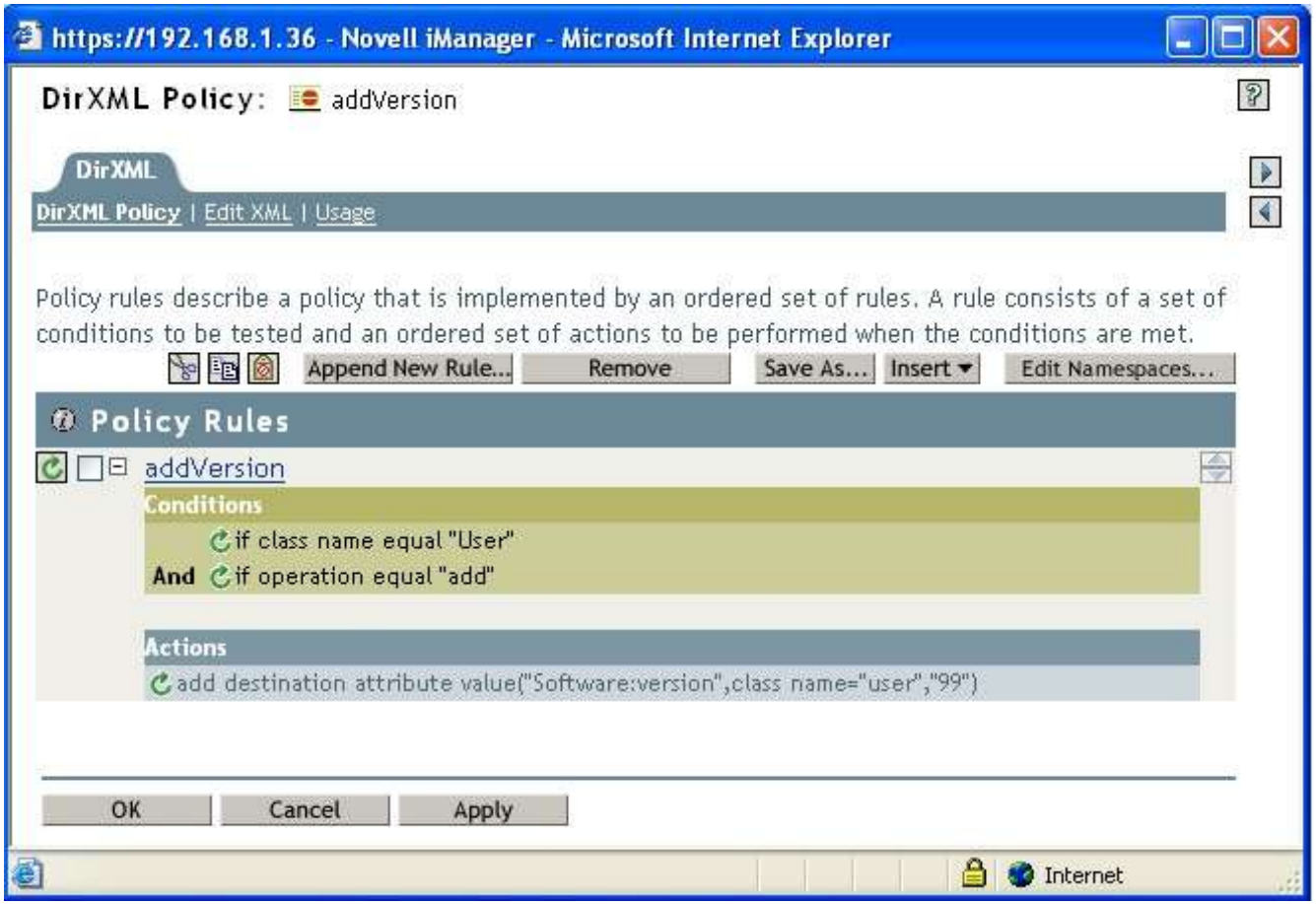
SPML Advanced Configurations



© April 25, 2005 Novell Inc.

Novell.

SPML Advanced Configurations



© April 25, 2005 Novell Inc.

Novell.

Demo SPML

Password Management

IDM Requirements

Before you can use most of the password self-service and user authentication features, you need to do the following in eDirectory:

- Enable **Universal Password**
- Create one or more **password policies**
- Assign the appropriate password policies to **users**

© April 25, 2005 Novell Inc.

Novell.

Password Portlets

Features

These portlets allow the end-user to change their password. This is not just simple UI for enter a new password. This exposes the Universal Password feature introduced in eDirectory 8.7.3 and some password management features in IDM2.

Administrator

- Configure password policies (length, types of characters, exclusion lists, time between changes, etc)
- Configure challenge questions grouped into sets, user definable challenges, and hints
- Configure forgotten password actions (reset, email, force change, etc)

End User

- Login prompts for required policy actions (hint, challenge response, password change)
- Configurable Portlets allow user to change these items at will

© April 25, 2005 Novell Inc.

Login and Authentication

IDM Login portlet replaces standard exteNd Director™ Login portlet

User authentication supported by Identity Manager (through Universal Password, password policies, and NMAS).

