Novell Identity Manager

3.0

www.novell.com

8 de diciembre de 2005

APLICACIÓN DE USUARIO DEL GESTOR DE IDENTIDADES: GUÍA DE ADMINISTRACIÓN

Novell®

Información legal

Novell, Inc. no otorga ninguna garantía respecto al contenido y el uso de esta documentación, y específicamente renuncia a cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Asimismo, Novell, Inc. se reserva el derecho a revisar esta publicación y a realizar cambios en su contenido en cualquier momento, sin obligación de notificar tales revisiones o cambios a ninguna persona o entidad.

Además, Novell, Inc. no ofrece ninguna garantía con respecto a ningún software, y rechaza específicamente cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Por otra parte, Novell, Inc. se reserva el derecho a realizar cambios en cualquiera de las partes o en la totalidad del software de Novell en cualquier momento, sin obligación de notificar tales cambios a ninguna persona ni entidad.

Todos los productos o información técnica que se proporcionen bajo este Contrato pueden estar sujetos a los controles de exportación de Estados Unidos y a las leyes de comercio de otros países. Usted acepta acatar las regulaciones de los controles de exportaciones y obtener todas las licencias necesarias para exportar, reexportar o importar bienes. Acepta no realizar exportaciones o reexportaciones a entidades que se encuentren en las actuales listas de exclusión de exportaciones estadounidenses ni a países con embargos comerciales o con problemas de terrorismo, tal como especifican las leyes de exportación de Estados Unidos. Acepta no utilizar bienes para uso nuclear, o fabricación de misiles o armas biológicas prohibidas. Para obtener más información acerca de la exportación del software de Novell, consulte www.novell.com/info/exports/. Novell no asume ninguna responsabilidad sobre su imposibilidad de obtención de las aprobaciones necesarias para la exportación.

Novell, Inc. tiene derechos de propiedad intelectual referentes a la tecnología empleada en el producto que se describe en el presente documento. Dichos derechos de propiedad intelectual pueden incluir específicamente, y sin limitación alguna, una o más patentes de los Estados Unidos incluidas en la lista de http://www.novell.com/company/legal/patents/ y una o más patentes adicionales o aplicaciones pendientes de patente en Estados Unidos y otros países.

El derecho a utilizar este Software y su documentación, las patentes, los copyright y el resto de derechos de propiedad que correspondan en todo momento es única y exclusivamente de Novell y los otorgadores de licencias, y el usuario no puede llevar a cabo ninguna acción que no sea coherente con ese uso. El Software está protegido por leyes de copyright y tratados internacionales. El usuario no debe eliminar ningún aviso de copyright ni cualquier otro tipo de avisos de propiedad del Software ni de su documentación, y deberá reproducir dichos avisos en todas las copias o extractos del Software o su documentación. El usuario no adquiere ningún derecho de propiedad del Software.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EE.UU.
www.novell.com

Documentación en línea: Para acceder a la documentación en línea sobre éste y otros productos Novell, así como obtener actualizaciones, consulte www.novell.com/documentation.

Marcas comerciales de Novell

Novell es una marca comercial registrada de Novell, Inc. en los Estados Unidos y en otros países.
SUSE es una marca comercial registrada de Novell, Inc. en los Estados Unidos y en otros países.

Materiales de otros fabricantes

Todas las marcas comerciales de otros fabricantes son propiedad de sus respectivas empresas.

Información legal de otros fabricantes

Licencia para el software Apache, versión 1.1

Copyright (c) 2000 The Apache Software Foundation. Reservados todos los derechos.

La redistribución y el uso en los formatos de código fuente y binario, con o sin modificaciones, están permitidos siempre y cuando se cumplan las condiciones siguientes:

1. Las redistribuciones de código fuente deben efectuarse conservando el aviso de copyright anterior, la presente lista de condiciones y la renuncia de responsabilidad siguiente.

1. Las redistribuciones de formato de código binario deben reproducir el aviso de copyright anterior, la presente lista de condiciones y la renuncia de responsabilidad siguiente en la documentación y/u otros materiales suministrados con la distribución.

3. La documentación (si existe) del usuario final incluida con la redistribución debe contener el reconocimiento siguiente: "Este producto incluye software desarrollado por Apache Software Foundation (http://www.apache.org/)".

Por otra parte, este reconocimiento puede aparecer en el mismo software, allí donde normalmente aparecen (si aparecen) los reconocimientos de otros fabricantes.

4. Los nombres "Apache" y "Apache Software Foundation" no deben utilizarse para respaldar ni promocionar productos derivados de este software, sin haber obtenido previamente un permiso por escrito. Para solicitar un permiso por escrito, póngase en contacto con apache@apache.org.

5. Los productos derivados de este software no se pueden llamar "Apache" y "Apache" no puede aparecer en su nombre, sin haber obtenido previamente un permiso por escrito de Apache Software Foundation.

ESTE SOFTWARE SE PROPORCIONA "TAL CUAL" Y SE RECHAZA CUALQUIER GARANTÍA IMPLÍCITA O EXPLÍCITA, INCLUIDAS, AUNQUE SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O ADECUACIÓN PARA UN FIN DETERMINADO. EN NINGÚN CASO, THE APACHE SOFTWARE FOUNDATION O SUS CONTRIBUIDORES SERÁN RESPONSABLES DE CUALQUIER DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENCIAL (INCLUIDOS AUNQUE SIN LIMITARSE A ELLOS, LA OBTENCIÓN DE ARTÍCULOS O SERVICIOS SUSTITUTIVOS, LA PÉRDIDA DE USO, DATOS O BENEFICIOS, O LA INTERRUPCIÓN DEL NEGOCIO), CON INDEPENDENCIA DE CUÁL HAYA SIDO LA CAUSA, O DE CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD ESTRICTA O PERJUICIO (INCLUIDOS LA NEGLIGENCIA U OTROS) QUE SE PRODUZCA COMO CONSECUENCIA DE CUALQUIER TIPO DE USO DE ESTE SOFTWARE, INCLUSO AUNQUE SE HAYA ADVERTIDO DE LA POSIBILIDAD DE QUE SE PRODUZCA DICHO DAÑO.

Autonomy

Copyright ©1996-2000 Autonomy, Inc.

Bouncy Castle

Copyright (c) de la licencia 2000 - 2004 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Por la presente, se otorga el permiso, de forma gratuita, a todas las personas que obtengan una copia de este software, así como de los archivos de documentación asociados (el "Software") a utilizar este software sin restricciones de ningún tipo, incluidos, sin limitarse a ellos, los derechos a utilizar, copiar, modificar, fusionar, publicar, distribuir, poner en sublicencia y/o vender copias del software y permitir que aquellas personas a las que se suministre el Software, hagan lo mismo, siempre y cuando cumplan las condiciones siguientes:

El aviso de copyright anterior y este aviso de permiso se incluirán en todas las copias o en partes de tamaño considerable del Software.

EL SOFTWARE SE PROPORCIONA "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, IMPLÍCITA O EXPLÍCITA, INCLUIDAS, AUNQUE SIN LIMITARSE A ELLAS, LAS GARANTÍAS DE COMERCIALIZACIÓN O ADECUACIÓN PARA UN FIN DETERMINADO Y LA NO INFRACCIÓN. EN

NINGÚN CASO EL AUTOR O LOS PROPIETARIOS DEL COPYRIGHT SERÁN RESPONSABLES DE CUALQUIER RECLAMACIÓN, DAÑO U OTRAS RESPONSABILIDADES, QUE SE PRESENTEN POR EFECTOS DEL CONTRATO, PERJUICIO U OTROS, Y QUE SE DEBA AL SOFTWARE O AL USO DE ÉSTE O LAS OPERACIONES REALIZADAS CON ÉSTE.

Castor Library

La licencia original se encuentra en http://www.castor.org/license.html

El código de este proyecto está indicado en una licencia de tipo BSD [license.txt]:

Copyright 1999-2004 (C) Intalio Inc y otros. Reservados todos los derechos.

La redistribución y el uso de este software, así como de la documentación asociada ("Software"), con o sin modificaciones, están permitidos siempre y cuando se cumplan las condiciones siguientes:

1. Las redistribuciones de código fuente deben efectuarse conservando las declaraciones de copyright y los avisos. Asimismo, las redistribuciones deben contener una copia del presente documento.

1. Las redistribuciones de formato binario deben reproducir el aviso de copyright anterior, la presente lista de condiciones y la renuncia de responsabilidad siguiente en la documentación y/u otros materiales suministrados con la distribución.

4. El nombre "ExoLab" no debe utilizarse para respaldar ni promocionar productos derivados de este Software, sin haber obtenido previamente un permiso por escrito de Intalio Inc. Para obtener un permiso por escrito, póngase en contacto con info@exolab.org.

4. Los productos derivados de este Software no se pueden llamar "Castor" y "Castor" no puede aparecer en los nombres, sin haber obtenido previamente un permiso por escrito de Intalio Inc. Exolab; Castor e Intalio son marcas comerciales de Intalio Inc.

5. ¿Deberá darse el crédito debido al proyecto ExoLab? (http://www.exolab.org/).

INTALIO Y OTROS CONTRIBUIDORES PROPORCIONAN ESTE SOFTWARE "TAL CUAL" Y SE RECHAZA CUALQUIER GARANTÍA IMPLÍCITA O EXPLÍCITA, INCLUIDAS, AUNQUE SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O ADECUACIÓN PARA UN FIN DETERMINADO. EN NINGÚN CASO, INTALIO O SUS CONTRIBUIDORES SERÁN RESPONSABLES DE CUALQUIER DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENCIAL (INCLUIDOS AUNQUE SIN LIMITARSE A ELLOS, LA OBTENCIÓN DE ARTÍCULOS O SERVICIOS SUSTITUTIVOS, LA PÉRDIDA DE USO, DATOS O BENEFICIOS, O LA INTERRUPCIÓN DEL NEGOCIO), CON INDEPENDENCIA DE CUÁL HAYA SIDO LA CAUSA, O DE CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD ESTRICTA O PERJUICIO (INCLUIDOS LA NEGLIGENCIA U OTROS) QUE SE PRODUZCA COMO CONSECUENCIA DE CUALQUIER TIPO DE USO DE ESTE SOFTWARE, INCLUSO AUNQUE SE HAYA ADVERTIDO DE LA POSIBILIDAD DE QUE SE PRODUZCA DICHO DAÑO.

Licencia de software de Indiana University Extreme! Lab

Versión 1.1.1

Copyright (c) 2002 Extreme! Lab, Indiana University. Reservados todos los derechos.

La redistribución y el uso en los formatos de código fuente y binario, con o sin modificaciones, están permitidos siempre y cuando se cumplan las condiciones siguientes:

1. Las redistribuciones de código fuente deben efectuarse conservando el aviso de copyright anterior, la presente lista de condiciones y la renuncia de responsabilidad siguiente.

1. Las redistribuciones de formato binario deben reproducir el aviso de copyright anterior, la presente lista de condiciones y la renuncia de responsabilidad siguiente en la documentación y/u otros materiales suministrados con la distribución.

3. La documentación (si existe) del usuario final incluida con la redistribución debe incluir el reconocimiento siguiente: "Este producto incluye software desarrollado por Indiana University Extreme! Lab (http://www.extreme.indiana.edu/)."

Por otra parte, este reconocimiento puede aparecer en el mismo software, allí donde normalmente aparecen (si aparecen) los reconocimientos de otros fabricantes.

4. Los nombres "Indiana University" e "Indiana University Extreme! Lab" no deben utilizarse para respaldar ni

promocionar productos derivados de este software, sin haber obtenido previamente un permiso por escrito. Para solicitar un permiso por escrito, póngase en contacto con http://www.extreme.indiana.edu/.

5. Los productos derivados de este software no pueden utilizar el nombre "Indiana University" y "Indiana University" no puede aparecer en su nombre, sin haber obtenido previamente un permiso por escrito de Indiana University.

ESTE SOFTWARE SE PROPORCIONA "TAL CUAL" Y SE RECHAZA CUALQUIER GARANTÍA IMPLÍCITA O EXPLÍTCITA, INCLUIDAS, AUNQUE SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O ADECUACIÓN PARA UN FIN DETERMINADO. EN NINGÚN CASO, LOS AUTORES, LOS POSEEDORES DEL COPYRIGHT O SUS CONTRIBUIDORES SERÁN RESPONSABLES DE CUALQUIER DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENCIAL (INCLUIDOS AUNQUE SIN LIMITARSE A ELLOS, LA OBTENCIÓN DE ARTÍCULOS O SERVICIOS SUSTITUTIVOS, LA PÉRDIDA DE USO, DATOS O BENEFICIOS, O LA INTERRUPCIÓN DEL NEGOCIO), CON INDEPENDENCIA DE CUÁL HAYA SIDO LA CAUSA, O DE CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD ESTRICTA O PERJUICIO (INCLUIDOS LA NEGLIGENCIA U OTROS) QUE SE PRODUZCA COMO CONSECUENCIA DE CUALQUIER TIPO DE USO DE ESTE SOFTWARE, INCLUSO AUNQUE SE HAYA ADVERTIDO DE LA POSIBILIDAD DE QUE SE PRODUZCA DICHO DAÑO.

JDOM.JAR

Copyright (C) 2000-2002 Brett McLaughlin & Jason Hunter. Reservados todos los derechos.

La redistribución y el uso en los formatos de código fuente y binario, con o sin modificaciones, están permitidos siempre y cuando se cumplan las condiciones siguientes:

1. Las redistribuciones de código fuente deben efectuarse conservando el aviso de copyright anterior, la presente lista de condiciones y la renuncia de responsabilidad siguiente.

2. Las redistribuciones de formato binario deben reproducir el aviso de copyright anterior, la presente lista de condiciones y la renuncia de responsabilidad que sigue a estas condiciones en la documentación y/u otros materiales suministrados con la distribución.

3. El nombre "JDOM" no debe utilizarse para respaldar ni promocionar productos derivados de este software, sin haber obtenido previamente un permiso por escrito. Para solicitar un permiso por escrito, póngase en contacto con license@jdom.org.

4. Los productos derivados de este software no se pueden llamar "JDOM" y "JDOM" no puede aparecer en su nombre, sin haber obtenido previamente un permiso por escrito de la dirección del proyecto JDOM (pm@jdom.org).

Asimismo, solicitamos (aunque no es obligatorio) que incluya en la documentación para el usuario final suministrada con la redistribución y/o en el mismo software un reconocimiento que equivalga a lo siguiente: "Este producto incluye software desarrollado por el proyecto JDOM (http://www.jdom.org/)".

Por otra parte, el reconocimiento puede ser de tipo gráfico mediante el uso de los logotipos disponibles en http://www.jdom.org/images/logos.

ESTE SOFTWARE SE PROPORCIONA "TAL CUAL" Y SE RECHAZA CUALQUIER GARANTÍA IMPLÍCITA O EXPLÍCITA, INCLUIDAS, AUNQUE SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O ADECUACIÓN PARA UN FIN DETERMINADO. EN NINGÚN CASO, LOS AUTORES DE JDOM O LOS CONTRIBUIDORES DEL PROYECTO SERÁN RESPONSABLES DE CUALQUIER DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENCIAL (INCLUIDOS AUNQUE SIN LIMITARSE A ELLOS, LA OBTENCIÓN DE ARTÍCULOS O SERVICIOS SUSTITUTIVOS, LA PÉRDIDA DE USO, DATOS O BENEFICIOS, O LA INTERRUPCIÓN DEL NEGOCIO), CON INDEPENDENCIA DE CUÁL HAYA SIDO LA CAUSA, O DE CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD ESTRICTA O PERJUICIO (INCLUIDOS LA NEGLIGENCIA U OTROS) QUE SE PRODUZCA COMO CONSECUENCIA DE CUALQUIER TIPO DE USO DE ESTE SOFTWARE, INCLUSO AUNQUE SE HAYA ADVERTIDO DE LA POSIBILIDAD DE QUE SE PRODUZCA DICHO DAÑO.

Phaos

Este software proviene, en parte, del kit de herramientas de SSLavaTM, que es Copyright ©1996-1998 de Phaos Technology Corporation. Reservados todos los derechos. Los clientes tienen prohibido acceder a las funciones del

software Phaos.

W3C

AVISO Y LICENCIA DE SOFTWARE W3C®

Este trabajo (así como el software y la documentación incluidos como los README (LÉAME) u otros elementos relacionados) ha sido suministrado por los propietarios del copyright con la licencia siguiente. Al obtener, utilizar y/o copiar este trabajo, (el licenciatario) confirma que ha leído, comprendido y cumplido los términos y condiciones siguientes.

Por la presente, se otorga el permiso para copiar, modificar o distribuir este software y su documentación, con o sin modificaciones, para cualquier fin y sin tener que pagar cuota o derecho alguno, siempre y cuando se incluya el texto siguiente en TODAS las copias del software y documentación o partes de éstas, incluidas las modificaciones:

1. El texto completo de este AVISO en un lugar visible para todos los usuarios del trabajo redistribuido o derivado.

2. Cualquier renuncia de responsabilidad, aviso o términos y condiciones de propiedad intelectual existentes previamente. Si no existe ninguno, deberá incluirse un aviso breve de software de W3C (preferible hipertexto, aunque el texto está permitido) dentro del cuerpo de cualquier código redistribuido o derivado.

3. Aviso de cualquier cambio o modificación en los archivos, incluida la fecha de las modificaciones. (Se recomienda el suministro de los URI a la ubicación a partir de la que se deriva el código).

ESTE SOFTWARE Y LA DOCUMENTACIÓN SE SUMINISTRAN "TAL CUAL" Y LOS PROPIETARIOS DEL COPYRIGHT NO OTORGAN NINGUNA REPRESENTACIÓN NI GARANTÍA, YA SEA IMPLÍCITA O EXPLÍCITA, (INCLUIDAS AUNQUE SIN LIMITARSE A ELLAS, LAS GARANTÍAS DE COMERCIALIZACIÓN O ADECUACIÓN PARA UN FIN DETERMINADO), DE QUE EL USO DEL SOFTWARE O LA DOCUMENTACIÓN NO INFRINGIRÁN LA PATENTE DE OTRO FABRICANTE, NI NINGÚN COPYRIGHT, MARCA COMERCIAL U OTRO DERECHO.

LOS PROPIETARIOS DEL COPYRIGHT NO SERÁN RESPONSABLES DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL O CONSECUENCIAL QUE SE PRODUZCA COMO CONSECUENCIA DEL USO DEL SOFTWARE O DE LA DOCUMENTACIÓN.

El nombre y las marcas comerciales de los propietarios del copyright NO se utilizarán en anuncios ni en publicidad que pertenezcan al software, sin un permiso explícito previo por escrito. La titularidad del copyright de este software y de cualquier documentación asociada permanecerá siempre en manos de los propietarios del copyright.

Tabla de contenido

Acerca de esta guía

Objetivo

En este manual se describe cómo administrar la *aplicación de usuario* del Gestor de identidades, incluidas:

- Las funciones de *autoservicio de identidades* suministradas con el Gestor de identidades
- Las funciones de *provisión basadas en el flujo de trabajo* proporcionadas si se añade el módulo de provisión del Gestor de identidades.

Para obtener información sobre cómo administrar las demás funciones del Gestor de identidades (comunes a todos los paquetes), consulte la *Novell Identity Manager Administration Guide* (Guía de administración del Gestor de identidades).

Público al que va dirigido

La información suministrada en la presente guía está destinada a *administradores, arquitectos y asesores de sistemas* responsables de *configurar, desplegar y gestionar* las funciones de autoservicio de identidad y/o las funciones de provisión basadas en el flujo de trabajo de la aplicación de usuario del Gestor de identidades.

La documentación para el usuario final de estas funciones se suministra en la *Aplicación de usuario del Gestor de identidades: Guía del usuario*.

Requisitos previos

En este libro se presupone que:

- *Tiene instalado el* Gestor de identidades y, posiblemente, también el módulo de provisión del Gestor de identidades.

Para encontrar instrucciones acerca de cómo instalar estos productos, consulte la guía *Novell Identity Manager: Installation Guide* (Gestor de identidades: Guía de instalación).

- *Tiene configuradas* las demás funciones del Gestor de identidades de la forma más adecuada a sus necesidades.

Consulte la *Novell Identity Manager: Administration Guide* (Gestor de identidades: Guía de administración).

Organización

A continuación se muestra un resumen de la información que encontrará en este manual:

Parte	Descripción
Parte I, “Descripción general”, en la página 11	Sirve de introducción a la aplicación de usuario del Gestor de identidades y le ayuda a planificar cómo utilizarla en su organización

Parte	Descripción
Parte II, “Configuración del entorno de la aplicación de usuario”, en la página 55	Cómo configurar diversos aspectos del entorno de la aplicación de usuario del Gestor de identidades (incluidos el controlador de la aplicación de usuario, el nivel de abstracción del directorio y el registro) para responder a las necesidades de su organización
Parte III, “Administración de la aplicación de usuario”, en la página 127	Cómo configurar y gestionar la aplicación de usuario del Gestor de identidades mediante la pestaña Administración de la interfaz de usuario
Parte IV, “Referencia de portlet”, en la página 237	Cómo configurar la identidad y los portlets del sistema utilizados en la interfaz de usuario del Gestor de identidades
Parte V, “Diseño y gestión de peticiones de provisión”, en la página 309	Cómo configurar, implantar y gestionar los recursos, los flujos de trabajo y las definiciones de peticiones necesarias para suministrar mediante el módulo de provisión del Gestor de identidades **Nota:** Esta parte sólo es relevante si dispone del módulo de provisión del Gestor de identidades.
Parte VI, “Apéndices”, en la página 363	Información de consulta adicional (extensiones del esquema) y temas avanzados (configuración del archivo de reserva de la aplicación) de la aplicación del usuario del Gestor de identidades

Consulta adicional

Para consultar información adicional de archivos README (LÉAME) y manuales relacionados, visite la página del Gestor de identidades (http://www.novell.com/idm/) del sitio Web de documentación de Novell.

Descripción general

Los capítulos siguientes sirven de introducción a la aplicación de usuario del Gestor de identidades y le ayudarán a planificar cómo utilizarla en su organización.

Descripción general

1

La aplicación de usuario del Gestor de identidades es una potente aplicación Web cuyo objetivo es proporcionar una experiencia de usuario plena, intuitiva, fácilmente configurable y administrable en un marco de trabajo de sofisticados servicios de identidad. Cuando se utiliza junto con el módulo de provisión del Gestor de identidades y con Novell Audit, la aplicación de usuario del Gestor de identidades proporciona una solución de provisión completa de extremo a extremo que es segura, escalable y fácil de gestionar.

La aplicación de usuario proporciona las siguientes funciones de usuario final basadas en Web:

- Páginas blancas
- Organizational chartsOrganigramas corporativosBúsqueda de usuarios (con la capacidad de guardar las configuraciones de búsqueda personalizadas)
- Autoservicio de gestión de contraseñas
- Herramientas ligeras de administración del usuario
- Iniciación y monitorización de flujos de trabajo (si el módulo de provisión está instalado)
- Gestión de tareas personales y/o del equipo (si el módulo de provisión está instalado)
- Capacidades de delegación y apoderados (proxy)

En el caso del administrador del sistema, la aplicación de usuario brinda una amplia variedad de posibilidades de configuración y administración, entre las que figuran:

- Una interfaz que permite configurar y gestionar los derechos de apoderado y de delegación.
- Acceso a herramientas de registro y Crystal Reports personalizados
- Configuración de flujos de trabajo basada en asistente (si el módulo de provisión está instalado)
- Gestión de flujos de trabajo (si el módulo de provisión está instalado), incluida la capacidad de reasignar o terminar flujos de trabajo en curso
- Diseñador basado en Eclipse para crear definiciones y relaciones de abstracción del directorio personalizadas

En la tabla siguiente se muestra una lista completa de las funciones y posibilidades.

Función	Descripción
Entorno de interfaz de usuario Web ampliable, basado en estándares, e independiente del navegador utilizado	El administrador puede cambiar los diseños de página, la página por defecto (principal), añadir nuevas páginas y modificar el aspecto general (temas). La aplicación de usuario se puede ampliar añadiendo portlets compatibles con JSR-168.
Flujos de trabajo de provisión (con el módulo de provisión instalado)	El administrador puede crear flujos de trabajo a medida para procesar las peticiones de provisión. Además, los usuarios finales que dispongan de los derechos pertinentes, pueden iniciar dichos flujos de trabajo.

Función	Descripción
Flujos de trabajo basados en eventos (con el módulo de provisión instalado)	Además de los flujos de trabajo iniciados por el usuario, el administrador puede configurar flujos de trabajo para que se inicien automáticamente cuando los eventos especificados se produzcan en el repositorio seguro de identidades.
Páginas blancas mejoradas	Permiten mostrar la información del usuario alfabéticamente, geográficamente, por conjuntos de habilidades, etc.
Organigrama corporativo	La aplicación de usuario incluye un portlet de creación de organigramas corporativos avanzado que aprovecha AJAX para proporcionar una amplia experiencia interactiva.
Búsqueda de usuarios	El usuario puede realizar búsquedas en identidades y guardar definiciones de búsquedas personalizadas para volverlas a utilizar más tarde.
Autoservicio de contraseñas	Gracias a esta aplicación los usuarios finales pueden acceder a las funciones de gestión de contraseñas, con lo que se elimina, por tanto, la necesidad de llamar al servicio de asistencia técnica.
Administración de usuarios ligera	La aplicación de usuario permite que los usuarios finales que no sean administradores de TI puedan realizar un conjunto limitado de tareas de gestión de identidades.
Diseñador basado en Eclipse	Los administradores del sistema, desarrolladores, consultores y otros especialistas de TI pueden realizar una serie de tareas, además de las tareas de configuración, de forma rápida y sencilla, mediante la aplicación Diseñador (Designer). Por ejemplo, Designer permite trabajar desconectado con definiciones de entidades y relaciones de entidades, filtros y directivas de controlador y una serie de tareas de configuración del controlador y del conjunto de controladores. Los cambios se pueden guardar en un proyecto y/o cargar en el repositorio seguro de identidades.
Funciones de apoderado (proxy) (con el módulo de provisión instalado)	La interfaz de usuario de la aplicación de usuario permite que el personal con la calificación adecuada, defina funciones de apoderado para usuarios específicos. (Un apoderado puede realizar las tareas de otro usuario, con todos los derechos de ese otro usuario).
Delegación de tareas (con el módulo de provisión instalado)	La interfaz de usuario permite que los supervisores (y los usuarios con los derechos pertinentes) configuren la delegación automática de tareas a compañeros en caso de que un usuario determinado no esté disponible. La delegación puede llegar a tener una gran precisión, ya que se pueden delegar tareas específicas a diferentes personas.

Función	Descripción
Nivel de abstracción del directorio	La estructura del tiempo de ejecución aísla la lógica de la aplicación Web de la mecánica de bajo nivel del acceso al repositorio seguro de identidades y del flujo de trabajo a fin de obtener una arquitectura de abstracción de directorio sólida y segura. El aislamiento se consigue mediante una capa intermedia conocida como nivel de abstracción del directorio (o sólo nivel de abstracción).
Control de acceso en toda la información orientada a usuario	El nivel de abstracción (que aprovecha el sofisticado modelo de derechos vigentes de eDirectory) limita automáticamente tanto la visibilidad de los flujos de trabajo y de los datos de identidad, así como el derecho del usuario a modificar los datos, de modo transparente al usuario e incluso a los mismos portlets.
Verificación de los datos de identidad del usuario final	La aplicación de usuario proporciona un medio para que los usuarios vean y validen/actualicen su propia información de identidad, tal como está representada en el repositorio seguro de identidades.
Registro flexible	Registre fácilmente una amplia variedad de eventos en un registro del servidor (mediante log4j) o en Novell Audit, o en ambos.
Informes de Novell Audit	El producto incluye plantillas predefinidas de Crystal Reports que reflejan las tareas de generación de informes más comunes relativas a la provisión.
Alta disponibilidad	Los elementos del flujo de aprobación y la aplicación de usuario se pueden agrupar en clúster para facilitar la escalabilidad. **Importante:** En esta versión del módulo de provisión, no se admite la migración automática de las instancias del flujo de trabajo en curso. No obstante, en el caso de los flujos en curso que se hayan interrumpido, éstos se podrán continuar hasta finalizar en los nodos de servidor restantes, interviniendo manualmente.
IU de gestión de plantillas de correo electrónico	Asocie y personalice plantillas de correo electrónico para flujos de trabajo mediante iManager.
Portlets accesorios	La aplicación de usuario se entrega con una serie de portlets listos para utilizar, entre ellos portlets para GroupWise, Exchange, Lotus Notes, Web-mail, Network File, NetStorage, HTML, Shortcut, RSS y Message.

Estas funciones se añaden a la funcionalidad estándar del Gestor de identidades. Consulte la guía *Identity Manager Administrator's Guide* (Guía del administrador del Gestor de identidades) para obtener más información sobre el conjunto de funciones estándar del producto.

1.1 Tipos de funciones admitidas

La aplicación de usuario del Gestor de identidades abarca un amplio conjunto de capacidades de gestión de identidades. No todos los usuarios necesitarán utilizar (ni podrán ver) todos los tipos de capacidades; dicha capacidad dependerá de la función de la persona.

Se asume que los usuarios entran en una o varias de las categorías siguientes (cada una utiliza sus propias funciones y herramientas). El vocabulario siguiente se irá utilizando a lo largo de esta documentación.

1.1.1 Administrador de LDAP

El administrador de LDAP es la persona que posee los máximos derechos de administración y configuración del sistema en relación con el repositorio seguro de identidades (eDirectory 8.7.x o 8.8). Se trata de una función lógica que también puede compartir el administrador de la aplicación de usuario (abajo), que es la persona o entidad que posee los derechos del sistema sobre el servidor de aplicación (JBoss), la base de datos (por ejemplo, MySQL) y/o la misma IU Web basada en el portal.

El administrador de LDAP puede elegir entre dos tipos de herramientas para realizar su tarea: el diseñador basado en Eclipse para las tareas poco frecuentes del Gestor de identidades (posiblemente puntuales) y las herramientas de iManager para las tareas de administración diarias.

A continuación, presentamos una serie de ejemplos de tareas poco frecuentes que se pueden realizar con el diseñador para el Gestor de identidades:

- Configurar las definiciones, los atributos y las relaciones del nivel de abstracción que se pueden utilizar en la aplicación de usuario del Gestor de identidades. (Consulte el capítulo Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75 para obtener más información).
- Validar las definiciones del nivel de abstracción del directorio. (Consulte el capítulo Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75).
- Introducir cambios en los valores del controlador de la aplicación de usuario. (Consulte el capítulo Capítulo 3, “Configuración del controlador de la aplicación de usuario”, en la página 57).
- Localizar el texto de visualización de las etiquetas de visualización de atributos y entidades, los nombres de las relaciones del organigrama corporativo y los elementos de la lista global y local. (Consulte el capítulo Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75).
- Importar o exportar el controlador de la aplicación de usuario y sus valores.
- Otros tipos de tareas realizadas sin conexión.

Normalmente, las tareas diarias en las que el administrador (ya sea el administrador de LDAP o el administrador de la aplicación de usuario descrito abajo) trabaja en un sistema activo se efectúan mediante iManager. Entre dichas tareas figuran:

- La gestión de plantillas de correo electrónico.
- La definición o designación de recursos provisionados o de definiciones de peticiones de provisión.

- La habilitación o inhabilitación de una definición de flujo de trabajo, con lo que ésta se activa o desactiva.
- La finalización de un flujo de trabajo en curso.
- La ejecución de informes basados en los datos registrados en Novell Audit.

Algunas de estas tareas (las relacionadas con el flujo de trabajo) sólo se aplican cuando está instalado el módulo de provisión. Además, un gran de número de ellas las puede ejecutar el administrador de la aplicación de usuario (abajo), en lugar del administrador de LDAP.

1.1.2 Administrador de la aplicación de usuario

El administrador de la aplicación de usuario ejecuta tareas asociadas a la gestión de la aplicación Web (la aplicación basada en navegador que se ejecuta en JBoss). El acceso a las herramientas de administración de esta función se produce mediante la pestaña Administración de la interfaz de usuario del Gestor de identidades.

Acciones que puede ejecutar en la aplicación de usuario:

- Configurar varios valores de la aplicación como los que indican a la aplicación de usuario cómo debe conectarse al repositorio seguro identidades (proveedor de LDAP). Para obtener información, consulte Capítulo 10, “Configuración del portal”, en la página 201.
- Determinar las páginas que se muestran en la interfaz de usuario del Gestor de identidades y quién tiene permiso para acceder a ellas. (Consulte Capítulo 7, “Administración de páginas”, en la página 135).
- Determinar los portlets disponibles en la interfaz de usuario del Gestor de identidades y quién tiene permiso para acceder a ellos. (Consulte Capítulo 9, “Administración de portlets”, en la página 179).
- Determinar el aspecto de la interfaz de usuario del Gestor de identidades. (Consulte Capítulo 8, “Configuración de temas”, en la página 173).
- Controlar los niveles de los mensajes de registro que desea que la aplicación de usuario del Gestor de identidades genere y cuáles de dichos mensajes (si los hay) se enviarán a Novell Audit. (Consulte Capítulo 12, “Configuración del registro”, en la página 213).
- Gestionar los diversos cachés que mantiene la aplicación de usuario del Gestor de identidades. (Consulte Capítulo 13, “Configuración del almacenamiento en caché”, en la página 219).
- Exportar o importar contenido Web (páginas y portlets) utilizado en la aplicación de usuario del Gestor de identidades. (Consulte Capítulo 14, “Herramientas para exportar e importar datos del portal”, en la página 229).
- Configurar derechos de apoderado (proxy) para determinadas personas.
- Varias tareas más relacionadas con la interfaz de usuario que el usuario final ve.

Ejemplos de tareas que puede realizar en iManager:

- Gestionar plantillas de correo electrónico.
- Definir o designar recursos provisionados o de definiciones de peticiones de provisión.
- Habilitar o inhabilitar una definición de flujo de trabajo, con lo que ésta se activa o desactiva.
- Terminar un flujo de trabajo en curso.
- Ejecutar informes basados en los datos registrados en Novell Audit.

Algunas de estas tareas (las relacionadas con el flujo de trabajo) sólo se aplican cuando está instalado el módulo de provisión.

1.1.3 Usuario final

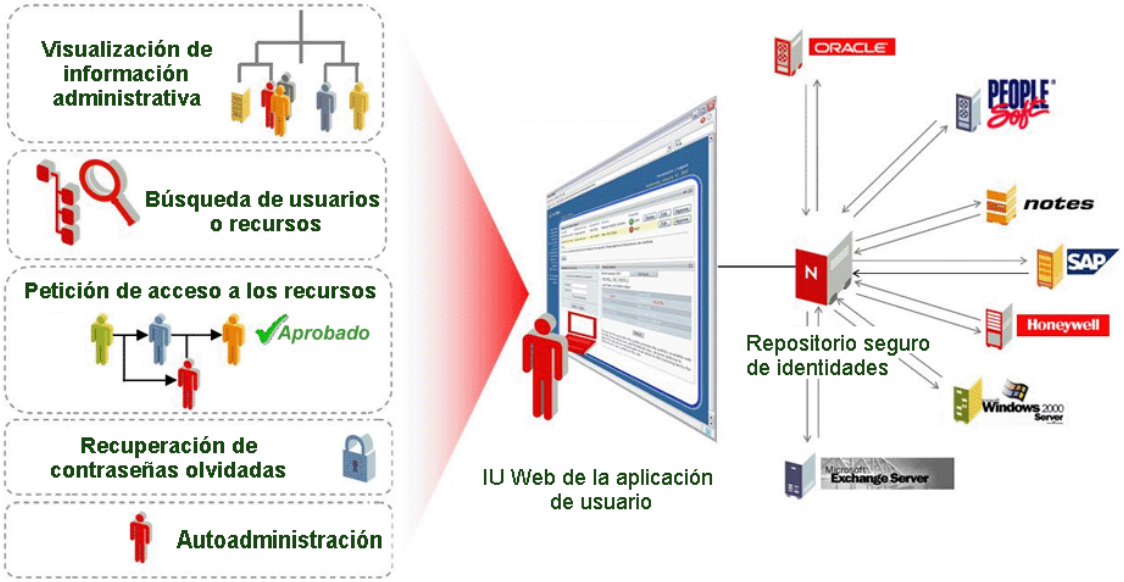
El usuario final es la persona que ve los diversos portlets y páginas Web que forman la interfaz de usuario de la aplicación del usuario e interactúa con éstos. Dentro de este contexto, se entiende que un usuario final es un empleado, un administrador o un apoderado (proxy) o delegado de un empleado o un administrador.

El usuario final potencialmente tiene ante sí una amplia gama de opciones, que dependen de la cantidad de funciones que el administrador haya habilitado. Como mínimo, los usuarios finales podrán utilizar la aplicación de usuario del Gestor de identidades para:

- Ver las relaciones jerárquicas entre los objetos Usuario mediante el portlet del organigrama corporativo.
- Ver y editar información de usuario (con los derechos pertinentes).
- Buscar usuarios o recursos mediante criterios de búsqueda avanzados (que pueden guardarse para volver a utilizarse posteriormente).
- Recuperar contraseñas olvidadas.
- Enviar mensajes de correo electrónico a miembros del equipo (individualmente o en masa).

Además, si se tiene el módulo de provisión instalado, la interfaz Web de la aplicación de usuario permite que los usuarios:

- Pidan un recurso (iniciar uno de los numerosos posibles flujos de trabajo definidos previamente).
- Ver el estado de las peticiones anteriores.
- Reclamar tareas y ver listas de tareas (según recurso, destinatario u otras características).
- Ver asignaciones de apoderados.
- Ver asignaciones de delegados.
- Especificar su disponibilidad (o no disponibilidad).
- Entrar en el modo de apoderado (proxy) para reclamar tareas en nombre de otra persona.
- Ver las tareas del equipo, solicitar recursos del equipo, etc. (sólo los supervisores).



1.1.4 Usuario delegado

Un usuario delegado o un delegado es un usuario final al que se le pueden delegar una o varias tareas específicas (adecuadas a los derechos de dicho usuario), a fin de que pueda trabajar en las mencionadas tareas en nombre de otra persona. Por ejemplo, John se va de vacaciones y desea que Mary se haga cargo de sus tareas mientras está fuera. Si Mary tiene los derechos adecuados para la tarea (o tareas) que John le delega, podrá convertirse en delegada de John. Cuando John indique en la aplicación de usuario que no está disponible, todas las tareas que normalmente aparecerían en la lista de tareas de John, aparecerán en la de Mary. Mary tiene, por lo tanto, la función de usuario delegado. Puede reclamar una tarea de John como si fuera totalmente suya (ya no es tarea de John). Compare esta definición con la de usuario apoderado (proxy) que indicamos más abajo.

Observe que la delegación se produce tarea por tarea. No se trata necesariamente de una transferencia de responsabilidad del tipo "o todo o nada" (aunque en realidad, la interfaz de usuario permite una delegación global de todas las tareas de usuario a un delegado concreto, si así se desea). Un usuario determinado puede designar más de un delegado. Los delegados sólo se pueden responsabilizar de la tarea o tareas que se le han asignado. (Por ejemplo, puede que John desee que Mary se haga cargo de las tareas de petición de las nuevas tarjetas de visita pero quizás desee que Pedro se encargue de las nuevas peticiones de cuentas de Siebel). La transferencia de responsabilidad (reasignación de nuevas tareas) se produce automáticamente cuando el propietario original de la tarea se declara no disponible para un tipo de tarea determinado. (El declarante tiene la posibilidad de especificar un período de caducidad para la delegación, en este caso también tarea por tarea). Esta transferencia se registra por motivos de cumplimiento.

Se puede encontrar una descripción detallada de las características de la interfaz de usuario para los usuarios delegados en el capítulo 1 del manual *Aplicación de usuario del Gestor de identidades: Guía del usuario*. Consulte también Sección 21.3, “Seguridad de la provisión”, en la página 321 en esta guía.

1.1.5 Usuario apoderado (proxy)

Un usuario apoderado (proxy) es un usuario final que actúa como si fuera temporalmente otro usuario y asume temporalmente la identidad de dicho usuario. Todos los derechos del usuario original se aplican al apoderado (proxy). El trabajo que sea propiedad del usuario original seguirá siendo propiedad de dicho usuario. Por ejemplo, mientras John está de viaje por China, desea que su asistente administrativo, Clive, pueda acceder y actuar en todas sus tareas (de John) John (si tiene los derechos pertinentes), puede nombrar a Clive apoderado (proxy). (Si no tiene los derechos adecuados, el administrador de la aplicación de usuario puede definirlos). Una vez se haya establecido la relación de apoderado (proxy), Clive podrá actuar con dos funciones: la función de Clive o la función de John. Si utiliza la función de John, podrá hacer lo mismo que éste. Cuando Clive realice trabajos, será como si John los hubiera realizado.

Observe que, si se compara con el mecanismo de delegación descrito en el apartado anterior, una relación de apoderado (proxy) permite que el usuario apoderado tenga una visibilidad total (y la capacidad de actuar) sobre los valores y tareas del usuario original. Además, mientras dure la función de apoderado (proxy), éste podrá acceder a cualquier atributo, relación o valor del sistema al que John pueda acceder.

Existe otra diferencia entre un delegado y un apoderado (proxy): mientras que un usuario puede delegar algunas tareas en un delegado y otra categoría de tareas en otro delegado, un apoderado (proxy) siempre obtendrá todas las tareas del usuario original. Dicho de otro modo, si nombra a alguien apoderado, dicha persona podrá ver todas sus tareas y trabajar en ellas. Es como si se convirtiera en usted.

Todas las acciones que un apoderado (proxy) lleve a cabo en nombre de otro usuario se registrarán como tales en Novell Audit (para demostrar su cumplimiento).

Puede encontrar información adicional sobre casos de apoderados (proxy) en "Configuración de los valores de provisión" en *Aplicación de usuario del Gestor de identidades: Guía del usuario*.

1.2 Abstracción de datos: la clave para una gestión de identidades flexible

Un concepto clave para comprender la aplicación de usuario del Gestor de identidades es la abstracción de datos o la capacidad para definir, ver y manipular instancias de las definiciones del nivel de abstracción del directorio.

La tecnología tradicional de almacenamiento, ya se trate de bases de datos relacionales, directorios X.500 u otros repositorios, normalmente, requiere que las entradas de datos (filas en una base de datos, objetos en un directorio X.500, etc.) cumplan de forma estricta un esquema bien definido. Las consultas sobre los datos almacenados pueden ser arbitrariamente complejas (en teoría) y los datos pueden incluir índices y/o enlaces en segundo plano, pero se espera que las entradas de datos en sí cumplan una definición fija. Es más, se asume que los esquemas aplicables no experimentarán grandes cambios (si los experimentan) a lo largo del tiempo.

Esto plantea un problema cuando la información (posiblemente con orígenes de datos diferentes y basada en esquemas distintos) debe agruparse para crear objetos de datos compuestos que se adapten al nuevo esquema arbitrario (y posiblemente transitorio). Un ejemplo clásico lo constituyen los datos de identidad, ya que las identidades tienden a ser compuestas y no estáticas. Es más, las piezas de información sobre las que se basa una identidad determinada pueden provenir de orígenes diferentes, cada una de las cuales puede tener administradores que, comprensiblemente, desean proteger la información.

La naturaleza de tipo distribuido de los datos de identidad plantea también problemas de gestión de identidades que difícilmente se pueden resolver mediante definiciones de esquemas rígidas (y vinculadas a la directiva). Una forma de enfrentarse a este problema consiste en reunir los datos de identidad en un repositorio lógico (aplicado como directorio) y agrupar según sea necesario, las identidades lógicas de los datos de origen, en función de uno o varios esquemas lógicos que asignen, por ejemplo, atributos y objetos LDAP tradicionales a atributos y definiciones del nivel de abstracción arbitrario. Así, los datos de identidad se convierten en elementos de alto nivel dinámico y de composición. Cambiar la definición de una identidad no implica que sea necesario introducir cambios en un esquema LDAP. Los objetos Identidad pueden volver a definirse tantas veces como se desee, para adaptarlos a aplicaciones concretas o incluso a usuarios concretos de aplicaciones concretas.

A menudo, se hace referencia a este enfoque general como abstracción de datos, lo que significa que las identidades se materializan según sea necesario y en la forma necesaria.

La abstracción de los datos de identidad aporta una serie de ventajas:

- Se pueden evitar los cambios perjudiciales y potencialmente peligrosos en los esquemas de directorio LDAP.
- La tecnología de abstracción no es intrusiva y no es preciso introducir cambios en los sistemas conectados.
- Se pueden establecer nuevas relaciones entre los datos.
- Las definiciones del nivel de abstracción se pueden cambiar o extender en cualquier momento.
- Los objetos pueden tener la cantidad de atributos que convenga.
- Se pueden fusionar atributos de clases de objetos LDAP no relacionadas en una definición de nivel de abstracción.
- Se pueden utilizar nombres arbitrarios para asignar nombres a atributos (no es obligatorio utilizar nombres LDAP).
- La directiva de control de acceso muy precisa sigue vigente (los usuarios sólo ven los datos que tienen derecho a ver).
- Pueden efectuarse búsquedas complejas en tipos de objetos nuevos (o combinaciones de atributos) que serían imposibles de efectuar en un entorno que sólo fuera de LDAP.

El Gestor de identidades aprovecha la abstracción para conseguir todos estos objetivos y mucho más.

1.3 Descripción arquitectónica de alto nivel

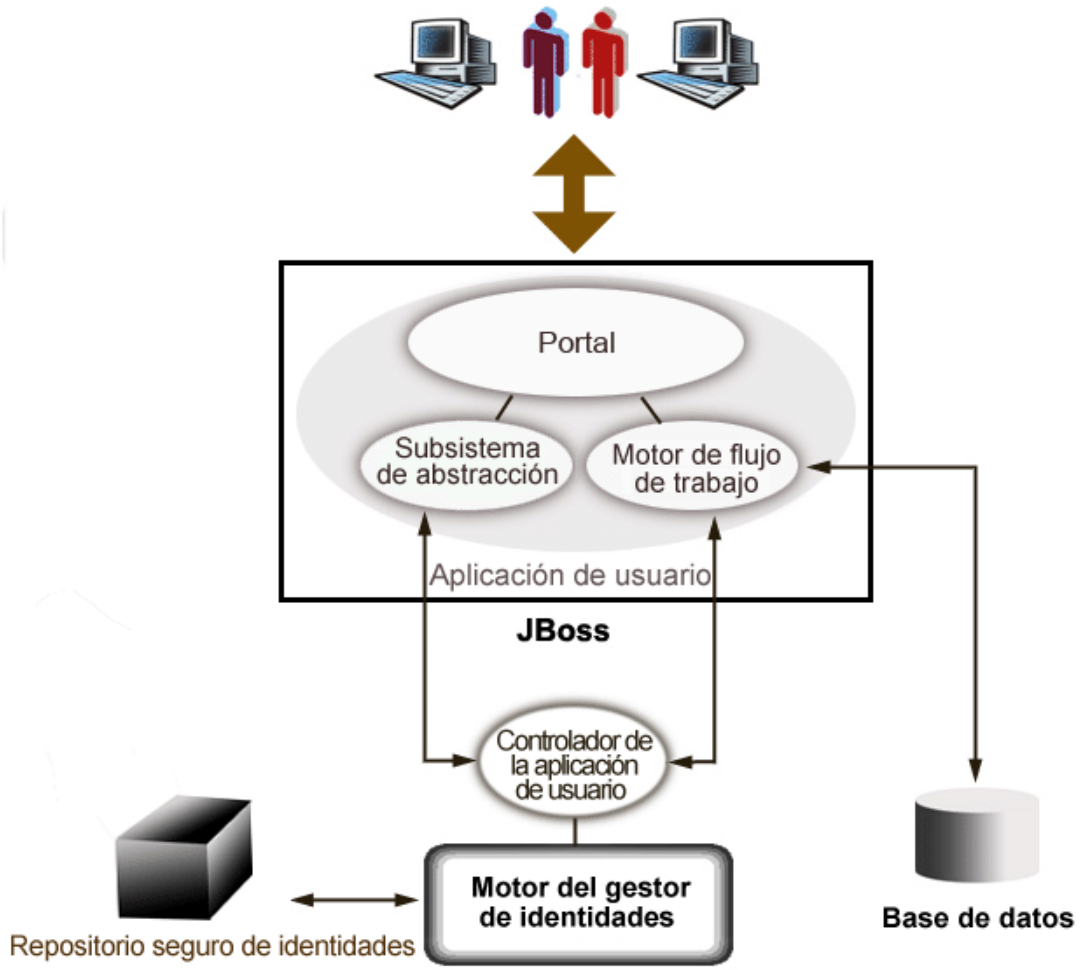
La aplicación de usuario del Gestor de identidades se basa en una serie de componentes independientes que interactúan. En la tabla siguiente se describen los componentes básicos, así como sus responsabilidades fundamentales.

Componente	Descripción
Repositorio seguro de identidades (eDirectory 8.7.3 ó 8.8)	Repositorio de datos del usuario (así como de otros datos de identidad) más controladores y conjunto de controladores de IDM, así como de diversos artefactos del nivel de abstracción y, si el módulo de provisión está instalado, de artefactos de flujo de trabajo.

Componente	Descripción
Motor del Gestor de identidades	Estructura del tiempo de ejecución en el Gestor de identidades que monitoriza los eventos en eDirectory (y los sistemas conectados), aplica las directivas y encamina los datos desde o hasta el repositorio seguro de identidades.
Controlador de la aplicación de usuario	El controlador de la aplicación de usuario se comunica con la aplicación de usuario para permitir que ésta actualice su caché cuando las definiciones del nivel de abstracción han cambiado. Cuando el módulo de provisión está instalado, el controlador de la aplicación de usuario también se puede configurar para permitir que eventos del repositorio seguro de identidades inicien flujos de trabajo. Asimismo, comunica información relativa a derechos al repositorio seguro de identidades para que se registre el derecho que se otorga (o no) cuando finaliza el flujo de trabajo.
Aplicación de usuario: IU Web	La IU Web de la aplicación de usuario es una aplicación Java basada en navegador a la que se conectan los portlets compatibles con JSR 168.
Aplicación de usuario: nivel de abstracción	El nivel de abstracción aísla la lógica del nivel de presentación del repositorio seguro de identidades, a fin de que todas las peticiones de datos de identidad tengan que pasar por el nivel de abstracción. El código de los portlets no puede obtener un acceso directo a la información de identidad. Todas las peticiones pasan por el nivel de abstracción y están sujetas a sus restricciones (por ejemplo, en el control de acceso).
Aplicación de usuario: motor del flujo de trabajo (disponible únicamente con el módulo de provisión)	El motor del flujo de trabajo es un conjunto de archivos ejecutables Java encargado de gestionar y ejecutar los pasos de un flujo de trabajo definido por el administrador.
Servidor de aplicación JBoss	El servidor de aplicación JBoss de código abierto proporciona la estructura de tiempo de ejecución en la que se ejecutan la aplicación de usuario, el nivel de abstracción y el motor del flujo de trabajo.
Base de datos (por defecto, MySQL)	La base de datos (consulte la guía de instalación para ver una lista de las bases de datos admitidas) almacena determinados tipos de información de configuración en nombre de la aplicación de usuario, así como el estado del flujo de trabajo (si el módulo de provisión está instalado).
Controlador del servicio Composer	El controlador del servicio Composer es la parte del controlador de la aplicación de usuario que se puede configurar de forma personalizada para responder a los eventos del repositorio seguro de identidades mediante el inicio de flujos de trabajo.
Novell Audit	Novell Audit es un servidor de registro independiente que puede conservar una serie de tipos de datos (como datos generados por pasos de un flujo de trabajo). Para obtener más información, consulte más adelante el capítulo relativo a cómo configurar el registro.