Redirects to the other EPM password portlets as needed during the login process (i.e. hint, challenge response).

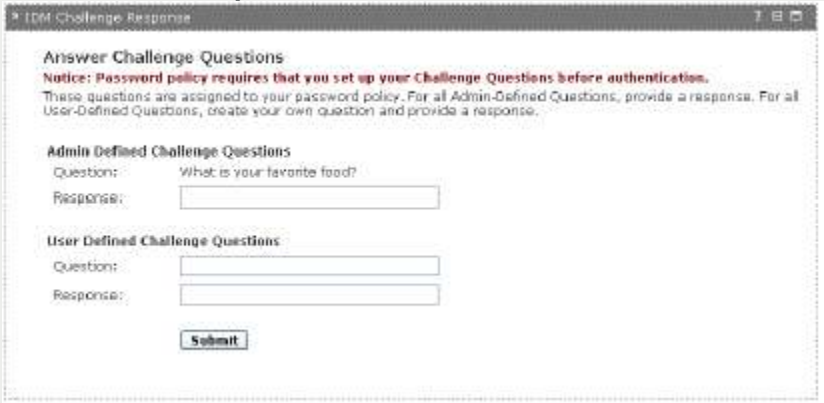
© April 25, 2005 Novell Inc.

Novell

IDM Challenge Response Portlet

This self-service portlet lets users:

- Set up the valid responses to administrator-defined challenge questions, and set up user-defined challenge questions and responses
- Change the valid responses to administrator-defined challenge questions, and change user-defined challenge questions and responses



© April 25, 2005 Novell Inc.

Novell.

IDM Hint Definition Portlet

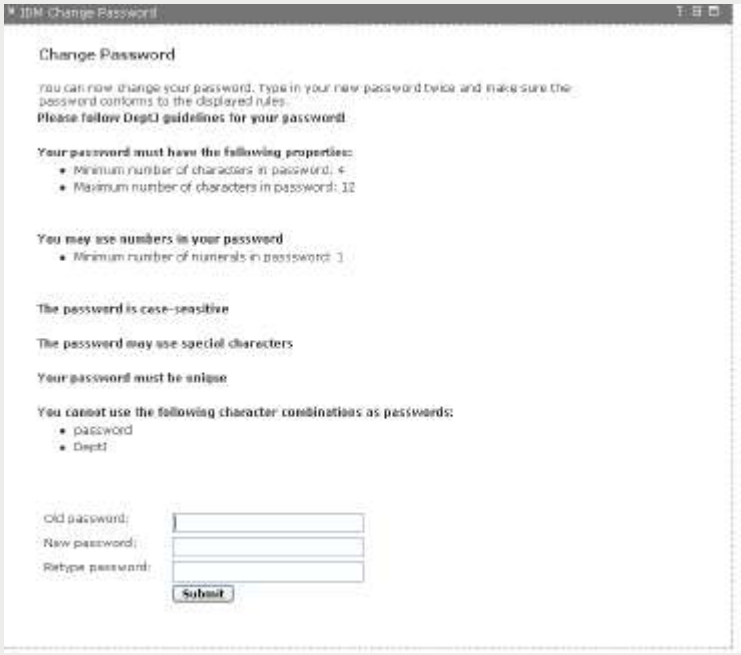
This self-service portlet lets the user set up or change their password hint (which may be displayed or emailed as a clue in forgotten password situations).

© April 25, 2005 Novell Inc.

Novell.

IDM Change Password Portlet

This self-service portlet lets the user change (reset) their Universal Password, according to the assigned password policy. It uses that policy to display the rules that the new password must conform to. If Universal Password is not enabled, this portlet changes the user's eDirectory (simple) password, as permitted in the user's Password Restrictions.



© April 25, 2005 Novell Inc.

Novell.

IDM Forgot Password Portlet

Uses challenge/response authentication to let the user get information about their password (from NMAS). The result, which depends on the assigned password policy, may include:

- Displaying the user's password hint on the screen
- Emailing the hint to the user
- Emailing the password to the user
- Prompting the user to reset (change) the password

© April 25, 2005 Novell Inc.

Novell.

Logging

Logging

EPM implements logging by using Log4j, open-source logging package distributed by The Apache Software Foundation.

Administrators can activate several logging channels, including

- Nsure® Audit
- File
- Console

© April 25, 2005 Novell Inc.

Novell.

What gets Logged

EPM logs the following event types

- Provisioning – approve, reject, SPML
- Password Change
- Entity operations – update, add, remove
- Search operations – requests, save query

© April 25, 2005 Novell Inc.

Novell.

Logging Reports

There are several ways to generate reports against data logged to an Nsure Audit database:

- Crystal Reports
  - Two predifined reports are included
- Nsure Audit Report application (Windows only)
- Write queries against the logged data using iManager
- Write your own SQL queries
- Use Spreadsheet application (i.e. OpenOffice, Excel)

© April 25, 2005 Novell Inc.

Demo Logging

Novell®

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Novell, Inc., makes no representations or warranties with respect to the contents of this document, 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 document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

Novell