En términos de flujo de la información, los componentes mencionados anteriormente están vinculados entre sí lógicamente tal como se muestra en el esquema siguiente. Desde un punto de vista físico, los componentes individuales pueden estar ubicados (y así ocurrirá en muchos casos) en

más de una máquina. Por ejemplo, aunque el repositorio seguro de identidades (y su principal herramienta de administración, iManager) se encuentren en la máquina que alberga el motor del Gestor de identidades, JBoss (y la aplicación de usuario), normalmente, estarán en otra máquina (o grupo de máquinas, si se agrupan en clúster). Asimismo, por motivos no sólo de rendimiento, sino también de seguridad y de recuperación tras fallos, la base de datos (MySQL) estará en su propia máquina.



1.3.1 Repositorio seguro de identidades

El repositorio seguro de identidades se utiliza para almacenar datos de identidades y definiciones de nivel de abstracción de diversos tipos. Con este fin, se utiliza una instancia de eDirectory (que se ejecuta en Windows, Solaris o Linux). Mediante eDirectory, el Gestor de identidades puede aprovechar el directorio LDAPv3 corporativo, ampliable masivamente y de eficacia demostrada con funciones de partición y réplica, más una herramienta de configuración y gestión flexible basada en Web (iManager) que ofrece un punto de integración administrativa todo en uno entre el Gestor de identidades y el mismo eDirectory.

1.3.2 JBoss

La aplicación de usuario está empaquetada como un archivo de la aplicación Web Java o un archivo WAR. El archivo WAR se implanta en JBoss, el conocido servidor de aplicación Java de código abierto (que utiliza Tomcat como motor servlet; no se muestra en el esquema). El uso de JBoss como entorno de ejecución aporta un gran número de ventajas, incluidas las siguientes:

- El código fuente está disponible gratuitamente.
- A partir de la versión 4.0.3, JBoss puede agruparse en clúster.
- JBoss es totalmente compatible con J2EE, lo que significa que cualquier aplicación J2EE puede ejecutarse en él. Se pueden albergar aplicaciones adicionales (por ejemplo, Servicios Web) en la misma instancia de JBoss en la que se ejecutan las aplicaciones del usuario.
- JBoss admite los servicios de autorización y seguridad JACC y JAAS estándar de Java (en los que se basa la aplicación de usuario para el acceso al repositorio seguro de identidades).
- JBoss se ejecuta en varias plataformas diferentes, entre las que figuran las conocidas versiones de Windows y Linux.

El archivo WAR de la aplicación de usuario contiene código ejecutable para la aplicación de usuario que, a su vez, se genera utilizando una arquitectura MVC (Modelo-Vista-Controlador), para separar temas. Las interfaces de usuario se ejecutan como portlets modulares dentro de la aplicación de usuario. Existen diferentes portlets para ver organigramas corporativos, realizar búsquedas, ver detalles del usuario, restaurar contraseñas, etc.

Para obtener más información acerca de los diversos aspectos de la implantación de aplicaciones Web en JBoss, consulte la documentación de JBoss en http://www.jboss.org/products/jbossas/docs (http://www.jboss.org/products/jbossas/docs).

1.3.3 Base de datos

La aplicación de usuario se basa en una base de datos (por defecto, MySQL; consulte la guía de instalación para ver una lista de las bases de datos admitidas) para almacenar varios tipos de información.

- Datos de la configuración de la aplicación de usuario: por ejemplo, definiciones de páginas Web, registros de instancias de portlets y valores preferidos.
- Si el módulo de provisión está instalado, se conserva la información de estado del flujo de trabajo en la base de datos. Las definiciones de flujo de trabajo reales se almacenan en el repositorio seguro de identidades.
- Registros de Novell Audit

1.3.4 Motor del Gestor de identidades

El Gestor de identidades está formado por un motor del tiempo de ejecución, controladores y directivas. El motor del Gestor de identidades responde a los eventos del repositorio seguro de identidades y gestiona el flujo y la transformación de los datos que van o vienen del repositorio. Los objetos Controlador encapsulan el código ejecutable y artefactos (como documentos de directivas) diseñados para proporcionar comportamientos de manejo de datos específicos de un sistema conectado concreto. La aplicación de usuario del Gestor de identidades es un sistema conectado. La comunicación entre el repositorio seguro de identidades, el nivel de abstracción de la aplicación de

usuario y el motor del flujo de trabajo se produce a través del controlador de la aplicación de usuario (véase abajo).

Dado que la aplicación de usuario se basa en varios objetos del directorio para almacenar artefactos de nivel de abstracción, es preciso extender el esquema de eDirectory para que albergue los objetos LDAP personalizados y los atributos que la aplicación de usuario necesita. La extensión del esquema se produce automáticamente como parte del proceso de instalación del Gestor de identidades. No obstante, la cumplimentación de los atributos y objetos personalizados con valores por defecto no se producirá hasta que se instale y active el controlador de la aplicación de usuario.

1.3.5 Controlador de la aplicación de usuario

El controlador de la aplicación de usuario es una pieza de habilitación importante de la aplicación de usuario. Una de las responsabilidades del controlador de la aplicación de usuario consiste en notificar al nivel de abstracción que han cambiado valores de datos importantes en el repositorio seguro de identidades, a fin de que el nivel de abstracción sepa que tiene que actualizar su caché.

Si el módulo de provisión está instalado, el controlador de la aplicación de usuario puede configurarse para que inicie automáticamente flujos de trabajo como respuesta a los cambios efectuados en los valores de los atributos en el repositorio seguro de identidades.

El controlador de la aplicación de usuario no sólo es un componente de tiempo de ejecución, sino también una empaquetadora de almacenamiento de objetos del directorio (incluidos los artefactos de tiempo de ejecución de la aplicación de usuario). A continuación, mostramos una representación habitual de los artefactos del directorio asociados al controlador de la aplicación de usuario.

Nota: Los nombres mostrados representan valores de nombre común (cn) de LDAP. La denominación de esquema real de las diversas clases de objetos se trata en otro punto.

Estas categorías de artefactos se tratan abajo más detalladamente.

Objeto Conjunto de controladores

En todas las instalaciones del Gestor de identidades es preciso que los controladores se agrupen en conjuntos. Sólo puede haber un conjunto de controladores activo a la vez (en un servidor de directorios determinado). Los controladores de dicho conjunto se pueden activar o desactivar individualmente, sin que ello repercuta sobre el conjunto de controladores en general. El controlador de la aplicación de usuario (al igual que cualquier otro controlador IDM) debe existir dentro de un conjunto de controladores. La aplicación de usuario no crea automáticamente el conjunto de controladores; es preciso crear un conjunto de controladores con anterioridad y, después, crear el controlador de la aplicación de usuario dentro de éste.

Controlador de la aplicación de usuario

El objeto Controlador de la aplicación de usuario (al que se puede asignar un nombre de forma arbitraria) contiene una serie de artefactos. Al igual que ocurre con todos los controladores del Gestor de identidades, el controlador de la aplicación de usuario aplica directivas y objetos de canal Suscriptor y Editor. La aplicación de usuario no utiliza el canal Editor, aunque está disponible para utilizar en caso de personalización.

Objeto AppConfig

El objeto AppConfig es un contenedor de diversos objetos de configuración de la aplicación de usuario:

RequestDefs

Contenedor de definiciones de peticiones de provisión; es decir, contiene las definiciones de peticiones configuradas por el administrador disponibles para el tiempo de ejecución de la aplicación de usuario (si el módulo de provisión existe). Las definiciones almacenadas aquí (como XML) representan las clases de peticiones de las que los usuarios finales que tengan los derechos adecuados pueden crear instancias mediante la aplicación de usuario. RequestDef asocia un WorkFlowDef (abajo) con un ResourceDef.

WorkFlowDefs

Contenedor para objetos Flujo de trabajo, incluidos descripciones de tiempo de diseño y cualquier plantilla o flujo sin utilizar.

ResourceDefs

Contenedor para definiciones de recursos provisionados, incluidos descripciones de tiempo de diseño y cualquier plantilla o destino sin utilizar.

ServiceDefs

Contenedor para objetos de definición de servicios, que empaquetan los Servicios Web llamados por los Flujos de trabajo.

DirectoryModel

Objetos de metanivel del nivel de abstracción (ChoiceDefs, EntityDefs, RelationshipDefs), que representan diferentes tipos de contenido (algunos definibles por el usuario, otros definidos por el administrador) del directorio y que los portlets de identidad pueden exponer.

AppDefs

Contenedor de objetos Configuración utilizado para inicializar el entorno de tiempo de ejecución como, por ejemplo, la información de configuración del caché y las propiedades de las notificaciones por correo electrónico.

ProxyDefs

Contenedor de definiciones de apoderados (proxy).

DelegateeDefs

Contenedor de definiciones de delegados.

1.3.6 Nivel de abstracción del directorio

Los portlets obtienen los datos de identidad mediante consultas efectuadas al nivel de abstracción del directorio, que es un nivel de código que aísla los detalles de acceso de los datos de identidad de los procesos cliente. Cuando, por ejemplo, un portlet necesita efectuar una búsqueda en datos de identidad, el nivel de abstracción efectúa, en nombre del portlet, las consultas LDAP adecuadas en el contenedor de destino del repositorio seguro de identidades. En ningún momento, ningún portlet efectúa consultas directas en el repositorio seguro de identidades.

El nivel de abstracción es también el nivel de código a través del cual se crean o cambian las definiciones del nivel de abstracción, tal como las especifican los administradores u otros usuarios cualificados del sistema. Para efectuar tales cambios, el experto en sistemas utiliza el editor del nivel de abstracción del directorio de la aplicación del diseñador, descrita más adelante en esta guía, en Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

En el momento de ejecución, el nivel de abstracción almacena en caché una serie de datos de definición de entidades y de configuración obtenidos del repositorio seguro de identidades. El administrador puede gestionar con gran precisión los diversos cachés que mantiene la aplicación de usuario. Para obtener información adicional acerca de cachés y de gestión de cachés, consulte Capítulo 13, “Configuración del almacenamiento en caché”, en la página 219.

1.3.7 Motor del flujo de trabajo

El motor del flujo de trabajo (disponible con el módulo de provisión) es el conjunto de clases de tiempo de ejecución responsable de ejecutar los pasos de un flujo de trabajo, tal como están especificados en una definición de proceso (un artefacto de tiempo de ejecución creado cuando se crea una instancia de un flujo de trabajo) y de realizar el seguimiento de la información de estado, que se conserva en una base de datos como MySQL u Oracle; consulte Sección 1.3.3, “Base de datos”, en la página 24, arriba.

Encontrará información adicional acerca del sistema de flujo de trabajo, incluido cómo crear flujos de trabajo, más adelante, en el capítulo llamado Capítulo 21, “Introducción a la provisión basada en el flujo de trabajo”, en la página 311 de esta guía.

1.3.8 Interfaz de usuario

La interfaz de usuario del Gestor de identidades está formada por un conjunto de portlets que cumplen con SR168 (y, en el caso del módulo de provisión, algunas páginas de servidor Java), que se ejecutan dentro de unas aplicaciones Web Java en JBoss. La arquitectura de portlets permite un

alto grado de modularidad, personalización de contenido y control de usuario sobre el aspecto de las páginas. La estructura de la aplicación de usuario proporciona servicios de contenedor de diversos tipos. Gestiona el estado de la ventana, las preferencias de los portlets, la consolidación, el almacenamiento en caché, los temas, los registros, etc. y actúa como vigilante de seguridad. Por su parte, el servidor de aplicación en el que se ejecuta la aplicación de usuario proporciona diversos servicios a la aplicación en general como, por ejemplo, la capacidad de ampliación mediante la agrupación en clúster, el acceso a la base de datos a través de JDBC y el soporte para la seguridad basado en certificados.

El alto grado de encapsulación que permite esta arquitectura proporciona un entorno de presentación sólido y seguro para la aplicación de usuario del Gestor de identidades. Asimismo, garantiza un alto grado de control administrativo sobre todos los aspectos de la interfaz de usuario.

Para obtener más información acerca de cómo administrar las diversas partes de la interfaz de usuario, consulte varios capítulos de esta guía en Parte III, “Administración de la aplicación de usuario”, en la página 127.

1.4 Herramientas de diseño y configuración

Varias funciones de la aplicación de usuario del Gestor de identidades se pueden personalizar o configurar de forma personalizada mediante la herramienta de Diseñador del Gestor de identidades (basada en Eclipse Rich Client Platform) o mediante módulos auxiliares (plug-in) de iManager.

En la tabla siguiente se describen las herramientas disponibles y sus usos.

Herramienta	Objetivo
Designer para el Gestor de identidades	Herramienta de configuración general del Gestor de identidades, que permite que el desarrollador, el consultor o el administrador del sistema puedan realizar cambios de configuración precisos en los conjuntos de controladores, los controladores, las definiciones de directivas y otros artefactos.
Módulo auxiliar del Editor del nivel de abstracción del directorio para el Diseñador	Permite definir relaciones y objetos personalizados y efectuar cambios en distintos valores de configuración del nivel de abstracción. Consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75 más adelante en esta guía.
Módulo auxiliar de configuración de peticiones de provisión	Permite definir y configurar los tipos de petición de provisión disponibles (en iManager).
Editor de recursos provisionados (disponible en breve)	Módulo auxiliar del diseñador que permite crear y configurar recursos (objetos que representan el recurso que se otorgará como respuesta a un flujo de trabajo).
Editor de definiciones de flujos de trabajo (disponible en breve)	Módulo auxiliar de definición de flujos de trabajo gráfico para el diseñador.
Editor de plantillas de correo electrónico del flujo de trabajo	Módulo auxiliar de iManager que permite a los administradores añadir, suprimir y editar plantillas de correo electrónico. El sistema de flujo de trabajo puede utilizar dichas plantillas para notificar a los usuarios los eventos del flujo de trabajo.

Herramienta	Objetivo
lreport.exe (herramienta de informes de registros) y la función de registro y auditoría de iManager	Existe una serie de informes de registros definidos previamente (que se entregan con el Gestor de identidades) disponibles en formato de Crystal Reports (.rpt) para filtrar los datos registrados en la base de datos de Novell Audit. La herramienta de informes de registros **lreport.exe** (sólo en Windows) es una forma de generar los informes. También se pueden utilizar otros métodos para generar los informes; consulte Capítulo 5, “Configuración de las entradas”, en la página 119 para obtener información.

Normalmente, un experto en diseño de sistemas empieza por utilizar el editor del nivel de abstracción del directorio (en el diseñador en el caso del Gestor de identidades) para configurar las definiciones del nivel de abstracción personalizado para la aplicación de usuario. A continuación, dichos objetos pasan a estar disponibles para que el nivel de abstracción los utilice (y, por consiguiente, los usuarios de la interfaz de usuario). Los valores de configuración precisos del control de acceso pueden ejercitarse en la definición y el uso de esos objetos para que el administrador y los usuarios finales puedan ver y manipular únicamente los objetos (y los atributos de los objetos) sobre los que tienen los derechos adecuados.

Si el módulo de provisión está instalado, el experto en diseño de sistemas o el administrador pueden utilizar los asistentes de configuración de las peticiones de provisión en iManager para definir los recursos provisionados y los flujos de trabajo que estarán disponibles para los usuarios de la aplicación de usuario. Al mismo tiempo, el administrador puede utilizar las funciones del editor de plantillas de correo electrónico (en iManager) para definir el contenido del cuerpo de las notificaciones de correo electrónico que los flujos de trabajo enviarán. Consulte Capítulo 23, “Gestión de los flujos de trabajo de provisión”, en la página 347 para obtener más información sobre este tema.

Una vez configurados el nivel de abstracción, las definiciones de petición de provisión, los requisitos de auditoría y las plantillas de correo electrónico, por lo general, el administrador efectuará varias operaciones de configuración relativas a la aplicación de usuario (funciones de seguridad, caché, etc.) utilizando las funciones de administración descritas en Capítulo 10, “Configuración del portal”, en la página 201. Por último, el administrador configurará los portlets individuales necesarios, mediante las interfaces descritas en los distintos capítulos que se encuentran en la parte IV de esta guía.

Nota: En el capítulo siguiente se describen con mayor detalle algunas tareas que se recomienda consultar antes de crear un entorno de producción.

1.5 Ejemplos de utilización

La aplicación de usuario del Gestor de identidades dispone de un gran número de funciones. A continuación, presentamos algunos ejemplos para dar una breve visión de las diversas formas en que se puede utilizar la aplicación de usuario para solucionar problemas de la vida real.

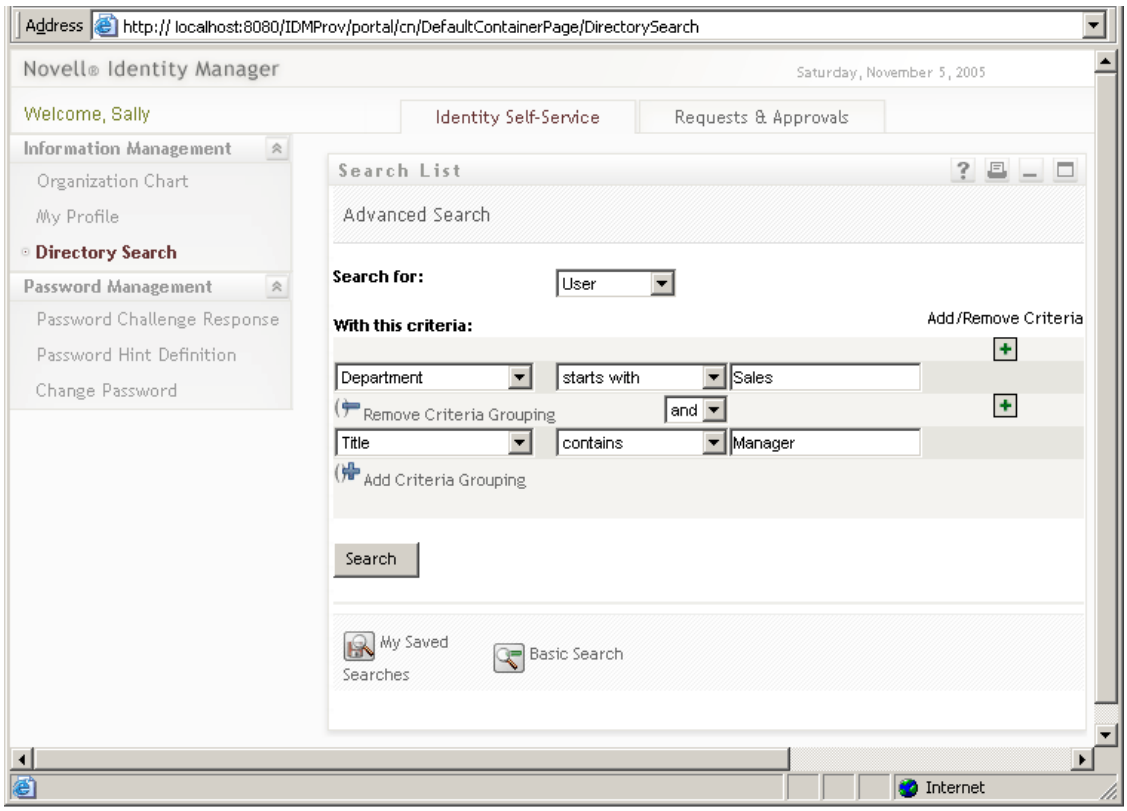
1.5.1 Ejemplo A: el usuario busca información relativa a otras personas de la organización.

Es habitual que un empleado desee encontrar información acerca de otra persona de la organización. Por ejemplo:

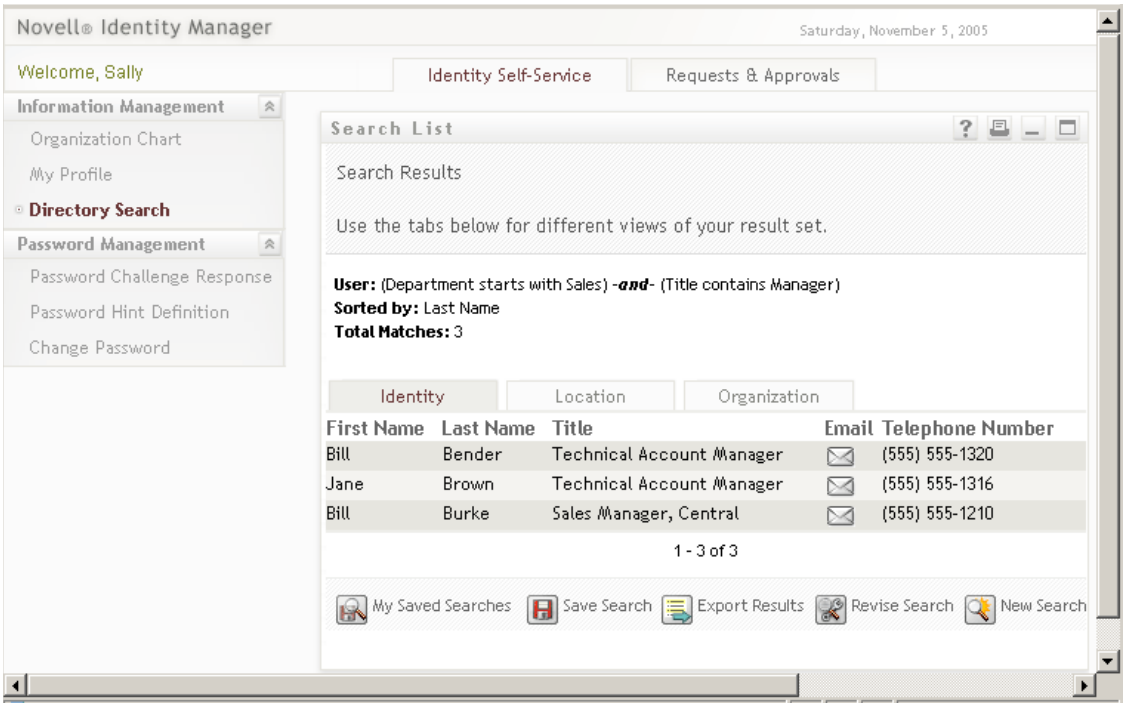
- Obtener el nombre completo de un compañero de trabajo y su información de contacto.
- Encontrar todas las personas que posean unos determinados conocimientos dentro de un área geográfica.
- Determinar quién es el supervisor de una persona en concreto.

Estos tipos de operaciones (incluidas las búsquedas más avanzadas basadas en consultas complejas) pueden efectuarse fácilmente mediante la interfaz de búsqueda en el Directorio. Normalmente, el usuario final entrará en la aplicación de usuario y activará la pestaña Autoservicio de identidades (si no lo está) y, a continuación, hará clic en el enlace Búsqueda en el Directorio en los enlaces de navegación de la columna situados a la izquierda.

En la pantalla siguiente, el usuario que ha entrado ha configurado una búsqueda avanzada para buscar todos los usuarios cuyo departamento empiece por `Sales` y cuyo `cargo` contenga la palabra Manager.



Cuando la búsqueda haya acabado, aparecerá una pantalla de resultados similar a la siguiente:

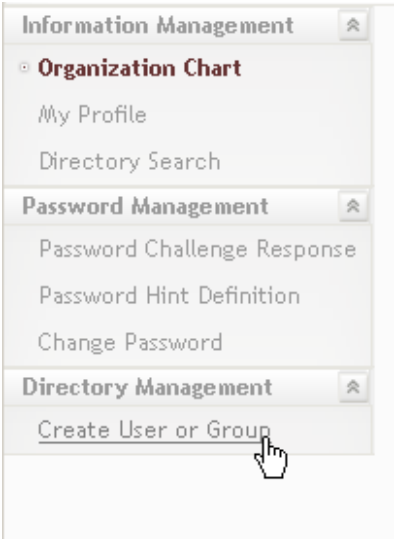


Observe la fila de botones situados en la parte inferior; estos botones permiten que el usuario guarde esa consulta avanzada concreta, modifique la consulta, vuelva a empezar con otra consulta, etc. Asimismo, observe las pestañas situadas sobre la lista de los individuos localizados. Los individuos se indican por identidad, aunque también se pueden mirar según la ubicación o la organización utilizando la pestaña adecuada.

1.5.2 Ejemplo B: El supervisor crea un nuevo usuario.

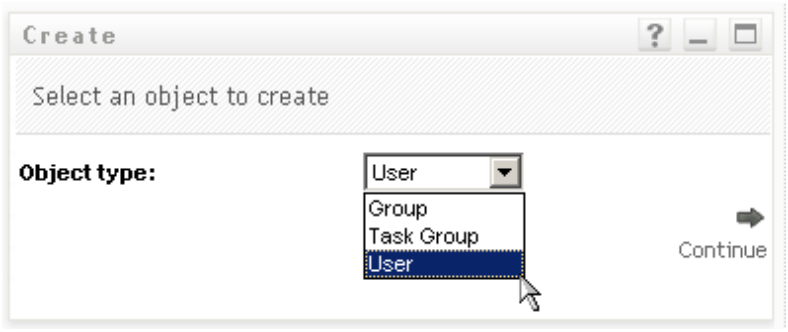
Supongamos que un departamento de una empresa haya contratado a un nuevo empleado en prácticas, un subcontratado u otra persona que no sea empleado (para que trabaje en la empresa sólo durante un corto período de tiempo). Esa nueva persona deberá estar en el sistema a fin de que pueda disponer de un conjunto de recursos limitado apropiado (y para que también se la pueda localizar mediante búsquedas de usuario como la que hemos descrito anteriormente). Dado que dicha persona no es un empleado habitual, no formará parte del sistema de recursos humanos normal de la empresa. No obstante, la identidad de dicha persona (y el acceso a los recursos) deberán gestionarse de forma segura.

Como supervisor del departamento en cuestión, tiene permiso para introducir usuarios en el sistema. Para ello, debe entrar y ver que hay un enlace de creación de usuarios o de grupos en la columna de los enlaces de navegación situada a la izquierda de la página (véase más abajo):

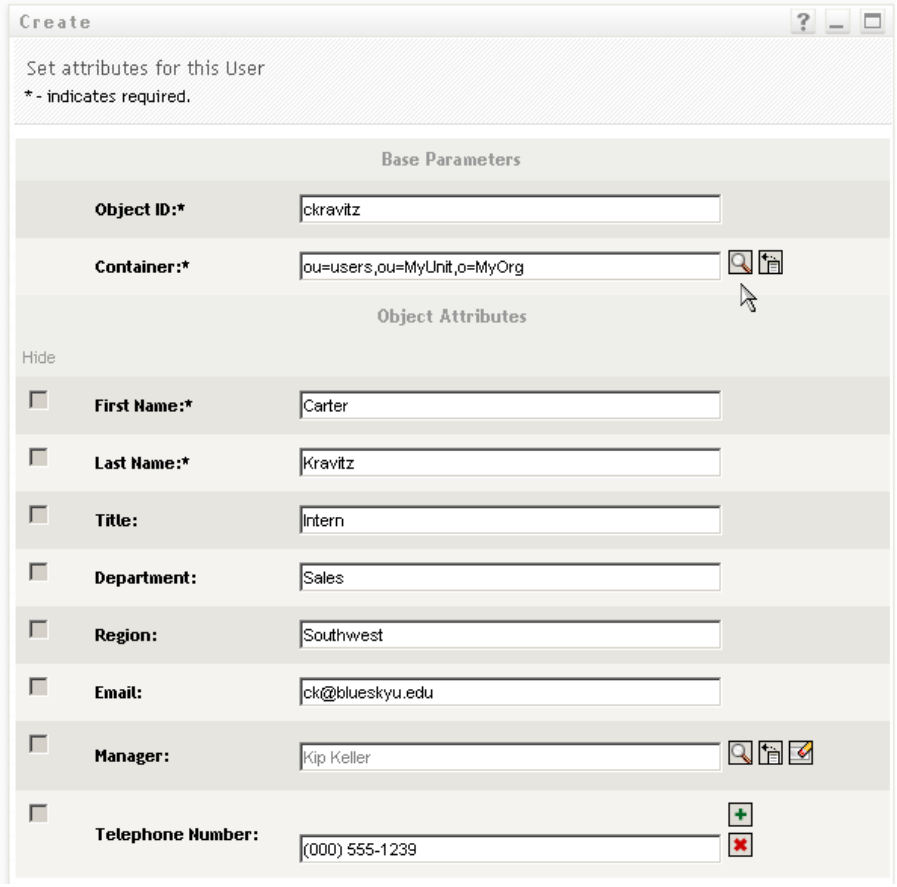


Nota: Este enlace no aparecerá a menos que el usuario que haya entrado disponga de los derechos adecuados.

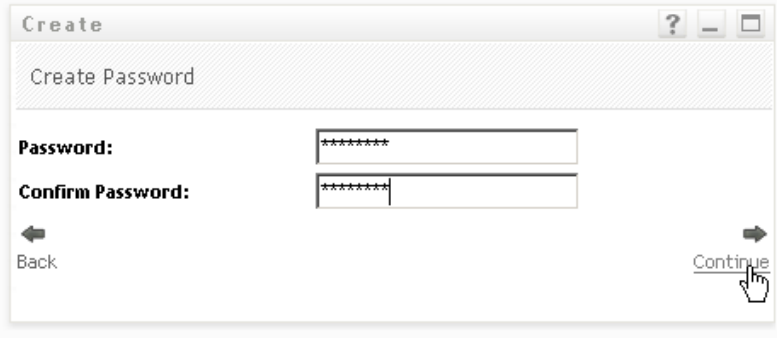
Después de hacer clic en el enlace, aparece una pantalla em la que se le pregunta si desea crear un nuevo grupo, un grupo de tareas o un usuario (tal como se muestra abajo).



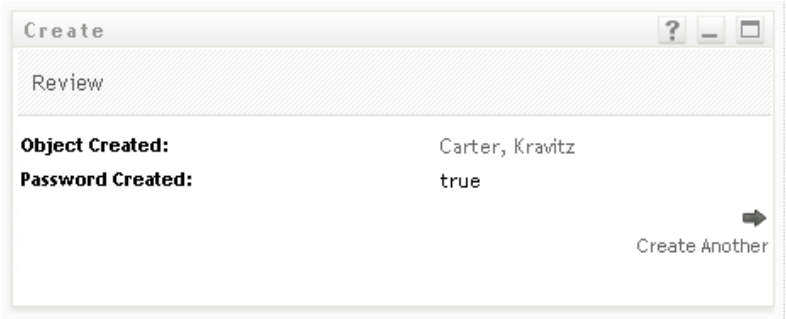
Después de seleccionar Usuario y hacer clic en Continuar, el siguiente panel del asistente le permitirá introducir la información personal del usuario:



La pantalla siguiente le permitirá asignar una contraseña al nuevo usuario:



La pantalla final muestra el resultado neto del proceso.



En este ejemplo, la persona que acaba de llegar se convierte en un usuario con todos los derechos de un usuario normal. Aunque también es posible, por ejemplo, definir un objeto Persona en prácticas, utilizando el editor del nivel de abstracción del directorio, que posea atributos y derechos únicos adecuados estrictamente a dicho tipo de objeto. En tal caso, `Persona en prácticas` se mostrará como una de las opciones de la primera lista de elección, junto con Grupo, Grupo de tareas y Usuario.

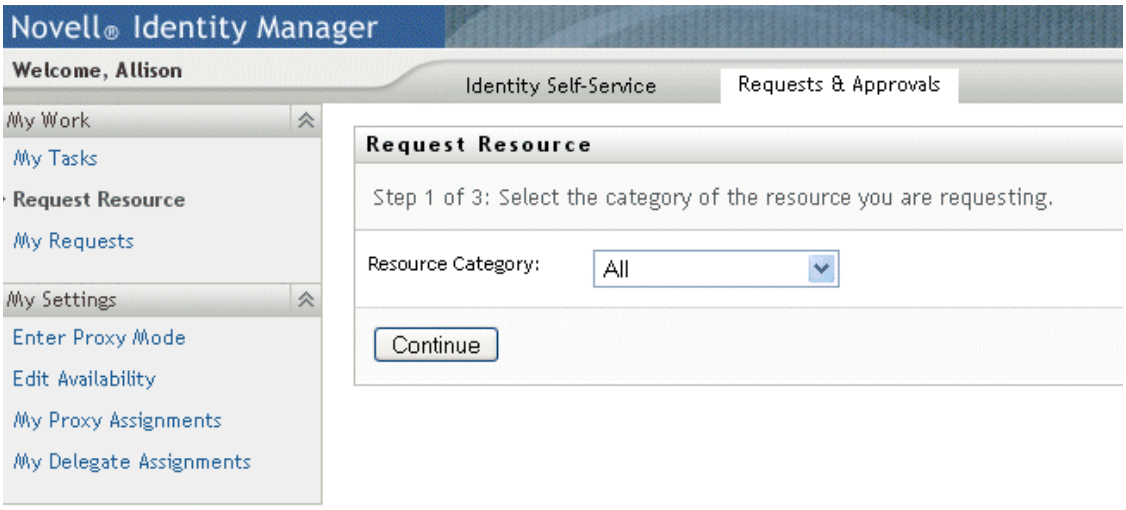
1.5.3 Ejemplo C: Provisión de usuario

A menudo, se da el caso de que un empleado necesita obtener un recurso (por ejemplo, algún tipo de equipamiento de oficina, una tarjeta de crédito de la empresa o el acceso a una base de datos) que necesita la aprobación de otra persona. Esta situación se conoce como petición de provisión. En el Gestor de identidades, si el módulo de provisión está instalado y configurado, dichas peticiones pueden atenderse mediante flujos de trabajo.

Nota: A diferencia de los ejemplos anteriores, en este ejemplo se necesita que el módulo de provisión esté instalado y configurado.

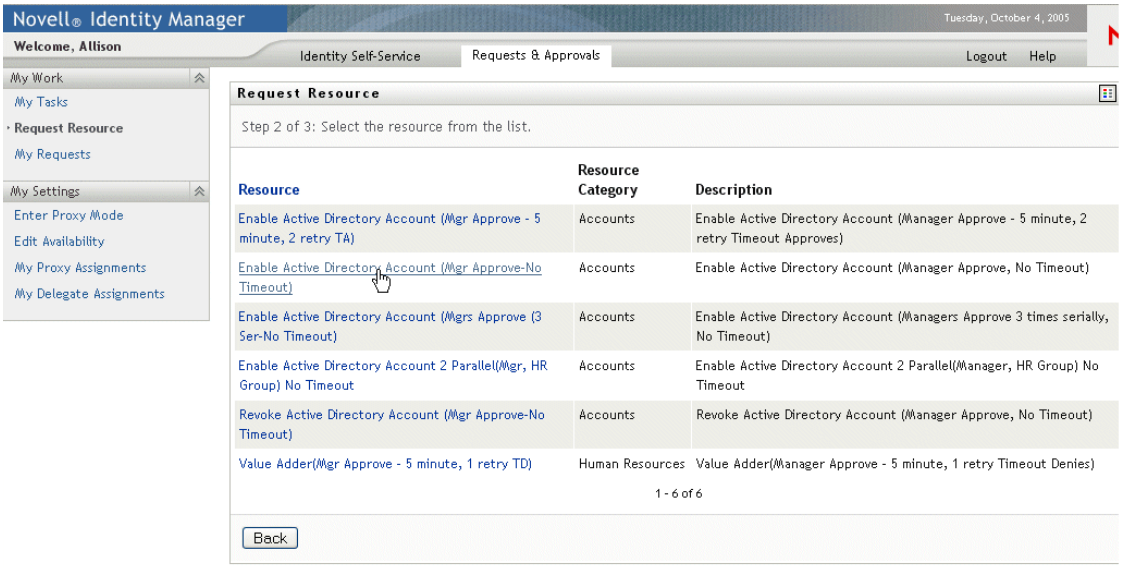
Primero, el usuario tiene que entrar en la aplicación de usuario para llegar a su propia página. En la parte superior de dicha página, el usuario deberá hacer clic en la pestaña *Peticiones y aprobaciones* y, a continuación, localizar el enlace *Petición de recurso* situado en el marco de navegación del lado

izquierdo. Al hacer clic en el enlace *Petición de recurso*, la aplicación de usuario muestra el formulario de petición inicial.



El menú desplegable Categoría de recurso puede contener varios tipos de recursos como, por ejemplo, derechos con nombres arbitrarios. (Consulte la guía de administración principal del Gestor de identidades para obtener más información acerca de los derechos y de cómo se crean). Para ver todos los recursos provisionados (dicho de otra forma, cualquier cosa que ese usuario en concreto con sus derechos pueda solicitar), sólo es preciso seleccionar `Todos`, tal como se indica.

Si el usuario elige continuar, la pantalla siguiente mostrará todos los tipos de peticiones de provisión sobre las que ese usuario tiene permiso de acceso.



En este ejemplo, el usuario desea solicitar una cuenta de Active Directory y, para ello, necesita la aprobación de su supervisor. Sólo con hacer clic en el enlace adecuado y cumplimentando un sencillo formulario, se iniciará el flujo de trabajo asociado y el supervisor de dicha persona recibirá

una notificación por correo electrónico adecuada a la tarea que necesita ejecutar. El supervisor, por su parte, puede entrar en su página *Peticiones y aprobaciones* y encontrar la petición del empleado esperando en su lista de tareas, preparada para que la apruebe o la rechace. (Si el supervisor está de vacaciones, se notificará al apoderado [proxy] que haya nombrado y éste podrá actuar tal como lo hubiera hecho el supervisor del empleado). Mientras tanto, la pantalla del navegador cambiará para mostrar una página de resumen que confirma que la petición de flujo de trabajo se ha enviado correctamente.

Otorgar una cuenta en el directorio de una empresa (tal como se muestra aquí) es un ejemplo de una petición de derecho. Se pueden configurar varios tipos de peticiones de derecho en la aplicación de usuario del Gestor de identidades, así como crear varios tipos de flujos de trabajo (con aprobación de uno o varios supervisores, de flujo en serie o de flujo paralelo, con o sin tiempos límite, etc.). En todos los casos, se dispone de un control de acceso preciso para gestionar la visibilidad de los flujos de trabajo y otra información.

En los últimos capítulos de esta guía encontrará más información acerca de estas funciones. (La información proporcionada en dichos capítulos es principalmente de interés para los administradores. El uso de las funciones se describe con más detalle en la guía del usuario de la aplicación del Gestor de Identidades:

1.6 Adónde ir a continuación

Si está dispuesto a aprender más sobre el diseño de un entorno de producción, vaya al capítulo siguiente (Capítulo 2, “Diseño del entorno de producción”, en la página 39). O bien, es posible que le interese ir directamente a uno de los capítulos posteriores de este manual para consultar los tipos de información siguientes:

Para obtener más información acerca de las *capacidades de auditoría o registro* de la aplicación de usuario, consulte Capítulo 5, “Configuración de las entradas”, en la página 119.

Para obtener más información acerca de la personalización del *aspecto de la interfaz de usuario*, consulte Capítulo 8, “Configuración de temas”, en la página 173.

Para obtener más información acerca de la *seguridad* tal como se administra a través de la interfaz administrativa de la aplicación de usuario (en comparación con iManager), consulte Capítulo 11, “Configuración de la seguridad”, en la página 209.

Para obtener más información acerca de las opciones de *gestión del caché* de la aplicación de usuario, consulte Capítulo 13, “Configuración del almacenamiento en caché”, en la página 219.

Para obtener más información acerca de las funciones de la *gestión de contraseñas*, consulte Capítulo 19, “Referencia de los portlets de gestión de contraseñas”, en la página 281.

Para obtener más información acerca de la *administración de portlets*, consulte Capítulo 9, “Administración de portlets”, en la página 179.

Para obtener más información acerca de la importación o exportación de datos del portal, consulte Capítulo 14, “Herramientas para exportar e importar datos del portal”, en la página 229.

Para obtener más información acerca de las funciones del *organigrama corporativo*, consulte Capítulo 18, “Referencia del portlet Organigrama corporativo”, en la página 265.

Para obtener más información acerca de las funciones de *búsqueda en el Directorio*, consulte Capítulo 20, “Referencia del portlet Lista de búsqueda”, en la página 295.

Para obtener más información acerca de las opciones de creación de objetos nuevos (portlet *Crear*) y de cómo se administran, consulte Capítulo 16, “Referencia del portlet de creación”, en la página 243.

Para obtener más información acerca de la configuración y administración del *flujo de trabajo*, consulte Capítulo 21, “Introducción a la provisión basada en el flujo de trabajo”, en la página 311, así como Capítulo 22, “Configuración de las definiciones de peticiones de provisión”, en la página 325 y Capítulo 23, “Gestión de los flujos de trabajo de provisión”, en la página 347.

Diseño del entorno de producción 2

En este capítulo se tratan temas relativos a la configuración de un entorno de producción. En él se proporcionan directrices sobre un cierto número de consideraciones que entrarán en juego cuando se pase de un entorno de prueba experimental (u otro entorno previo a la producción) a un entorno de producción.

El presente capítulo está organizado de acuerdo con las secciones principales siguientes:

2.1 Topología

El número de instancias de cada subsistema principal y las formas en que éstas se pueden conectar son, potencialmente, elevadas. No todos los diseños están admitidos. Es importante no sólo comprender las posibilidades, sino también por qué se prefieren algunas configuraciones sobre otras.

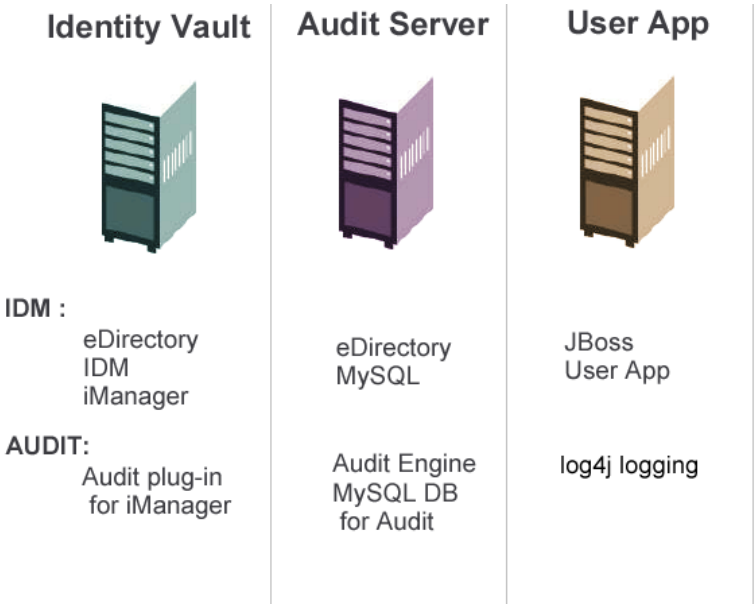
2.1.1 Diseño mínimo

La configuración lógica más sencilla de la aplicación de usuario corresponde a una instalación del tipo "uno de cada", que consiste en un árbol de repositorio seguro de identidades, una instancia del motor del Gestor de identidades y controladores y una instancia de JBoss ejecutando una única instancia de la aplicación de usuario. Desde el punto de vista de la aplicación física, en teoría, se pueden ejecutar todos juntos. Aunque en una situación real, esta disposición no es recomendable por una serie de motivos (principalmente de seguridad, mantenimiento y rendimiento). A la hora de decidir el número de máquinas necesarias para una instalación real, tendrá que tener en cuenta (como mínimo) las consideraciones siguientes:

- *Servidor de Novell Audit:* Esta parte es la encargada de capturar información relativa a eventos (y posiblemente buena parte de la información restante) en el entorno de la aplicación de usuario en el momento de ejecutarse. Es posible que su tarea sea también doble como almacén de consolidación para otras aplicaciones de su empresa. Por una serie de motivos, probablemente no deseará poner otras partes importantes del sistema del Gestor de identidades (como, por ejemplo, JBoss o el repositorio seguro de identidades) en la misma máquina que el servidor de Audit.
- *Repositorio seguro de identidades:* Este componente tiene una carga de tráfico elevada y tanto su rendimiento como su capacidad de ampliación deben ser buenos. Por todo ello, es muy probable que piense en poner el repositorio seguro de identidades en una máquina dedicada. Es decir, probablemente no deseará que otro sistema con tráfico elevado como JBoss, con una implantación de la aplicación de usuario, se ejecute junto con el repositorio seguro de identidades en la misma máquina.

- *Base de datos:* Si esta instancia de MySQL (u otra base de datos admitida) es también la base de datos de Novell Audit, probablemente estará en una máquina dedicada. Tenga en cuenta que la aplicación de usuario utiliza esta parte de la forma siguiente:
- Como almacén de consolidación de los datos de configuración del portal
- Como almacén de consolidación de la información de estado acerca de los flujos de trabajo que están en curso (si el módulo de provisión está instalado).
- Opcionalmente, como almacén de registros de Novell Audit.
- *JBoss:* Por motivos de rendimiento y capacidad, es probable que desee ejecutar esta parte en una máquina dedicada.

Basándose en las observaciones anteriores, se sugiere el uso de las configuraciones con un mínimo de 3 máquinas que se detallan a continuación:



2.1.2 Diseño de alta disponibilidad

La agrupación en clúster para obtener una mayor capacidad y disponibilidad se trata con más detalle en una sección posterior de este capítulo. Por ahora, tenga en cuenta que:

- El Gestor de identidades admite una alta disponibilidad del repositorio seguro de identidades, el motor y los controladores mediante mecanismos de instalación multinodo y de almacenamiento compartido descritos en el capítulo relativo a la “Alta disponibilidad” de la guía de administración principal del Gestor de identidades. Encontrará instrucciones completas acerca de cómo configurar un sistema de este tipo con SUSE Linux en el artículo que se encuentra en:

  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm)
- Se puede conseguir una alta disponibilidad de la aplicación de usuario a través de la agrupación en clúster de JBoss. Por ejemplo, puede configurar un clúster de JBoss de tal manera que cada nodo ejecute una instancia de la aplicación de usuario. Todas las instancias serán iguales (pares). No obstante, tenga en cuenta que no se producen réplicas de sesiones entre las

instancias. Cada instancia es responsable de su propia unidad de trabajo y no terminará ninguna sesión iniciada en un nodo hermano.

- No se admite una migración de recursos automática (por los motivos que acabamos de indicar). Si bien, se puede reanudar un flujo de trabajo interrumpido después de la pérdida de un nodo de clúster, si se conecta otro nodo con el mismo ID del motor del flujo de trabajo que el nodo desactivado. (En este caso, la reanudación del flujo de trabajo interrumpido se produce automáticamente, tan pronto como el nuevo motor del flujo de trabajo se inicia).

Consulte también Sección 2.4, “Agrupación en clúster”, en la página 48 (más adelante) para obtener información detallada acerca de estas cuestiones.

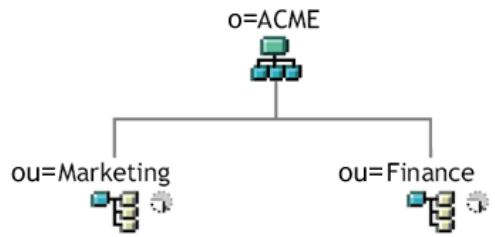
2.1.3 Restricciones de diseño

Por lo general, las dos restricciones arquitectónicas principales que deben tenerse en cuenta son:

- Ninguna instancia de la aplicación de usuario puede atender (buscar y consultar, añadir usuarios a, etc.) a más de un contenedor de usuarios. Asimismo, una vez que se ha asociado un contenedor de usuario a la aplicación, dicha asociación será permanente.
- Ningún controlador de la aplicación de usuario puede asociarse a más de una aplicación de usuario, salvo en el caso en que las aplicaciones de usuario estén instaladas en nodos hermano del mismo clúster de JBoss. Dicho de otro modo, no se admite una asignación del tipo "uno a varias" de controlador a varias aplicaciones de usuario.

La primera restricción aplica un alto grado de encapsulación en el diseño de la aplicación de usuario.

Supongamos que tiene la siguiente estructura administrativa:



Durante la instalación de la aplicación de usuario, el sistema le solicita que especifique el contenedor de usuario de máximo nivel que la instalación buscará en el repositorio seguro de identidades. En dicho caso, puede especificar *ou=Marketing,o=ACME* o bien (como alternativa) *ou=Finance,o=ACME*. No se pueden especificar ambos. Todas las búsquedas y consultas de la aplicación de usuario (y entradas del administrador) se realizarán en el ámbito del contenedor que especifique.

Nota: En teoría, puede especificar un ámbito de *o=ACME* a fin de incluir Marketing y Finance. No obstante, en las grandes organizaciones con posiblemente varios contenedores *ou* (en vez de sólo dos relativos a Marketing y Finance), probablemente esto no sea práctico.

Evidentemente, es posible crear dos instalaciones independientes de la aplicación de usuario (que no compartan recursos comunes), una para Marketing y otra para Finance. En tal caso, cada instalación tendrá su propia base de datos, su propio controlador de la aplicación de usuario configurado de

forma adecuada, y cada aplicación de usuario se administrará por separado y, posiblemente, poseerá temas únicos.

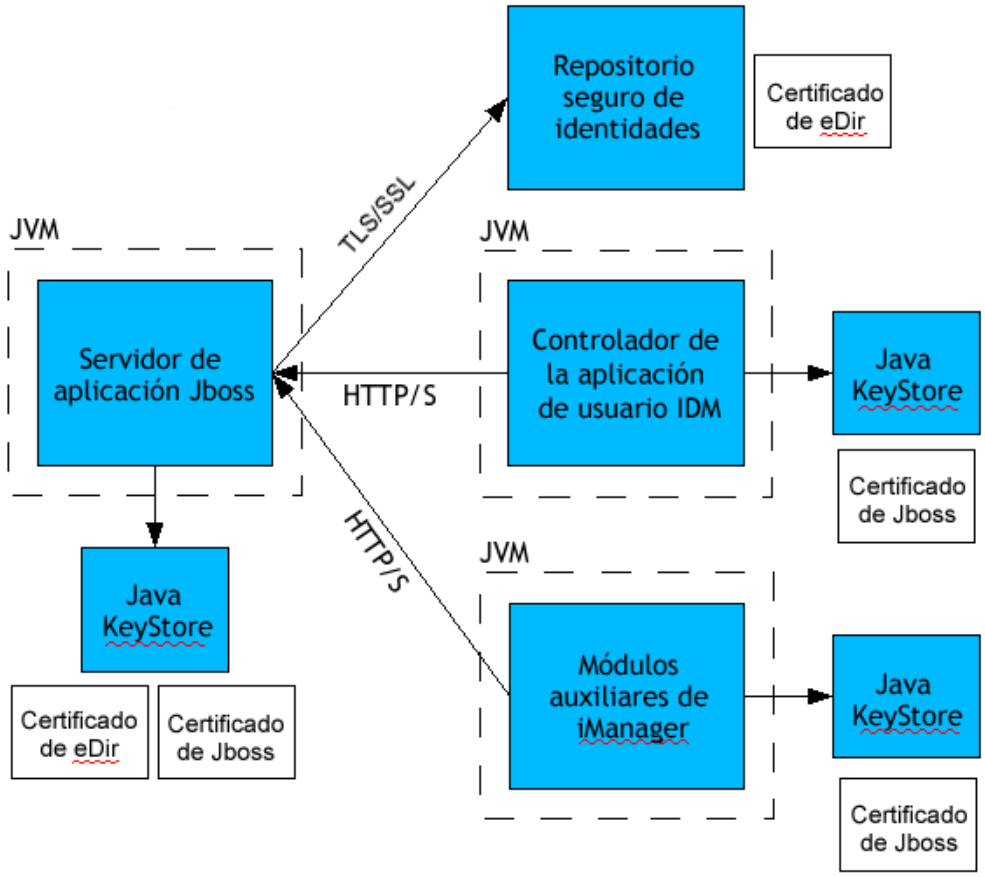
Si realmente necesita tener Marketing y Finance en el mismo ámbito para una instalación de la aplicación de usuario, puede aplicar una de las dos tácticas siguientes. Una de ellas consiste en insertar un objeto Contenedor nuevo (por ejemplo, *ou=MarketingAndFinance*) en la jerarquía, por encima de los dos nodos hermanos y, a continuación, indicar el nuevo contenedor como la raíz del ámbito. La otra táctica consiste en crear una réplica filtrada (un tipo especial de árbol eDirectory) que combina las partes que se necesitan del árbol ACME original y en apuntar aplicación de usuario al contenedor raíz de la réplica. (Consulte la publicación Novell eDirectory Administration Guide [Novell eDirectory: Guía de administración] para obtener más información acerca de las réplicas filtradas).

Si tiene alguna duda o pregunta acerca de una determinada disposición del sistema, póngase en contacto con el representante de Novell para que éste le aconseje o le ayude.

2.2 Seguridad

Pasar de una etapa previa a la producción a la etapa de producción implica, por lo general, reforzar los aspectos de seguridad del sistema. En las pruebas experimentales, es posible que haya estado utilizando HTTP normal para conectar el controlador de la aplicación de usuario con JBoss o bien puede que haya utilizado un certificado autofirmado (como medida temporal) para la comunicación del tipo controlador/servidor de aplicación. Por otra parte, en producción, probablemente necesitará utilizar conexiones seguras, con una autenticación de servidor basada en el certificado Verisign (u otro proveedor de confianza) de su empresa.

Es normal utilizar certificados X.509 en una serie de lugares del entorno de la aplicación de usuario del Gestor de identidades, tal como se muestra en el esquema siguiente.



Todas las comunicaciones entre la aplicación de usuario y el repositorio seguro de identidades son seguras utilizando, por defecto, Transport Layer Security. La instalación del certificado del repositorio seguro de identidades (eDirectory) en el almacén de claves de JBoss se efectúa automáticamente en el momento de la instalación. A menos que se indique lo contrario, el programa de instalación de la aplicación de usuario pondrá una copia del certificado de eDirectory en el almacén *cacerts* de JRE.

Si las comunicaciones deben ser seguras, es preciso que el certificado del servidor esté en varios lugares, tal como se muestra en el esquema. Es posible que deba efectuar una configuración diferente, en función de si piensa utilizar un certificado autofirmado en los diversos lugares del esquema donde aparece un recuadro que indica *JBoss cert* o si, en vez de ello, desea utilizar un certificado emitido por una autoridad certificadora (CA) de confianza como, por ejemplo, Verisign.

Certificados autofirmados

Si utiliza un certificado de una autoridad certificadora reconocida y de confianza (como, por ejemplo, Verisign), no necesitará realizar ningún tipo de configuración especial. No obstante, si piensa crear y utilizar un certificado autofirmado, deberá seguir los pasos siguientes:

1 Cree un almacén de claves con un certificado autofirmado, utilizando una sintaxis de línea de comando similar a la siguiente:

```
keytool -genkey -alias tomcat -keyalg RSA -storepass changeit -
keystore jboss.jks -dname
"cn=JBoss,ou=exteNd,o=Novell,l=Waltham,s=MA,c=US" -keypass
changeit
```

Observe que va a crear el archivo “jboss.jks”, además de crear el certificado.

2 Copie el archivo almacén de claves (jboss.jks) en el directorio de la aplicación de usuario de JBoss; por ejemplo:

```
cp jboss.jks ~/jboss-4.0.2/server/spitfire/conf
```

Activación de SSL en JBoss

Para habilitar SSL en JBoss, localice el archivo *jbossweb-tomcat55.sar* en *[IDM]/jboss/server/IDM/deploy/*. En éste, busque el archivo *server.xml* y ábralo en un editor de texto. Habilite SSL eliminando el comentario o añadiendo una sección similar a la siguiente:

```
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true" scheme="https" secure="true"
clientAuth="false" keystoreFile="${jboss.server.home.dir}/spitfire/
conf/jboss.jks" keystorePass="changeit" sslProtocol = "TLS" />
```

Activación de la seguridad SOAP

En *IDM.war*, busque el archivo *web.xml* y ábralo en un editor de texto. En la parte inferior del archivo, elimine el comentario de la sección siguiente:

```
<security-constraint> <web-resource-collection> <web-resource-
name>IDMProv</web-resource-name> <url-pattern>/*</url-pattern> <http-
method>POST</http-method> <http-method>GET</http-method>
<description>IDM Provisioning Edition</description> </web-resource-
collection> <user-data-constraint> <transport-guarantee>CONFIDENTIAL</
transport guarantee> </user-data-constraint> </security-constraint>
```

Guarde el archivo y el archivo de reserva. Reinicie JBoss.

2.2.1 Autenticación mutua

La aplicación de usuario del Gestor de identidades admite los casos de *autenticación de usuario* normales (tal como se utilizan habitualmente en las sesiones https con *páginas Web seguras* en la Web), pero no admite la autenticación basada en certificados bidireccionales por defecto. No obstante, esta función se puede obtener con Novell iChain. Así, si, por ejemplo, su organización necesita que los usuarios entren mediante un certificado de usuario, en lugar de entrar utilizando una contraseña, lo conseguirá añadiendo iChain a su entorno.

Si desea obtener más información, consulte al representante de Novell.

2.3 Ajuste del rendimiento

El ajuste del rendimiento es un tema complejo. La aplicación de usuario del Gestor de identidades se basa en tecnologías diversas con varias interacciones. No es posible anticipar cada caso único de configuración o de interacción de usuarios con bajo rendimiento. No obstante, algunos subsistemas pueden estar sujetos a mejoras recomendadas que pueden incrementar el rendimiento. A continuación, las tratamos.

2.3.1 Registro

La aplicación de usuario permite registrar tanto a través de Novell Audit como de la estructura *log4j* de Apache de código abierto. Por defecto, el registro a través de Novell Audit está desactivado. No obstante, por defecto, el registro de la consola y archivos a través de *log4j* está habilitado.

Nota: Los tipos de eventos que puede registrar y cómo habilitar o inhabilitar el registro, se tratan en Capítulo 5, “Configuración de las entradas”, en la página 119 y en Capítulo 12, “Configuración del registro”, en la página 213 más adelante en esta misma guía.

Los valores de configuración de *log4j* se encuentran en un archivo denominado *log4j.xml* en *$IDMINSTALL/jboss/server/IDMProv/conf/*. Cerca de la parte inferior de este archivo, encontrará la entrada siguiente:

```
<root>     <priority value="INFO" />     <appender-ref ref="CONSOLE" /
>     <appender-ref ref="FILE" /> </root>
```

Si asigna un valor a `root`, se asegurará de que cualquier agregador de registros que no tenga un nivel asignado herede explícitamente el nivel de `root` (en este caso, INFO). Por ejemplo, por defecto, el agregador FILE no tiene asignado un nivel de umbral y acepta el de root.

Los posibles niveles de registro que *log4j* utiliza son DEBUG, INFO, WARN, ERROR y FATAL, tal como están definidos en la clase *org.apache.log4j.Level*. Si no se presta atención al uso adecuado de estos valores, puede tener graves consecuencias sobre el rendimiento.

Por lo general, una buena estrategia es utilizar INFO o DEBUG sólo cuando se está depurando un problema determinado.

Cualquier agregador incluido en root que tenga un nivel umbral definido, lo deberá tener en ERROR, WARN o FATAL, a menos que, (como acabamos de explicar), esté depurando.

El resultado del rendimiento con un nivel de registros elevado tiene menos que ver con los detalles de los mensajes que con el simple hecho de que el registro de los archivos y la consola en *log4j* implica escrituras síncronas. Existe una clase `AsyncAppender`, si bien su uso no garantiza un mejor rendimiento. Los problemas (que son bien conocidos y están relacionados con *log4j* de Apache y no con el Gestor de identidades) se tratan en la dirección siguiente *http://logging.apache.org/log4j/docs/api-1.2.8/org/apache/log4j/performance/Logging.html*.

El valor por defecto de INFO en el archivo de configuración del registro (descrito más arriba) de la aplicación de usuario es adecuado para un gran número de entornos; sin embargo, cuando el nivel de rendimiento es fundamental, debe cambiar la entrada de *log4j.xml* anterior por:

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

Dicho de otro modo, elimine CONSOLE y defina el nivel de registro como ERROR. Para obtener una configuración de producción depurada y totalmente probada, no es preciso registrarse en el nivel INFO, ni tampoco es necesario dejar el registro de CONSOLE habilitado. La repercusión de su desactivación sobre el rendimiento puede ser significativa.

Para obtener más información acerca de *log4j*, consulte la documentación disponible en *http://logging.apache.org/log4j/docs*.

Para obtener más información acerca de cómo utilizar Novell Audit con el Gestor de identidades, consulte la publicación Novell Identity Manager Administration Guide (Gestor de identidades: Guía de administración).

2.3.2 Repositorio seguro de identidades

Las consultas de LDAP pueden producir atascos en un entorno de directorio-servidor de gran utilización. Para mantener un alto nivel de rendimiento con un gran número de objetos, Novell eDirectory (que es la base del repositorio seguro de identidades en el Gestor de identidades) registra la información más solicitada y la almacena en índices. Cuando se ejecuta una consulta compleja en objetos que tienen atributos con índices, la respuesta a la consulta es mucho más rápida.

Cuando se entrega, eDirectory tiene los atributos siguientes ya indexados:

```
Aliased Object Name cn dc Equivalent to Me extensionInfo Given Name
GUID ldapAttributeList ldapClassList Member NLS: Common Certificate
Obituary Reference Revision Surname uniqueID uniqueID_SS
```

Cuando se instala el Gestor de identidades, el esquema del directorio por defecto se amplía con los nuevos tipos de clase de objeto y los nuevos atributos que pertenecen a la aplicación de usuario. Por defecto, los atributos específicos de la aplicación de usuario no están indexados. Para obtener un mejor rendimiento, probablemente le será útil indexar algunos atributos (y puede que también algunos atributos LDAP tradicionales), en especial, si su contenedor de usuarios va a contener más de 5.000 objetos.

La idea general consiste en indexar sólo aquellos atributos que sabe que se consultarán regularmente. (Que muy bien podrían ser diferentes atributos para diferentes entornos de producción). La única manera de saber con seguridad qué atributos se van a utilizar más a menudo es recopilar estadísticas de predicados en el tiempo de ejecución. (No obstante, el proceso de recolección produce una degradación del rendimiento).

El proceso de recolección de estadísticas de predicado se trata en profundidad en la publicación eDirectory Administration Guide (Novell eDirectory: Guía de administración). En dicha guía también encontrará una descripción en profundidad de los índices. Normalmente, tendrá que hacer lo siguiente:

- Utilizar ConsoleOne para activar la recolección de estadísticas de predicados para detectar los atributos de interés
- Poner el sistema en carga
- Inhabilitar la recolección de estadísticas y analizar los resultados

- Crear un índice por cada tipo de atributo que sea interesante tener

Si ya sabe qué atributos desea indexar, no necesita utilizar ConsoleOne. Puede crear y gestionar índices en iManager mediante Mantenimiento de eDirectory > Índices. Por ejemplo, si sabe que los usuarios del organigrama corporativo probablemente realizarán búsquedas basadas en el atributo *isManager*, puede intentar crear un índice para dicho atributo para ver si mejora el rendimiento.

Nota: Como práctica recomendada, se aconseja crear un índice, como mínimo, de los atributos *manager* e *isManager*.

Para consultar un estudio detallado de los índices de atributos y el rendimiento, vaya al capítulo dedicado al "ajuste de eDirectory" en la publicación *Novell's Guide to Troubleshooting eDirectory* (Guía de Novell para la resolución de problemas de eDirectory) de Peter Kuo y Jim Henderson (QUE Books, ISBN 0-7897-3146-0).

Consulte también el capítulo "Maintaining Novell eDirectory" (Mantenimiento de Novell eDirectory) que contiene una orientación para ajustar el rendimiento, en la publicación *eDirectory Administration Guide* (Novell eDirectory: Guía de administración).

2.3.3 JVM

La cantidad de memoria de pila asignada a la máquina virtual de Java puede repercutir sobre el rendimiento. Si especifica valores máximos o mínimos de memoria demasiado altos o bajos (y por demasiado altos se entiende valores por encima de la memoria física de la máquina), podría sufrir un intercambio excesivo del archivo de paginación.

Puede definir el tamaño de JVM máximo para el servidor JBoss editando el archivo `run.conf` o `run.bat` (el primero para Linux y el segundo para Windows) en `[IDM]/jboss/bin/` en un editor de texto. Aumente "-Xmx" de *128m* a *512m* o más si es posible. Es posible que sea necesario hacer pruebas para determinar cuál es el valor óptimo para su entorno concreto.

Nota: Puede encontrar consejos de ajuste de rendimiento de JBoss y Tomcat en http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming (http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming)

2.3.4 Valor de tiempo límite de la sesión

El tiempo límite de la sesión (tiempo que un usuario puede dejar una página sin atender en su navegador Web antes de que el servidor haga aparecer un diálogo de advertencia de tiempo límite de la sesión) puede cambiarse en el archivo *web.xml* del archivo *IDM.war*. Este valor debe ajustarse para que se adapte al entorno de uso y del servidor donde se ejecutará la aplicación. Por lo general, se aconseja que el tiempo límite de la sesión sea lo mínimo posible. Si los requisitos de la empresa pueden permitir un tiempo límite de sesión de 5 minutos, el servidor podría liberar los recursos no utilizados en la mitad de tiempo que si el valor de tiempo límite fuera de 10 minutos. Esto permite que la aplicación Web tenga un mayor rendimiento y se pueda ampliar más.

Cuando ajuste el tiempo límite de una sesión, tenga en cuenta las consideraciones siguientes:

- Los tiempos límite de sesión largos pueden hacer que el servidor JBoss se quede sin memoria, si varios usuarios deciden entrar en un corto espacio de tiempo. Y lo mismo ocurre con cualquier servidor de aplicación que tenga demasiadas sesiones abiertas.

- Cuando un usuario entra en la aplicación de usuario, se crea una conexión LDAP para el usuario y se vincula a la sesión. Por consiguiente, cuantas más sesiones haya abiertas, mayor será el número de conexiones LDAP mantenidas. Cuanto más dure el tiempo límite de una sesión, más tiempo estarán abiertas dichas conexiones. Y demasiadas conexiones abiertas en el servidor LDAP (aunque estén inactivas) pueden producir una degradación del rendimiento del sistema.
- Si el servidor empieza a experimentar errores OutOfMemoryErrors y los parámetros de ajuste de recolección de datos inservibles y de la pila JVM ya se han definido en un nivel óptimo, debería considerar la posibilidad de disminuir el tiempo límite de sesión.

Para ajustar el valor de tiempo límite de la sesión, necesitará abrir el archivo de reserva *IDM.war*, encontrar el archivo *web.xml* que contiene y editar la parte siguiente de dicho archivo (en concreto, el valor numérico que aquí se muestra como 20 para indicar 20 minutos, que es el valor por defecto):

```
<session-config>     <session-timeout>20</session-timeout> </session-
config>
```

A continuación, deberá guardar el archivo y el archivo de reserva y reiniciar el servidor.

Nota: La edición manual de los archivos de reserva de Web debe efectuarla personal experimentado en la instalación y desarrollo de aplicaciones Web Java.

2.4 Agrupación en clúster

Cuando utilice la aplicación de usuario en un entorno de clúster, debe tener en cuenta tres cuestiones:

- La configuración en clúster de JBoss (consulte Sección 2.4.1, “Agrupación en clúster de JBoss”, en la página 48)
- La configuración de caché de la aplicación de usuario (consulte Sección 2.4.3, “Configuración del caché del grupo de clústeres de la aplicación de usuario”, en la página 53)
- La configuración del motor de flujos de trabajo (consulte Sección 2.4.4, “Configuración de los flujos de trabajo para la agrupación en clúster”, en la página 54)

2.4.1 Agrupación en clúster de JBoss

Un clúster es un conjunto de nodos del servidor de aplicación que proporciona una serie de servicios. El objetivo de un clúster es aumentar el rendimiento y la fiabilidad de las aplicaciones. Por lo general, un clúster aporta tres ventajas clave a las aplicaciones de empresa:

- Alta disponibilidad
- Capacidad de ampliación (más capacidad)
- Balance de la carga

Por alta disponibilidad se entiende que una aplicación es fiable y se puede disponer de ella durante la mayor parte del tiempo que está abierta. Los clústeres aportan una alta disponibilidad ya que la misma aplicación se ejecuta en todos los nodos. Si uno de los nodos falla, la aplicación podrá seguir ejecutándose en los otros nodos. Cuando la aplicación de usuario del Gestor de identidades se ejecuta en un clúster, se beneficia de una mayor disponibilidad. No obstante, no admite la réplica de

sesiones HTTP. Esto significa que, si una sesión se está procesando en un nodo y dicho nodo falla, la información de la sesión se perderá.

Por balance de carga se entiende la práctica de distribuir la carga de trabajo entre los miembros de un clúster. Su objetivo es mejorar el rendimiento. El balance de carga se puede conseguir de diferentes maneras (por ejemplo, por carga rotativa de DNS o por balance de carga de hardware). Visite el sitio http://www.onjava.com/pub/a/onjava/2001/09/26/load.html (http://www.onjava.com/pub/a/onjava/2001/09/26/load.html) para consultar un estudio de los diferentes métodos de balance de carga. Con independencia del método seleccionado, probablemente deseará incluir el balance de carga en su configuración de clúster.

Grupos de clústeres de JBoss

Los clústeres de JBoss se basan en un módulo de comunicaciones denominado JGroups. JGroups se instala con JBoss (también se puede utilizar sin JBoss). JGroups se encarga de las comunicaciones entre grupos que comparten un mismo nombre, una dirección de multidifusión y un puerto multidifusión.

Cuando se instala un servidor JBoss agrupado en clúster, JBoss define dos grupos JGroups diferentes para utilizarlos en la gestión del clúster. Uno de ellos se denomina *DefaultPartition* y está definido en /deploy/cluster-service.xml. JBoss utiliza este grupo de clústeres para proporcionar servicios de agrupación en clúster básicos. JBoss también define otro grupo de clústeres denominado *Tomcat-Cluster*. Este grupo de clústeres está definido en /deploy/tc-cluster-service.xml y proporciona réplicas de sesiones para el servidor Tomcat que se ejecuta dentro de JBoss.

La aplicación de usuario del Gestor de identidades utiliza un tercer grupo de clústeres. Dicho grupo de clústeres utiliza un nombre UUID para minimizar el peligro de conflictos con otros grupos de clústeres que los usuarios puedan añadir a sus servidores. Por defecto, el grupo de clústeres se denomina `c373e901aba5e8ee996644453544200`. Este clúster no se configura utilizando un archivo de servicio de JBoss, sino que los valores de configuración se encuentran en el directorio y se pueden configurar utilizando las funciones de administración de la aplicación de usuario. Si está familiarizado con la agrupación en clúster de JGroups y JBoss, podrá ajustar la configuración de clúster de la aplicación de usuario utilizando esta interfaz. Los cambios de la configuración de clúster sólo entran en vigor en los nodos de servidor cuando dichos nodos se reinician.

El grupo de clústeres de la aplicación de usuario sólo se utiliza para coordinar los cachés de la aplicación de usuario en un entorno de clústeres. No depende de los dos grupos de clústeres de JBoss ni interactúa con ellos de ninguna manera. Por defecto, el grupo de clústeres de la aplicación de usuario y los dos grupos JBoss utilizan nombres de grupos, direcciones multidifusión y puertos multidifusión diferentes, para que no sea necesaria una reconfiguración.

Los valores del grupo de clústeres de la aplicación de usuario los comparte cualquier aplicación de Identity Manager 3 que comparte la configuración del directorio. El objetivo de la opción de valores locales en la interfaz de administración de la aplicación de usuario es permitir que el administrador elimine un nodo de un clúster o que cambie la pertenencia de los servidores de un clúster. Por ejemplo, la agrupación en clúster se puede inhabilitar globalmente y, a continuación, habilitarla localmente para un subconjunto de servidores que comparten la configuración del directorio.

Grupo de aplicaciones

JBoss permite realizar implantaciones activas en el clúster copiando una aplicación EAR, WAR o JAR en el directorio de grupo de una instancia de JBoss agrupada en clúster. La implantación activa

en una máquina hace que el componente se implante automáticamente en todas las instancias contenidas en el clúster, mientras éste está ejecutándose.

No se recomienda este tipo de implantación de la aplicación con la versión de JBoss Application Server (4.0.2) que se incluía en el programa de instalación de la aplicación de usuario en el momento en que se escribió este documento, ya que sigue habiendo problemas sin solucionar relativos a su uso. No obstante, hemos descrito los pasos básicos que deben llevarse a cabo (consulte "Implantación de la aplicación de usuario en un clúster utilizando el grupo de JBoss" en la página 52) para implantar correctamente la aplicación de usuario utilizando la tecnología de grupo de JBoss, ya que se esperan mejoras en esta tecnología tras la publicación de este documento.

Base de datos MySQL

El programa de instalación de la aplicación de usuario instala el gestor de la base de datos MySQL y crea una base de datos para utilizar en la aplicación de usuario, o bien utiliza una base de datos Oracle, Microsoft SQL Server o MySQL ya existente. La base de datos es la encargada de la consolidación de los datos. Todos los nodos del clúster de JBoss deben acceder a la misma instancia de la base de datos. La aplicación de usuario utiliza llamadas JDBC estándar para acceder a la base de datos y actualizarla. La aplicación de usuario utiliza un origen de datos JDBC asociado al árbol JNDI para abrir una conexión con la base de datos. Si crea el clúster de JBoss utilizando el programa de instalación de la aplicación de usuario, el sistema instalará el origen de los datos. Si elige configurar manualmente el clúster de JBoss, necesitará copiar los archivos de origen de datos (IDM-ds.xml) en el directorio de implantación de todos los nodos del clúster. Asimismo, si utiliza MySQL, deberá copiar el controlador JDBC de MySQL (*mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*), que se encuentra en el directorio JBoss /server/IDM/lib, en el directorio JBoss server/IDM/lib.

Registro

Para habilitar el registro de los clústeres, deberá editar el archivo de configuración log4j.xml, situado en el directorio \conf de la configuración del servidor de JBoss (por ejemplo, \server\IDM\conf) y eliminar el comentario de la sección situada en la parte inferior y que es parecida a la siguiente:

```
<!--  Clustering logging --> - <!-- Elimine lo siguiente para redirigir
las categorías org.jgroups y org.jboss.a un archivo cluster.log.
<appender name="CLUSTER"
class="org.jboss.logging.appender.RollingFileAppender"> <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/> <param
name="File" value="${jboss.server.home.dir}/log cluster.log"/> <param
name="Append" value="false"/> <param name="MaxFileSize" value="500KB"/
> <param name="MaxBackupIndex" value="1"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%d %-5p [%c] %m%n"/> </layout> </
appender> <category name="org.jgroups"> <priority value="DEBUG" />
<appender-ref ref="CLUSTER"/> </category> <category
name="org.jboss.ha"> <priority value="DEBUG" /> <appender-ref
ref="CLUSTER"/> </category> -->
```

El archivo *cluster.log* se encuentra en el directorio *log* de la configuración del servidor de JBoss (por ejemplo, *\server\IDM\log*).

2.4.2 Instalación de la aplicación de usuario en un clúster de JBoss

El método recomendado de instalación de la aplicación de usuario consiste en utilizar el programa de instalación de la aplicación de usuario para instalarla en cada uno de los nodos del clúster. Si bien no recomendamos implantar la aplicación de usuario en un clúster mediante el grupo de JBoss, hemos incluido un procedimiento que se puede utilizar como método alternativo.

Utilización del programa de instalación de la aplicación de usuario en cada nodo del clúster

JBoss se entrega con tres configuraciones de servidor listas para utilizar: *mínima*, *por defecto* y *completa*. La agrupación en clúster sólo está habilitada en la configuración *completa*. El archivo cluster-service.xml, que se encuentra en la carpeta /deploy, describe la configuración de la partición de clúster por defecto. Cuando instale la aplicación de usuario e indique al programa de instalación que desea realizar la instalación en un clúster, dicho programa hará una copia de la configuración *completa*, la denominará *IDM* (por defecto, el programa de instalación permite cambiar el nombre) e instalará la aplicación de usuario en dicha configuración.

Para instalar la aplicación de usuario en todos los nodos de un clúster utilizando el programa de instalación de la aplicación de usuario:

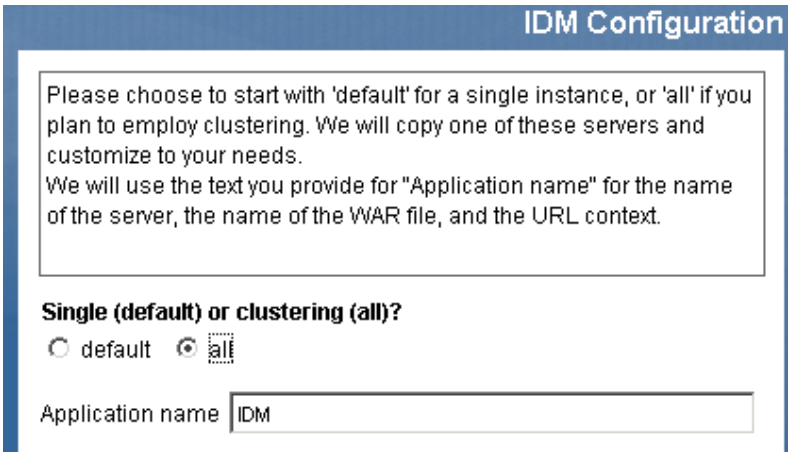
1. Efectúe una instalación completa de la aplicación de usuario (MySQL, JBoss y la aplicación de usuario) en el primer nodo de JBoss. Para obtener información acerca de cómo utilizar el programa de instalación de la aplicación, consulte la publicación *Identity Manager 3 Installation Guide* (Identity Manager 3: Guía de instalación).
   - Si utiliza MySQL como la base de datos de la aplicación de usuario, el programa de instalación de la aplicación de usuario creará una nueva instalación de MySQL. Anote la contraseña de usuario root de MySQL que especifique; necesitará esta información cuando instale la aplicación de usuario en los nodos restantes del clúster.
   - En la pantalla *Configuración del Gestor de identidades* del programa de instalación, seleccione la opción "*agrupación en clúster (todos)* ".
   - Seleccione las opciones de instalación adecuadas para su entorno.
2. Si MySQL todavía no está ejecutándose, inicie MySQL utilizando el archivo *start-mysql.bat* que se encuentra en el directorio /IDM/mysql.

Nota: En Linux, el comando shell siguiente será útil para determinar si el daemon de MySQL está ejecutándose:

```
ps -A | grep mysqld
```

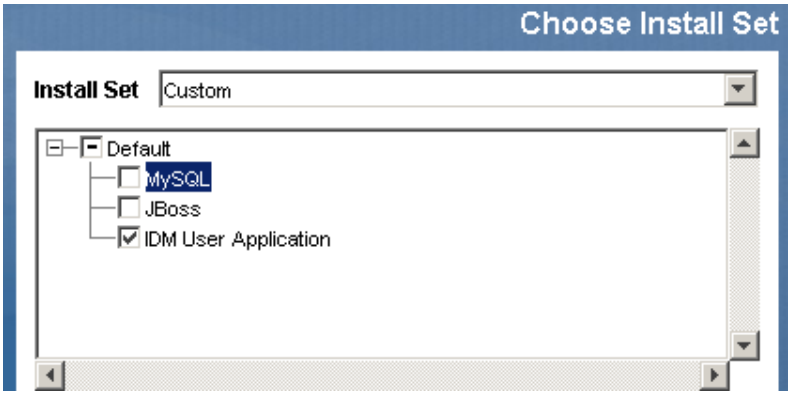
Si este comando devuelve varias líneas que terminan por `mysqld`, el daemon está ejecutándose.

3 Inicie JBoss y la aplicación de usuario utilizando el archivo *start-jboss.bat* (Windows) o *start-jboss.sh* (Linux), situado en el directorio *IDM*.



4 Efectúe una instalación personalizada de la aplicación de usuario en cada nodo adicional del clúster de JBoss.

- Seleccione sólo la aplicación de usuario para la instalación:



- Especifique la dirección IP o el nombre de host del servidor en el que se instalará la base de datos de la aplicación de usuario.
- Especifique el nombre de usuario y la contraseña de la base de datos de la aplicación de usuario. Si utiliza MySQL, el nombre de usuario es `root` y la contraseña será la que haya especificado durante el proceso de instalación en Paso 1.
- En la pantalla *Configuración del Gestor de identidades* del programa de instalación, seleccione la opción "*agrupación en clúster (todos)*".
- Seleccione las opciones de instalación adecuadas para su entorno.

5 Inicie cada uno de los nodos del clúster de JBoss utilizando el archivo *start-jboss.bat* (Windows) o *start-jboss.sh* (Linux), que se encuentra en el directorio *IDM*.

Implantación de la aplicación de usuario en un clúster utilizando el grupo de JBoss

No utilice el grupo de JBoss con JBoss versión 4.0.2 o anterior, ya que puede tener problemas (consulte http://jira.jboss.com/jira/browse/JBAS-1899 (http://jira.jboss.com/jira/browse/JBAS-1899)). Recomendamos que instale la aplicación de usuario con el programa de instalación de dicha

aplicación en todos los nodos del clúster (consulte “Utilización del programa de instalación de la aplicación de usuario en cada nodo del clúster” en la página 51 de este capítulo). No obstante, si desea utilizar el grupo para implantar la aplicación de usuario en un clúster de JBoss utilizando JBoss 4.0.3 o una versión superior, siga los pasos que indicamos a continuación.

Nota: Estos pasos se indican para aquellos clientes que deseen utilizar JBoss 4.0.3 por su cuenta y riesgo, de forma experimental. La versión admitida oficialmente es la 4.0.2.

Para implantar la aplicación de usuario en un clúster utilizando el grupo de JBoss:

1. Efectúe una instalación personalizada de la aplicación de usuario en uno de los nodos del clúster de JBoss, seleccionando la aplicación de usuario y MySQL (si utiliza MySQL; de lo contrario, instale sólo la aplicación de usuario) para la instalación. Puede realizar la instalación con todos los clústeres del nodo ejecutándose, aunque el nodo en el que instale la aplicación de usuario deberá ser el primer nodo del clúster en iniciarse.
2. Copie el archivo del controlador JDBC (por ejemplo, si utiliza MySQL, el controlador JDBC es *mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*), que se encuentra en el directorio /server/IDM/lib, en el directorio correspondiente de cada nodo del clúster.
3. Copie el archivo *cacerts* del directorio /lib/security de JRE que se instaló con la aplicación de usuario en el directorio JRE /lib//security de todos los nodos del clúster.
4. Mueva el archivo IDM.war y el archivo de origen de datos IDM-ds.xml del directorio /deploy del directorio de configuración del servidor al directorio /farm del directorio de configuración del servidor. En realidad debe mover los archivos. No deje los originales en el directorio /deploy.
5. Inicie la base de datos de la aplicación de usuario (si utiliza la base de datos MySQL suministrada, inicie MySQL utilizando el archivo *start-mysql.bat* situado en el directorio /IDM/mysql).
6. Inicie JBoss y la aplicación de usuario utilizando el archivo *start-jboss.bat* (Windows) o *start-jboss.sh* (Linux), situado en el directorio *IDM* del nodo en el que ha instalado la aplicación de usuario y la base de datos de la aplicación de usuario.
7. Inicie los nodos restantes del clúster.

2.4.3 Configuración del caché del grupo de clústeres de la aplicación de usuario

Los usuarios que están familiarizados con la agrupación en clúster de JGroups y JBoss pueden modificar la configuración del caché del grupo de clústeres mediante la interfaz de usuario de administración de la aplicación de usuario (consulte Sección 13.3.5, “Valores de caché para los clústeres”, en la página 226). Los cambios de la configuración de clúster sólo entran en vigor en los nodos de servidor cuando se reinicia el nodo del servidor.

2.4.4 Configuración de los flujos de trabajo para la agrupación en clúster

El funcionamiento de la agrupación en clúster del motor del flujo de trabajo es independiente de la estructura de caché de la aplicación de usuario. Debe ejecutar varios pasos para asegurarse de que el motor del flujo de trabajo funciona correctamente en un entorno de clúster.

- Todos los servidores del clúster deben apuntar a la misma base de datos. Si instala la aplicación de usuario en el clúster utilizando el método recomendado (consulte "Utilización del programa de instalación de la aplicación de usuario en cada nodo del clúster" en la página 51), esto se consigue especificando, durante el proceso de instalación, la dirección IP o el nombre de host del servidor en el que está instalada la base de datos de la aplicación de usuario. Si utiliza el grupo para implantar la aplicación de usuario en los nodos del clúster (consulte "Implantación de la aplicación de usuario en un clúster utilizando el grupo de JBoss" en la página 52), esto se consigue moviendo el archivo de origen de datos (IDM-ds.xml) desde el directorio /deploy al directorio /farm en el nodo en el que se instaló por primera vez la aplicación de usuario. Esto hará que el origen de datos se implante en todos los nodos del clúster.
- Cada servidor del clúster necesita iniciarse con un ID de motor exclusivo. Para ello, ajuste la propiedad del sistema *com.novell.afw.wf.engine-id* al iniciarse el servidor. Por ejemplo, si desea iniciar JBoss y asignar el ID de motor `ENGINE1` al motor del flujo de trabajo de dicho servidor, utilice el comando siguiente:

  run.sh -Dcom.novell.afw.wf.engine-id=ENGINE1 (Linux)

  run.bat -Dcom.novell.afw.wf.engine-id=ENGINE1 (Windows)

Una instancia de proceso de flujo de trabajo, una vez iniciada por un motor del flujo de trabajo que se ejecuta en un servidor determinado, sólo se puede ejecutar y completar en dicho servidor. Esto permite asegurarse de que el proceso de flujo de trabajo se ejecute con seguridad. No obstante, no proporciona soporte para migración de recursos de la instancia de un proceso. Si un servidor del clúster se detiene, la instancia del proceso no se reiniciará hasta que un motor con el mismo ID se reinicie.

Si el equipo de un servidor no se puede reiniciar debido a un fallo grave del software o del hardware, puede iniciar el servidor de aplicación en otro equipo, utilizando el mismo ID del motor del flujo de trabajo utilizado en la máquina que no se puede recuperar. Dado que el ID del motor es un nombre lógico y no una asignación directa con el equipo físico en el que se ejecutaba el motor, la instancia del proceso interrumpido se completará correctamente en el equipo nuevo.

Las instancias de proceso son propiedad del motor que ha iniciado el proceso; no obstante, un usuario puede entrar en cualquier aplicación de usuario de un clúster para ver detalles del proceso, retraer procesos o completar tareas que se le han asignado. Los procesos retraídos o las tareas completadas en un motor que no es propietario del proceso entran en el estado de pendiente y la ejecución sólo se reanuda cuando son detectados por el motor que es su propietario.

Configuración del entorno de la aplicación de usuario

II

En los capítulos siguientes se indica cómo configurar diversos aspectos del entorno de la aplicación de usuario del Gestor de identidades para responder a las necesidades de su organización.

Configuración del controlador de la aplicación de usuario

3

3.1 Acerca del controlador de la aplicación de usuario

El controlador de la aplicación de usuario es el encargado de iniciar los flujos de trabajo de provisión y de notificar a la aplicación de usuario los cambios que se han producido en el repositorio seguro de identidades (por ejemplo, cuando se introducen cambios en el nivel de abstracción del directorio utilizando el Diseñador del Gestor de identidades). En este controlador sólo se utiliza el canal Suscriptor. El controlador procesa los mensajes del repositorio seguro de identidades a la aplicación de usuario que se ejecuta en un servidor de aplicación. Aunque algunos eventos que se producen en la aplicación de usuario se notifican al repositorio seguro de identidades, dichos eventos no pasan por el canal Editor del controlador de la aplicación de usuario.

Cuando se inicia el servidor de aplicación, el controlador establece una sesión con dicho servidor. El controlador envía mensajes a la aplicación de usuario que se ejecuta en el servidor de aplicación (por ejemplo, “recupera un nuevo conjunto de definiciones de directorio virtuales”).

Los componentes de origen del controlador son:

- ComposerDriverShim.jar: el controlador suplementario de Composer. Se instala en el directorio *lib \Novell\NDS\lib* de Windows o en el directorio *classes /usr/lib/dirxml/classes* en Linux
- srvprvUAD.jar: el controlador suplementario de la aplicación. Se instala en el directorio *lib \Novell\NDS\lib* de Windows o en el directorio *classes /usr/lib/dirxml/classes* en Linux
- UserApplicationDriver.xml: archivo que contiene datos de preconfiguración para configurar el nuevo controlador. Se instala en el directorio *DirXML.Drivers \Tomcat\webapps\nps\DirXML.Drivers* en Windows o en */usr/lib/dirxml/rules/DirXML.Drivers* en Linux

Los componentes del controlador de la aplicación de usuario se instalan cuando se instala Identity Manager 3. Para poder ejecutar la aplicación de usuario de Identity Manager 3, primero, debe añadir el controlador de la aplicación de usuario a un conjunto de controladores nuevos o ya existentes y, a continuación, activar el controlador.

Según el entorno de trabajo, deberán efectuarse muy pocas tareas de configuración del controlador de la aplicación de usuario o deberá aplicar un complejo conjunto de reglas empresariales en las directivas de controlador. El controlador de la aplicación de usuario proporciona los mismos mecanismos flexibles para la sincronización de datos que otros controladores del Gestor de identidades.

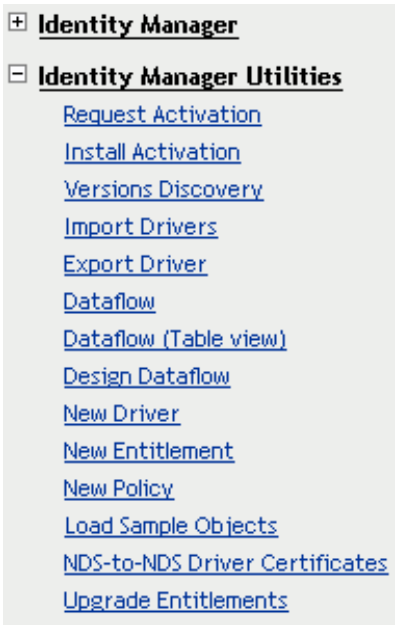
En este capítulo se describe cómo crear, configurar e iniciar un controlador de la aplicación de usuario y cómo configurar el controlador para iniciar automáticamente un flujo de trabajo basado en un evento del repositorio seguro de identidades. Se incluyen las secciones siguientes:

- Sección 3.2, “Creación de un controlador de la aplicación de usuario”, en la página 58
- Sección 3.3, “Inicio del controlador de la aplicación de usuario”, en la página 64
- Sección 3.4, “Configuración de los flujos de trabajo para que se inicien automáticamente”, en la página 65

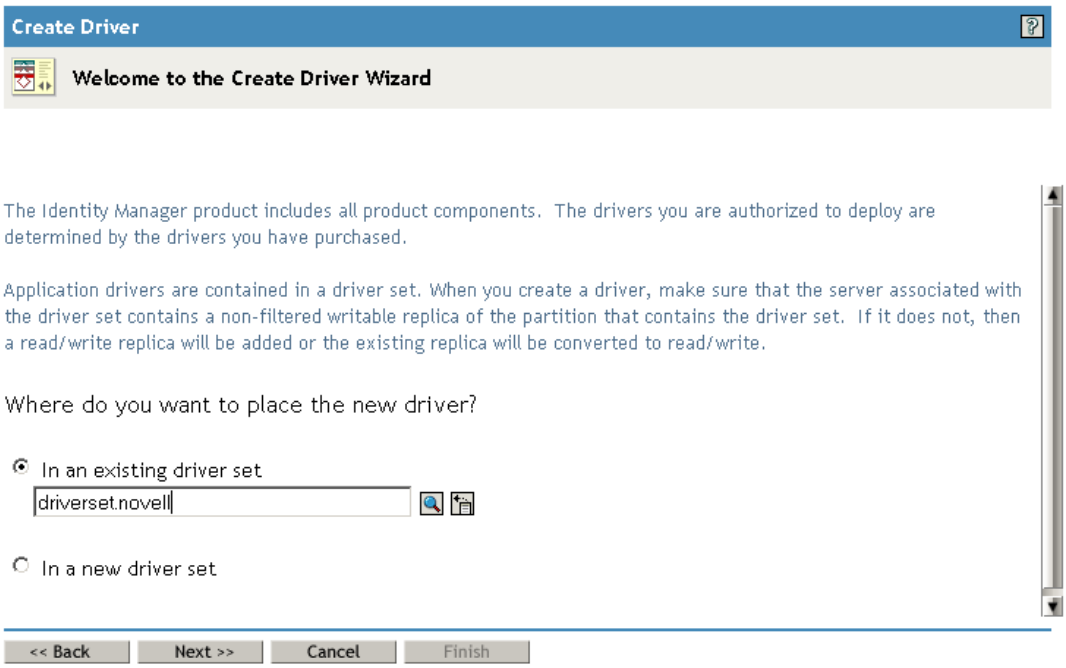
3.2 Creación de un controlador de la aplicación de usuario

Para crear un controlador:

1. Entre en la instancia de iManager que gestiona el repositorio seguro de identidades.
2. Abra el nodo *Utilidades del Gestor de identidades* de la estructura de navegación de iManager.



3 Haga clic en *Controlador nuevo*. Aparecerá el asistente de creación de controladores:

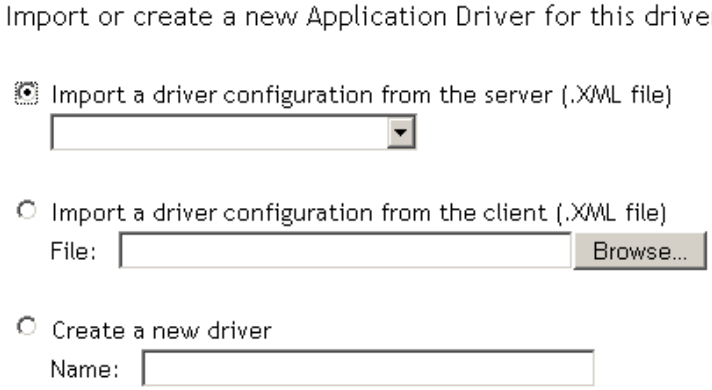


El paso siguiente consiste en seleccionar dónde desea crear el nuevo controlador. Puede crearlo en un conjunto de controladores ya existente o bien crear un conjunto de controladores nuevo.

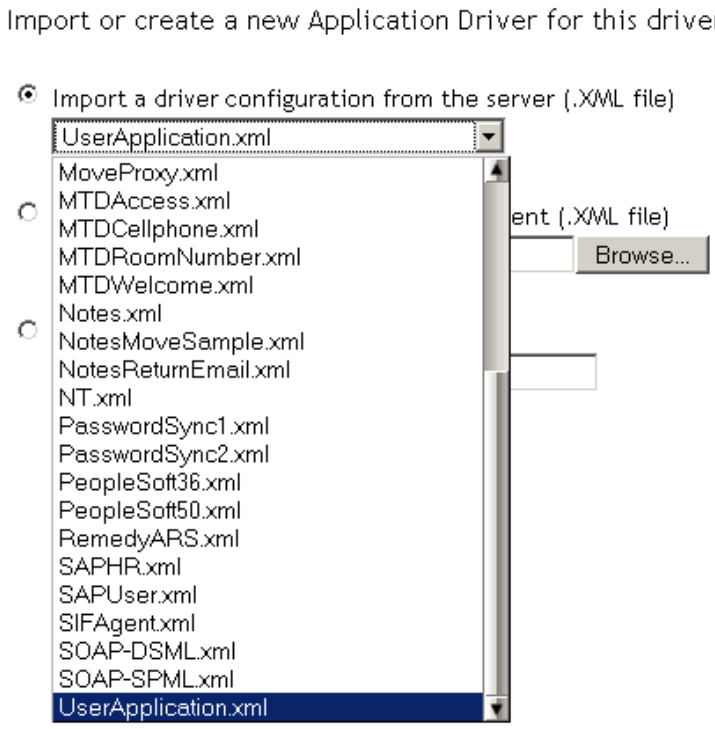
4 Si selecciona *En un conjunto de controladores existente*, aparecerá un asistente que debe utilizar para examinar el repositorio seguro de identidades para localizar el conjunto de controladores. Seleccione el conjunto de controladores existente y, a continuación, *Siguiente.*

Si selecciona *En un conjunto de controladores nuevo*, aparecerá una pantalla que deberá utilizar para definir las propiedades del nuevo conjunto de controladores. Especifique un nombre, un contexto de árbol y un servidor para el conjunto de controladores y, a continuación, seleccione *Siguiente*.

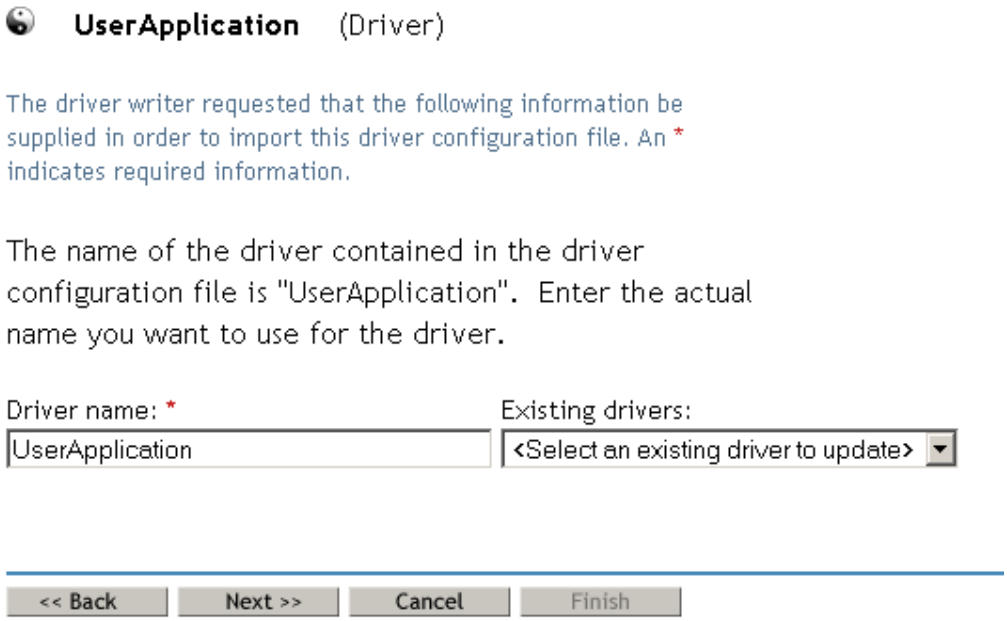
Aparecerá la pantalla siguiente de *Asistente para crear controlador*:



5 Haga clic en la opción *Importar la configuración de un controlador del servidor* y, a continuación, seleccione *UserApplication.xml* en la lista de archivos XML:



6 Haga clic en *Siguiente*. El *Asistente para crear controlador* mostrará una página que deberá utilizar para asignar un nombre al controlador y configurarlo:



El nombre por defecto del controlador es UserApplication. Puede utilizar dicho nombre o bien asignarle otro con más sentido para su proyecto.

7 Si así lo desea, escriba un nombre nuevo para el controlador en el campo *Nombre del controlador*.

8 En el campo *ID de autenticación*, especifique el DN del administrador de la aplicación de usuario (consulte Sección 1.1.2, “Administrador de la aplicación de usuario”, en la página 17 para obtener una descripción del administrador de la aplicación de usuario), utilizando el formato de puntos (por ejemplo, admin.orgunit.novell).

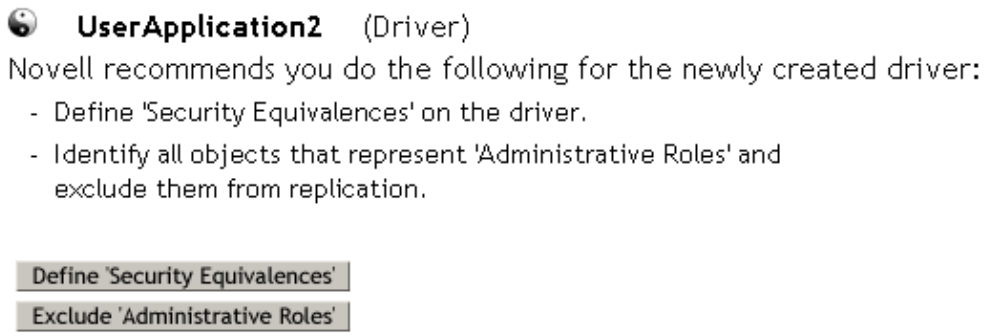
9 En los campos *Contraseña de la aplicación* y *Reintroducir la contraseña*, especifique la contraseña del administrador de la aplicación de usuario identificada en el campo *ID de autenticación*.

10 En el campo *Contexto de la aplicación*, escriba el nombre de la aplicación especificado al instalar la aplicación de usuario. El nombre por defecto es `IDM`.

11 En el campo *Host*, especifique el nombre de host o la dirección IP del servidor de aplicación en el que se ejecuta la aplicación de usuario.

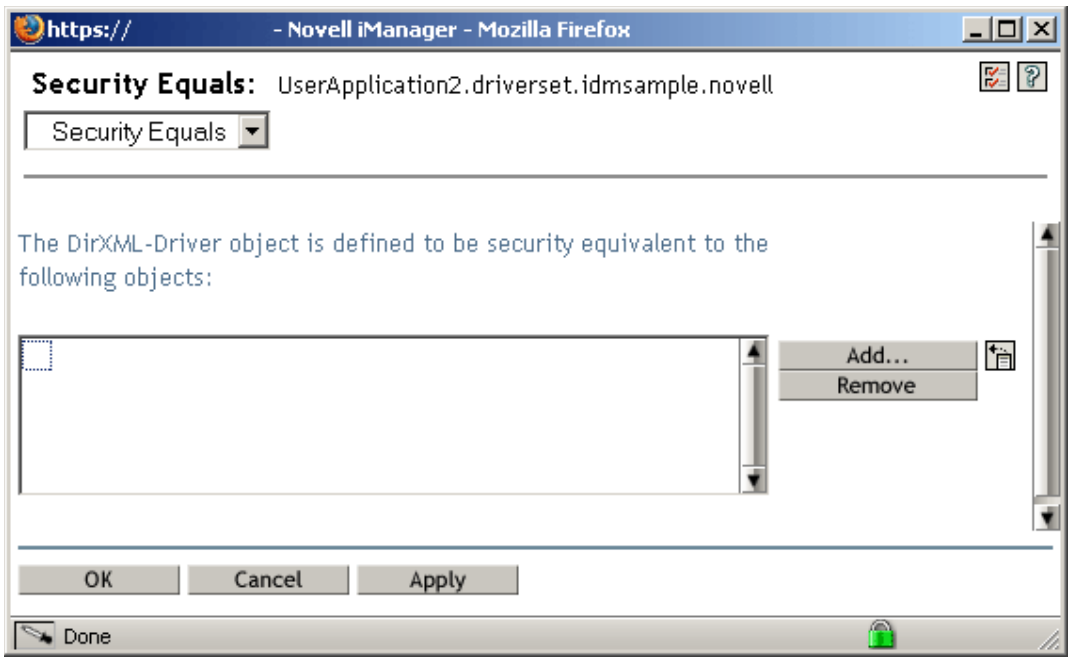
12 En el campo *Puerto*, especifique el puerto en el que el controlador se comunicará con la aplicación que se ejecuta en el servidor de aplicación (por ejemplo, 8080).

13 Haga clic en *Siguiente*. Aparecerá un mensaje que indica que la configuración del controlador se está importando y, a continuación, se visualizará la página siguiente del Asistente para *crear controlador*:

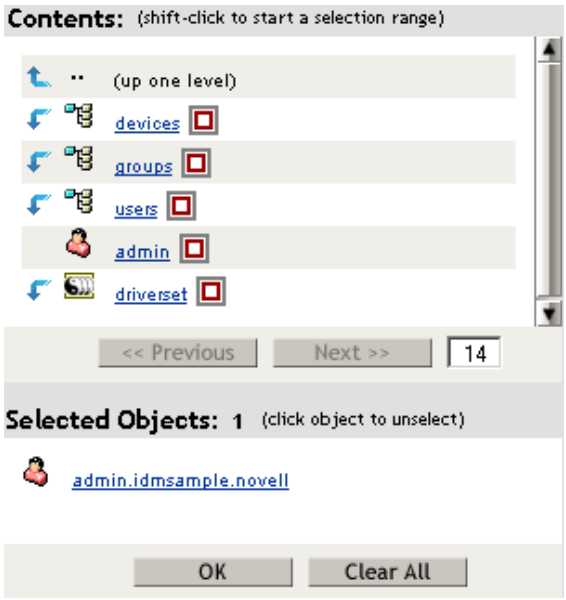


El objeto Controlador debe tener suficientes derechos del repositorio seguro de identidades sobre todos los objetos que lea o escriba. Para ello, es preciso otorgar *Equivalencias de seguridad* al objeto Controlador. El controlador debe tener acceso de lectura y escritura a las listas de usuarios, oficinas postales, recursos y distribución, así como derechos de creación, lectura y escritura sobre el contenedor de oficinas postales. Por lo general, debe darse al controlador la misma seguridad que al administrador.

14 Haga clic en *Definir equivalencias de seguridad*. Aparecerá una ventana nueva:



15 Haga clic en *Añadir*. Aparecerá una ventana para seleccionar un objeto del árbol que tenga el nivel de derechos adecuado, para asignarlo al controlador (por ejemplo, `admin`):



16 Seleccione un objeto que tenga el nivel deseado de derechos sobre el repositorio seguro de identidades en el árbol y haga clic en *Aceptar*. Regresará a la ventana anterior.

17 Haga clic en *Aceptar*. Regresará al Asistente para *crear controlador*.

18 Haga clic en *Excluir funciones administrativas*. Aparecerá la ventana *Usuarios excluidos*. Utilice esta función para evitar que un administrador quede bloqueado fuera del controlador de

la aplicación de usuario si la contraseña del administrador cambia en otro repositorio seguro de identidades que se duplica en el árbol al que pertenece el controlador.

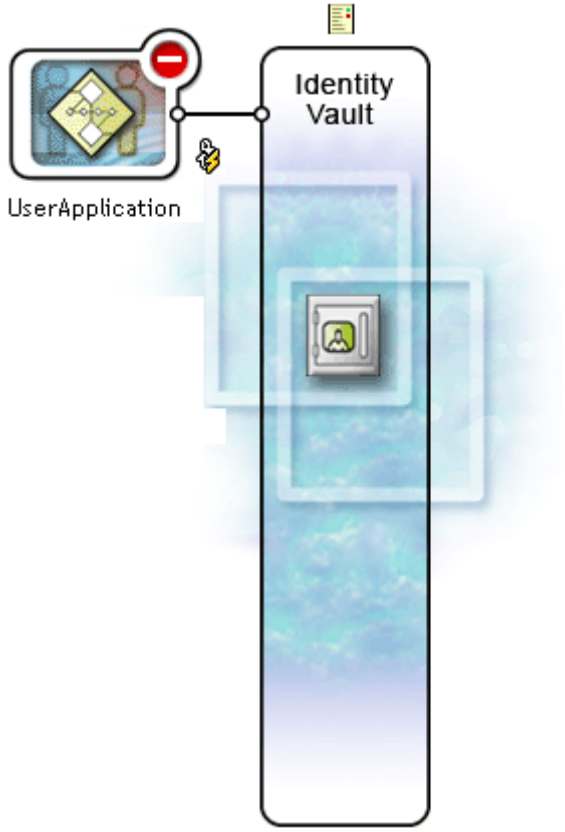
19 Haga clic en *Añadir*. Aparecerá una ventana para desplazarse por el árbol de directorios y buscar los usuarios cuyos datos no deben pasarse al controlador. Por lo general, es buena idea excluir los objetos ADMIN, dado que la duplicación de sus datos en la conexión de un controlador no es, en la mayoría de los casos, una práctica recomendada.

20 Seleccione las funciones administrativas que desea excluir y, a continuación, haga clic en *Aceptar*. Regresará a la ventana anterior.

21 Haga clic en *Aceptar*. Regresará al Asistente para *crear controlador*.

22 Haga clic en *Siguiente.* Aparecerá una página de resumen del controlador.

23 Haga clic en *Finalizar la descripción general*. Se mostrará una representación gráfica del controlador en el repositorio seguro de identidades:



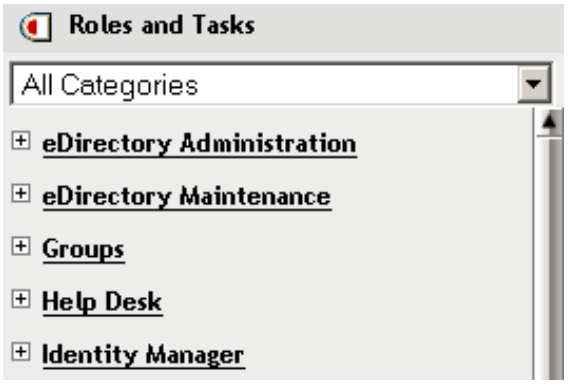
Nota: Puede volver a ver esta pantalla utilizando el enlace *Descripción del Gestor de identidades* bajo *Gestor de identidades* en el árbol de navegación de iManager.

El nuevo controlador aparecerá como un icono grande conectado al repositorio seguro de identidades.

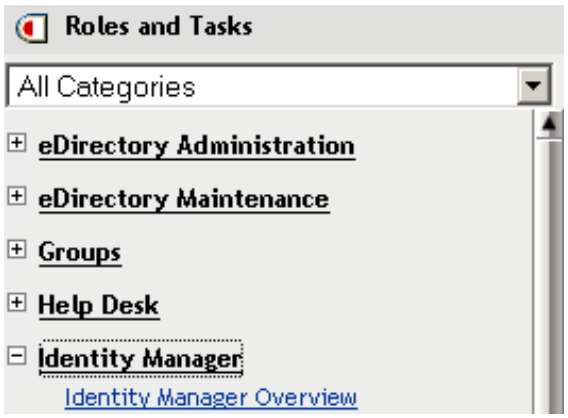
3.3 Inicio del controlador de la aplicación de usuario

Para iniciar el controlador de la aplicación de usuario:

1. Haga clic en el enlace *Gestor de identidades* del árbol de navegación de iManager para ver los comandos disponibles en la categoría Gestor de identidades:



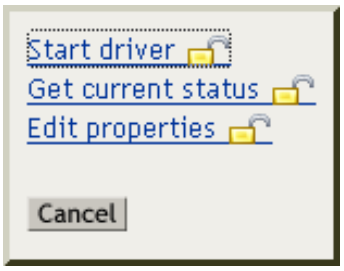
2. Haga clic en el enlace *Descripción del Gestor de identidades* que está bajo *Gestor de identidades* en el árbol de navegación de iManager:



   Aparecerá un asistente que puede utilizar para examinar el sistema y localizar el conjunto de controladores que contiene el controlador que desea activar.

3. Seleccione el conjunto de controladores y, a continuación, haga clic en *Siguiente*. Aparecerá la página *Descripción del Gestor de identidades*.
4. Haga clic en el indicador de estado rotativo en la esquina superior derecha del icono del controlador:

Aparecerá un menú que muestra una lista de los comandos para iniciar y detener el controlador, así como para editar las propiedades de éste:



5 Haga clic en *Iniciar controlador*.

3.4 Configuración de los flujos de trabajo para que se inicien automáticamente

Si está instalado el módulo de provisión, los flujos de trabajo se inician automáticamente cuando un usuario inicia una petición de provisión mediante la solicitud de un recurso. Por otra parte, el controlador de la aplicación de usuario del Gestor de identidades escucha los eventos del repositorio seguro de identidades y, cuando está configurado para ello, responde a los eventos iniciando el flujo de trabajo de provisión adecuado. Por ejemplo, puede configurar el controlador de la aplicación de usuario para que inicie automáticamente un flujo de trabajo de provisión si se añade un usuario nuevo al repositorio seguro de identidades. Puede configurar el controlador de la aplicación de usuario para que inicie automáticamente flujos de trabajo utilizando reglas y directivas del Gestor de identidades.

3.4.1 Acerca de las directivas

Los filtros y directivas se pueden utilizar con el controlador de la aplicación de usuario igual que con los demás controladores del Gestor de identidades. Cuando se produce un evento en el repositorio seguro de identidades, el Gestor de identidades crea un documento XML que describe el evento. Este documento pasa por el canal hasta el sistema conectado (en este caso, el sistema conectado es la aplicación de usuario). Los filtros y las directivas asociados al controlador permiten definir cómo responder al evento y, en el proceso, transformar el documento XML al formato que el sistema conectado espera. El Gestor de identidades proporciona varias categorías de directivas (por ejemplo, de transformación de eventos, de comandos, de asignación de esquema o de transformación de la salida) que se pueden aplicar, en un orden prescrito, para transformar el documento XML. En esta sección, presentamos un ejemplo de cómo iniciar un flujo de trabajo basado en eventos en el repositorio seguro de identidades. Aunque se puede utilizar cualquier directiva para iniciar un flujo de trabajo, en este ejemplo se muestra el método más sencillo y útil.

Cuando se crea un controlador de la aplicación de usuario, se crea también una directiva de transformación de eventos para que el controlador la utilice. Dicha directiva es la encargada de crear el documento XML que las directivas del canal Suscriptor restantes procesarán.

Nota: No cambie la directiva de transformación de eventos que se creó al mismo tiempo que el controlador de la aplicación de usuario. El DN de esta directiva empieza por `Manage.Modify.Subscriber`. Si cambia esta directiva, el proceso del flujo de trabajo puede fallar.

Asimismo, se crea una directiva de asignación de esquemas. Puede utilizar dicha directiva como punto de partida para iniciar un flujo de trabajo basado en eventos del repositorio seguro de identidades.

3.4.2 Configuración del inicio de un flujo de trabajo basado en un evento del repositorio seguro de identidades

El método más sencillo de iniciar automáticamente un flujo de trabajo se consigue utilizando el editor de la directiva de asignación de esquemas; a tal efecto, el controlador de la aplicación de usuario proporciona una directiva vacía para que el usuario la edite.

El editor de directivas de asignación de esquemas se utiliza para asignar atributos del repositorio seguro de identidades (incluido el atributo *trigger* de eDirectory que, cuando cambia, inicia el flujo de trabajo) a los datos de tiempo de ejecución de un flujo de trabajo de destino. Los datos de tiempo de ejecución vienen determinados por la plantilla de definición de flujos de trabajo (consulte Capítulo 22, “Configuración de las definiciones de peticiones de provisión”, en la página 325 para obtener información acerca de las plantillas de definición de flujos de trabajo). Los datos de tiempo de ejecución son necesarios para que el flujo de trabajo se complete correctamente. Cuando se crea un flujo de trabajo, se crean también una serie de *atributos globales* en el repositorio seguro de identidades que pueden utilizarse para personalizar el funcionamiento del controlador de la aplicación de usuario. Un atributo global es un atributo que no pertenece a ninguna clase de objeto del repositorio seguro de identidades. Dichos atributos se llaman <workflowName>_StartWorkflow, <workflowName>_recipient y <workflowName>_reason. Existen también dos atributos más denominados AllWorkflows:reason y AllWorkflows:recipient. El atributo _StartWorkflow se utiliza para iniciar un flujo de trabajo. Los atributos _recipient y _reason se utilizan para aceptar los datos de tiempo de ejecución que el flujo de trabajo del repositorio seguro de identidades necesita.

Antes de ejecutar este procedimiento, debe saber cuál es el nombre del atributo del repositorio seguro de identidades que desea utilizar como activador del flujo de trabajo. También necesita saber el nombre del flujo de trabajo que desea iniciar. Todos los flujos de trabajo incluyen un atributo especial denominado `<workflowName>_StartApprovalFlow`. El flujo de trabajo se configura para iniciarse automáticamente basándose en un evento del repositorio seguro de identidades asignando el atributo de eDirectory deseado al atributo <workflowName>_StartApprovalFlow del flujo de trabajo.

Para configurar un flujo de trabajo para que se inicie basándose en un evento del repositorio seguro de identidades:

1. En iManager, haga clic en el enlace *Descripción del Gestor de identidades* bajo Gestor de identidades en el árbol de navegación de iManager.

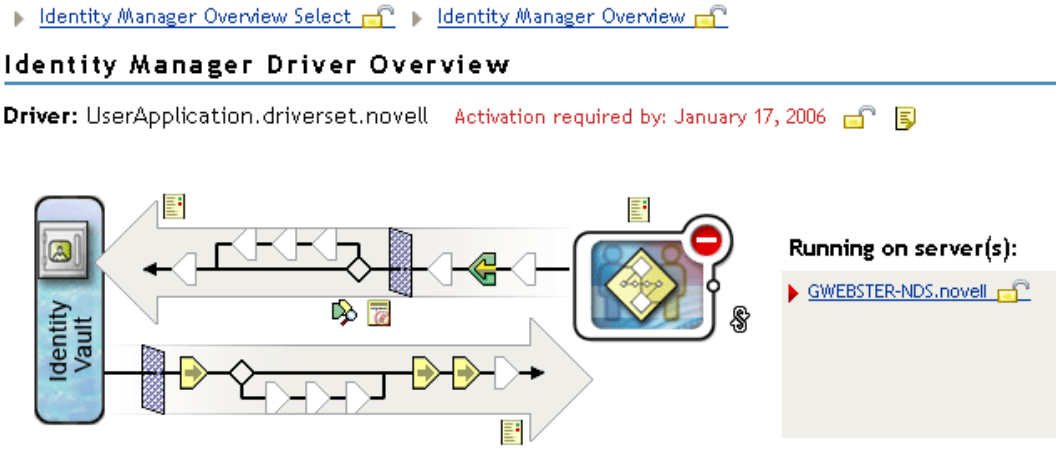
   

   Aparecerá la página *Descripción del Gestor de identidades*. Esta página le solicitará que seleccione un conjunto de controladores.

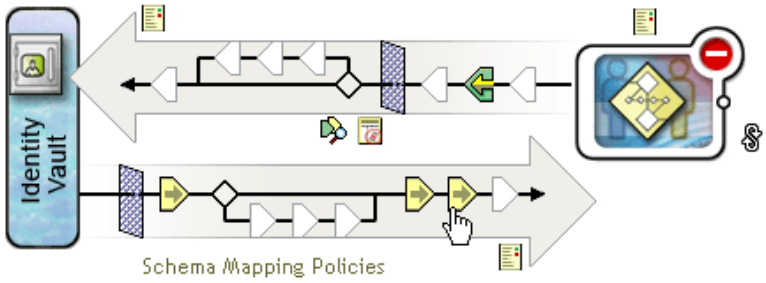
2. Haga clic en *Buscar árbol completo* y, a continuación, haga clic en *Buscar*. Aparecerá la página *Descripción del Gestor de identidades* con un gráfico que muestra los controladores que tiene el conjunto de controladores seleccionado en ese momento.

3 Haga clic en el icono de controlador más grande del controlador de la aplicación de usuario:

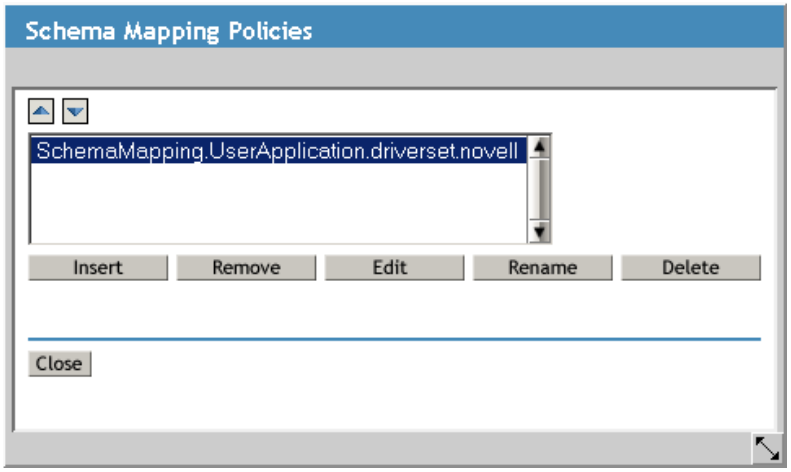
Aparecerá la página *Descripción del controlador del Gestor de identidades*:



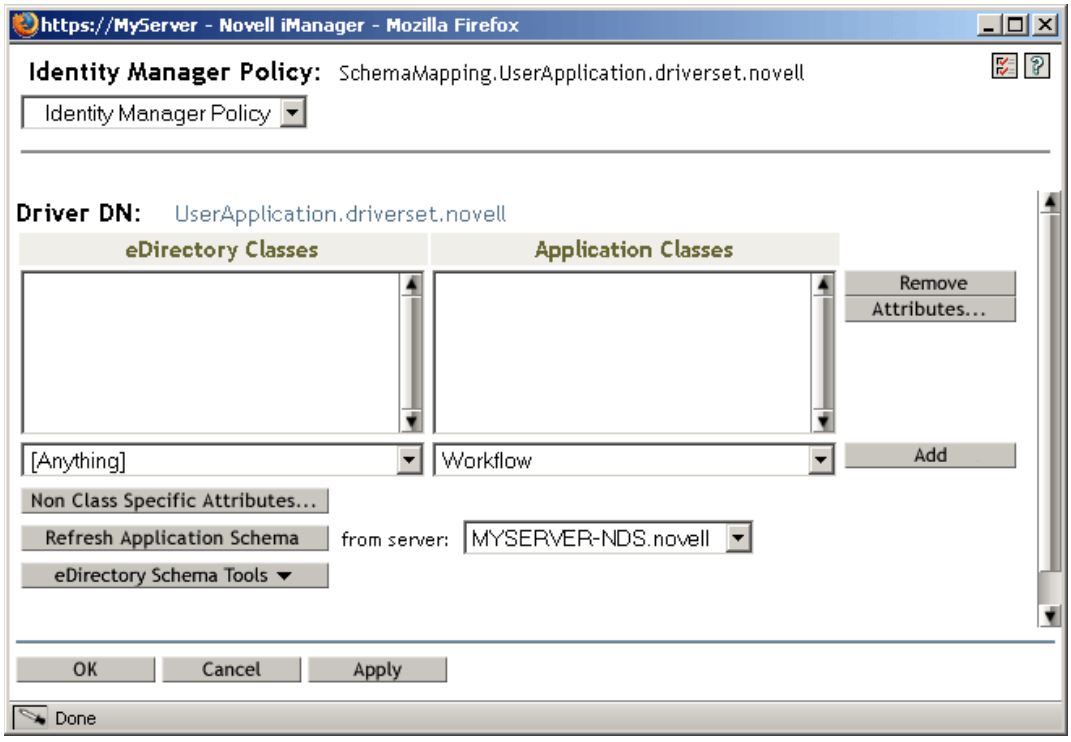
La flecha horizontal superior representa el canal Editor (que no se utiliza en el controlador de la aplicación de usuario) y la flecha horizontal inferior representa el canal Suscriptor. Si pasa el puntero del ratón por encima de un objeto del gráfico, verá que aparece una descripción de dicho objeto:



4 Haga clic en el icono *Directivas de asignación de esquema* para el canal Suscriptor. Aparecerá el recuadro de diálogo *Directiva del Gestor de identidades* con el nombre de la directiva de asignación de esquema por defecto resaltada:



5 Haga clic en *Editar*. Aparecerá el recuadro de diálogo *Directiva del Gestor de identidades*. Este recuadro de diálogo se utiliza para asignar las clases del repositorio seguro de identidades a las clases de aplicación. Este procedimiento no utiliza esta función. En su lugar, asignaremos los atributos de eDirectory a los atributos de la aplicación de usuario global.



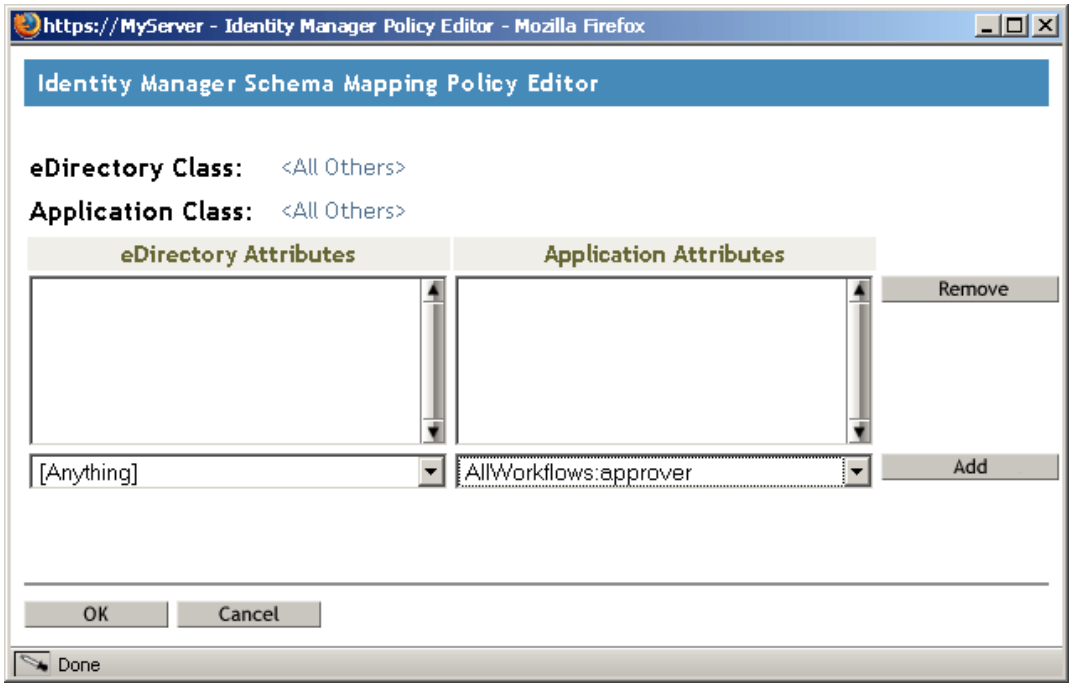
6 Haga clic en *Actualizar el esquema de aplicación*. Aparecerá un mensaje que informa que debe detenerse el controlador para leer el esquema y, a continuación, reiniciarlo. El esquema tardará alrededor de 60 segundos en actualizarse. Este paso lee la última información del flujo de

trabajo para preparar el paso siguiente, que especifica la información que se moverá del repositorio seguro de identidades al flujo de trabajo que se iniciará.

7 Haga clic en *Aceptar* para actualizar el esquema. Aparecerá un mensaje cuando la actualización del esquema haya finalizado.

8 Haga clic en *Aceptar* para cerrar el mensaje de actualización del esquema. Regresará al recuadro de diálogo *Directiva del Gestor de identidades*.

9 Haga clic en *Atributos que no son específicos de la clase*. Aparecerá el *editor de directivas de asignación de esquema del Gestor de identidades*.



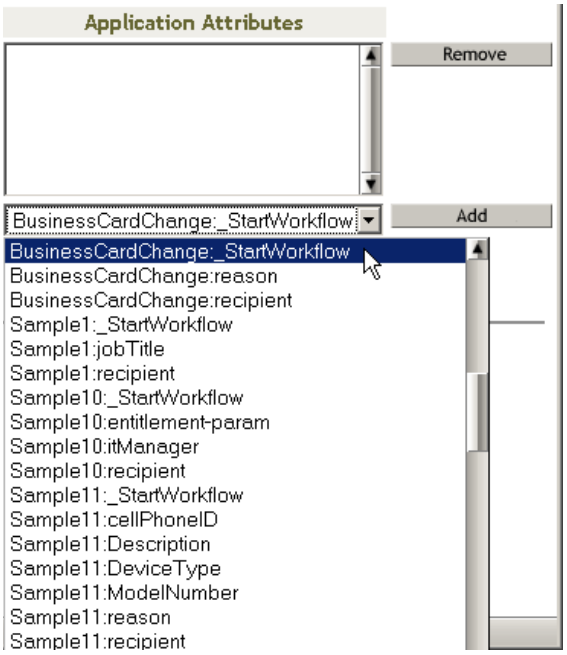
La lista desplegable *Atributos de eDirectory* contiene todos los atributos de eDirectory.

La lista desplegable *Atributos de la aplicación* contiene todos los atributos de todos los flujos de trabajo activos. Los atributos de la lista van precedidos de `AllWorkflows` (lo que significa que el atributo se aplica a todos los flujos de trabajo) o bien del nombre de un flujo de trabajo específico. Si, por ejemplo, desea que el mismo atributo de eDirectory (por ejemplo, `manager`) se asigne al atributo `manager` de todos los flujos de trabajo, asigne `manager` a `Allworkflows:manager`. Si desea que se utilice otro atributo de eDirectory (por ejemplo, `HRmanager`) para un flujo de trabajo específico, asigne el atributo de eDirectory a un atributo del flujo de trabajo específico (por ejemplo, `BusinessCardChange:manager`).

Los atributos asignados se muestran uno al lado del otro en las columnas *Atributos de eDirectory* y *Atributos de la aplicación*.

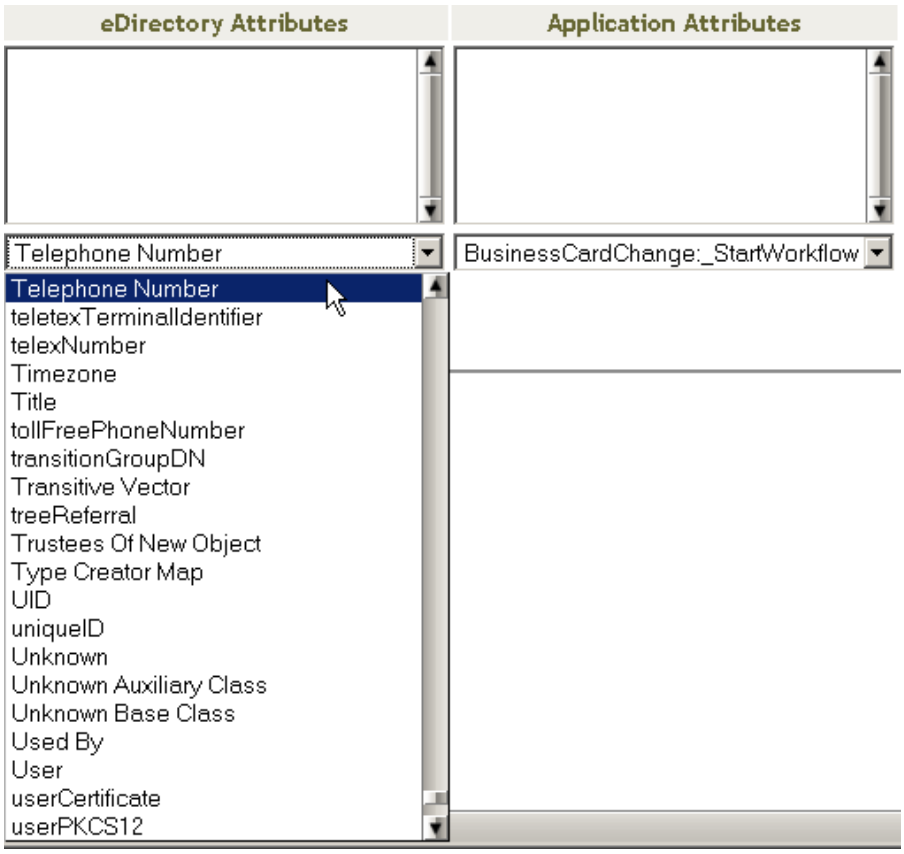
En los pasos siguientes, asignaremos el atributo de eDirectory que deseamos utilizar para iniciar el flujo de trabajo, al atributo _StartWorkflow de dicho flujo de trabajo. Si el flujo de trabajo espera más atributos de eDirectory, deberá asignar también esos atributos. Por ejemplo, si un atributo `Address` de eDirectory sirve para activar un flujo de trabajo, dicho flujo de trabajo también necesitará atributos como `City` y `State`. También es posible asignar estos atributos en directivas.

10 En la lista *Atributos de la aplicación*, seleccione el atributo _StartWorkflow para el flujo de trabajo que desee configurar. El ejemplo siguiente muestra el atributo _StartWorkflow para el flujo de trabajo BusinessCardChange (BusinessCardChange_StartWorkflow).

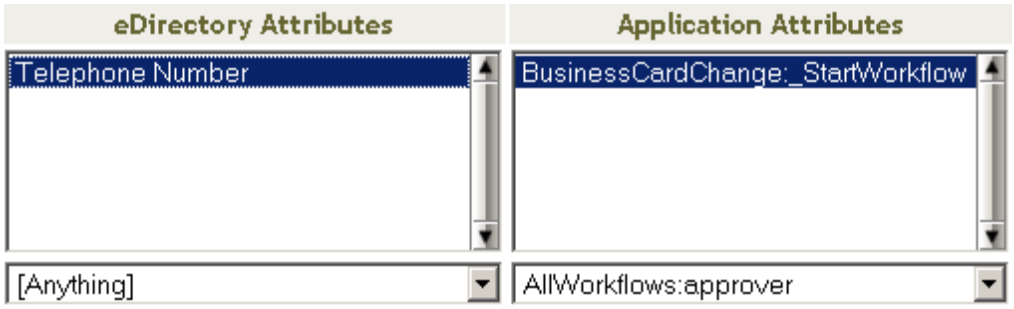


11 En la lista *Atributos de eDirectory*, seleccione el atributo eDirectory que desee utilizar para iniciar el flujo de trabajo cuando el atributo cambie. En el ejemplo siguiente, está seleccionado

el atributo Telephone. Esto significa que el flujo de trabajo BusinessCardChange se iniciará siempre que el número de teléfono de un empleado cambie.



12 Haga clic en *Añadir*. El atributo de eDirectory se asigna al atributo de la aplicación.



13 Si el flujo de trabajo necesita atributos de eDirectory adicionales, repita desde Paso 10 hasta Paso 12 hasta que todos los atributos que necesite estén asignados.

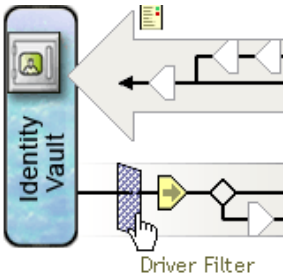
El flujo de trabajo se iniciará automáticamente cuando se produzca un cambio en el atributo de eDirectory asignado a un atributo de aplicación _StartApprovalFlow. No obstante, el atributo sólo llegará a la directiva de asignación de esquema si el atributo de eDirectory está incluido en el filtro del controlador del canal suscriptor. En los pasos siguientes, añadiremos el atributo de eDirectory al filtro del controlador del canal suscriptor.

14 Haga clic en *Aceptar* para cerrar el *editor de directivas de asignación de esquema del Gestor de identidades*.

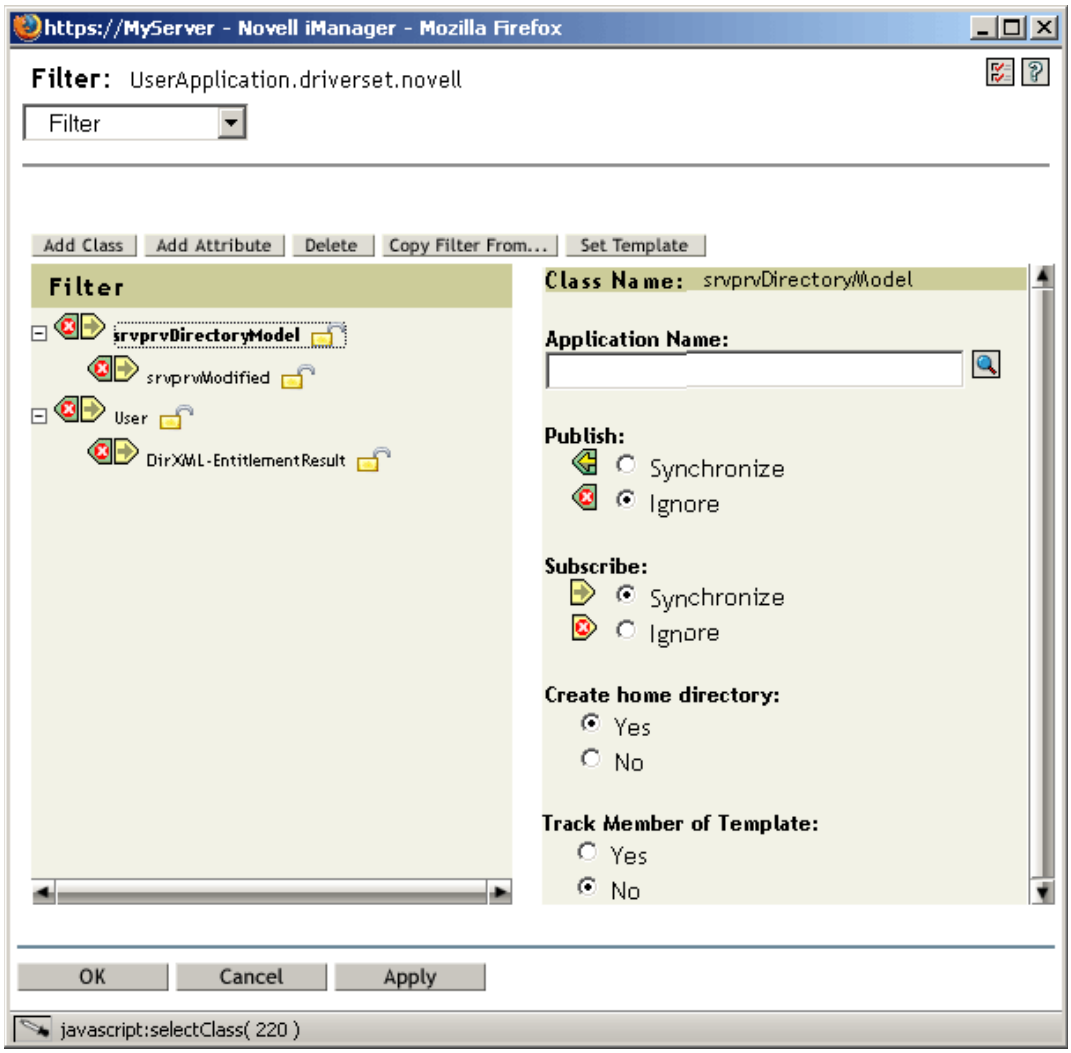
15 Haga clic en *Aceptar* para cerrar el recuadro de diálogo *Directiva del Gestor de identidades*.

16 Haga clic en *Cerrar* para cerrar el recuadro de diálogo de directivas de asignación de esquema.

17 Haga clic en el icono *Filtro del controlador*para el canal suscriptor.



Se visualizará la ventana del filtro:



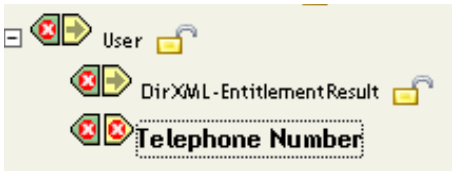
Los filtros de eventos especifican las clases de objetos y los atributos para los que el motor del Gestor de identidades procesa los eventos. La lista de *Filtro* de sólo lectura situada a la

izquierda, muestra los atributos de la clase. La lista *Nombre de clase* situada a la derecha muestra las opciones asociadas al objeto de destino.

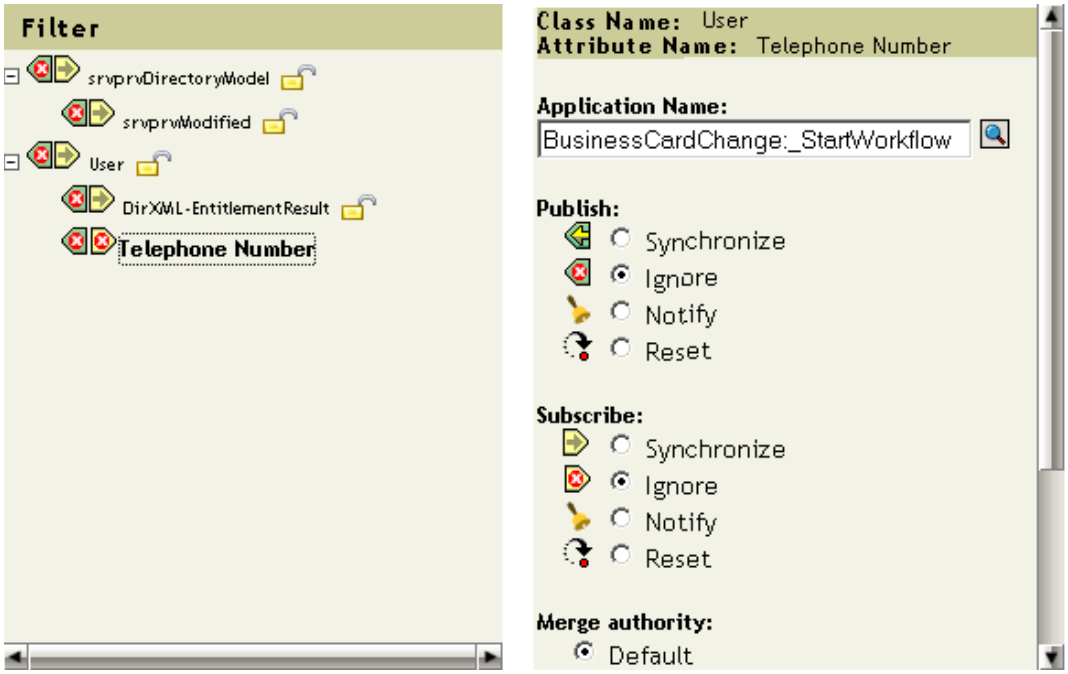
18 Haga clic en el nombre de la clase a la que pertenece el atributo que desea añadir al filtro (por ejemplo, Usuario).

19 Haga clic en *Añadir atributo*. Aparecerá una lista de atributos.

20 Seleccione un atributo y, a continuación, haga clic en *Aceptar*. El atributo se añadirá a la lista *Filtro*.



21 Haga clic en el nombre del atributo. Las opciones de sincronización del atributo se mostrarán en el panel de la derecha.



22 En *Suscribir*, haga clic en *Sincronizar*.

23 Especifique cualquier atributo adicional del filtro. Seleccione *Sincronizar* para un atributo si desea que se notifiquen y sincronicen los cambios de atributos. Seleccione *Ignorar* si no desea que los cambios en los valores de atributo se notifiquen y sincronicen.

24 Haga clic en *Aceptar.* Aparecerá un mensaje que le solicitará si desea que se reinicie el controlador para que los cambios entren en vigor.

25 Haga clic en *Aceptar*. Regresará a la página *Descripción del controlador del Gestor de identidades*.

Configuración del nivel de abstracción del directorio

4

En este capítulo se describe cómo utilizar el editor del nivel de abstracción del directorio para definir los datos del nivel de abstracción del directorio utilizados por la aplicación de usuario del Gestor de identidades. Los temas son:

4.1 Acerca de las definiciones del nivel de abstracción del directorio

El *nivel de abstracción del directorio* es un conjunto de definiciones de datos que aportan una visión lógica de un repositorio seguro de identidades. El nivel de abstracción del directorio define:

- Los objetos y atributos del repositorio seguro de identidades que se pueden utilizar en la aplicación de usuario del Gestor de identidades.
- Cómo se muestran los datos del repositorio seguro de identidades en la interfaz de usuario.
- La relación disponible para el portlet del organigrama corporativo.

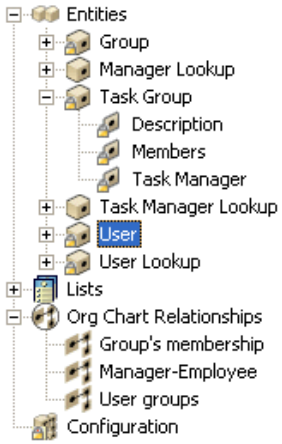
El *editor del nivel de abstracción del directorio* se utiliza para cambiar estas definiciones si se desea modificar la apariencia o el funcionamiento de la aplicación de usuario. Puede cambiarla:

- Añadiendo otros objetos del repositorio seguro de identidades
- Cambiando el conjunto de atributos disponible para una objeto del repositorio seguro de identidades
- Cambiando el contenido de las listas
- Mostrando las diversas relaciones entre los objetos del repositorio seguro de identidades

El procedimiento de instalación de la aplicación de usuario del Gestor de identidades instala e implanta el conjunto base de las definiciones del nivel de abstracción necesarias para que la aplicación de usuario funcione correctamente. Dicha instalación también crea las extensiones del esquema de eDirectory que el controlador de la aplicación de usuario y la aplicación de usuario utilizan. Si desea obtener más información acerca de las extensiones del esquema, consulte Apéndice A, “Extensiones del esquema”, en la página 365. Este mismo conjunto base de archivos se

crea en el sistema de archivos local al crear una nueva instancia del controlador de la aplicación de usuario a través del Diseñador para el Gestor de identidades.

Definiciones de datos del nivel de abstracción de datos obligatorias Cuando empiece a personalizar la aplicación de usuario del Gestor de identidades, probablemente querrá introducir cambios en los objetos del nivel de abstracción del directorio. No obstante, tenga en cuenta que determinados objetos del repositorio seguro de identidades (llamados entidades), atributos, relaciones y listas no se pueden eliminar ni cambiar; de lo contrario, la aplicación de usuario no funcionará correctamente. Las definiciones que no se pueden eliminar, están identificadas mediante un icono de candado. En este ejemplo, verá que la entidad Grupo de tareas y todos sus atributos están bloqueados.



Lugar donde se almacenan las definiciones del nivel de abstracción del directorio Las definiciones del *nivel de abstracción del directorio* son archivos XML que:

- Se *almacenan* localmente en el sistema de archivos de la máquina del diseñador, en el subdirectorio Provisioning\AppConfig\DirectoryModel del proyecto de provisión. Si tiene más de una aplicación de usuario en el proyecto, los nombres de directorio estarán numerados, como, por ejemplo, AppConfig1, AppConfig2, etc.
- Se *implantan* en el contenedor AppConfig.DirectoryModel del controlador de la aplicación de usuario. Los archivos XML se almacenan en el atributo XMLData del objeto de definición del nivel de abstracción del directorio correspondiente. Cada entidad, relación y lista es una instancia de objeto única que se encuentra en el contenedor AppConfig.DirectoryModel del controlador de la aplicación de usuario.
- Se *almacenan en el caché* del servidor de aplicación donde se implanta la aplicación de usuario.

4.2 Inicio

Utilizará las funciones del Diseñador de la vista de provisión del Gestor de identidades y el editor del nivel de abstracción del directorio para definir el contenido del nivel de abstracción del directorio. Siga los pasos siguientes para empezar:

Paso	Tarea	Descripción
1	Cree un proyecto del Gestor de identidades	Esto incluye: ◆ Configurar el repositorio seguro de identidades ◆ Especificar las propiedades del conjunto de controladores Consultar la documentación del Gestor de identidades.
2	Añada un controlador de la aplicación de usuario al modelador	Puede encontrar el controlador de la aplicación de usuario del Gestor de identidades en la carpeta Provisión de la paleta del modelador. 
3	Complete la configuración del controlador de la aplicación de usuario	Consulte el procedimiento Sección 4.2.1, “Configuración del controlador de la aplicación de usuario”, en la página 77.
4	Acceda a la vista de provisión	Consulte Sección 4.2.2, “Acceso a la vista de provisión”, en la página 81.
5	Inicie el editor del nivel de abstracción del directorio	Consulte “Para abrir el editor del nivel de abstracción del directorio:” en la página 82.

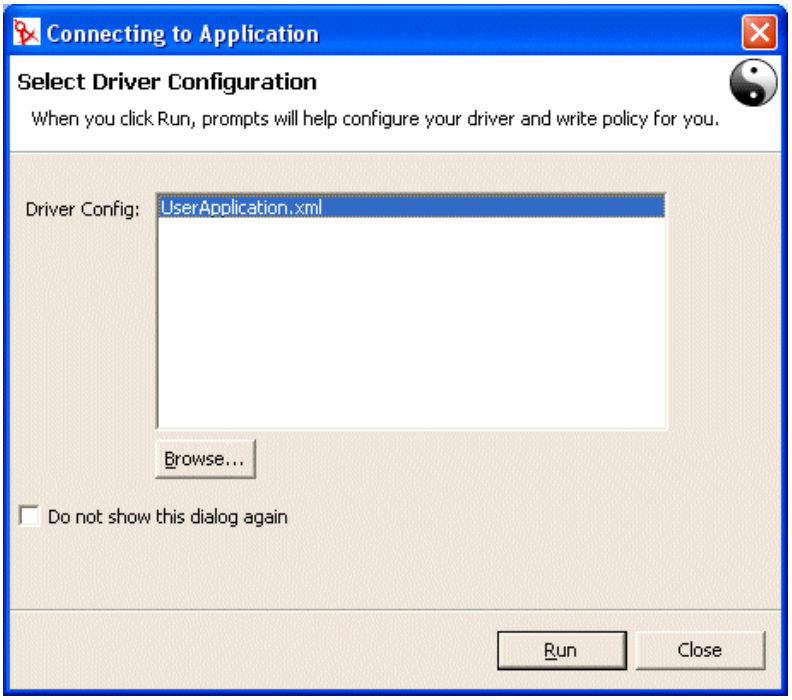
4.2.1 Configuración del controlador de la aplicación de usuario

Siga los pasos siguientes cuando tenga un proyecto del Gestor de identidades creado.

Para completar la configuración del controlador de la aplicación de usuario:

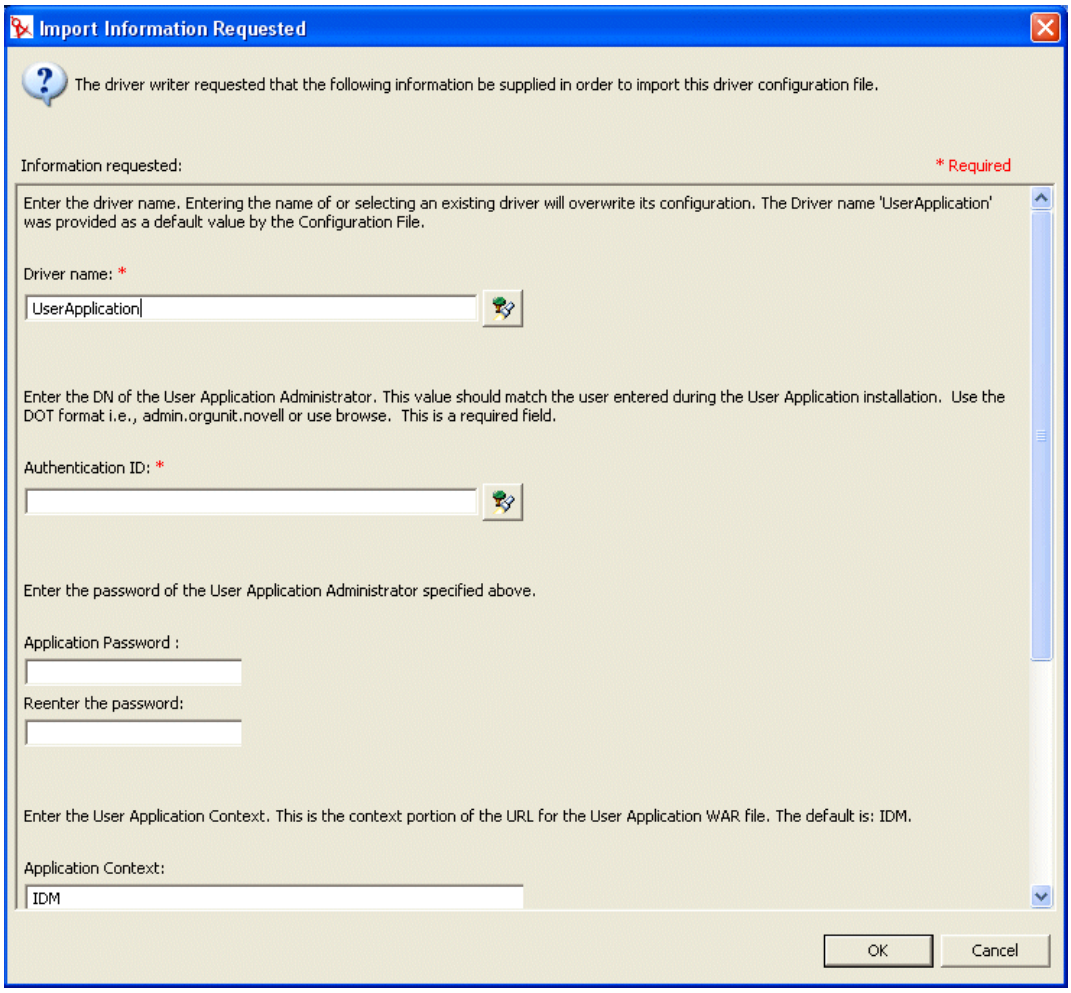
1 Suelte un icono de controlador de la *aplicación de usuario* en el */*lienzo.

El sistema le solicitará una configuración del controlador.



2 Seleccione *UserApplication.xml* (valor por defecto) y, a continuación, haga clic en *Ejecutar*.

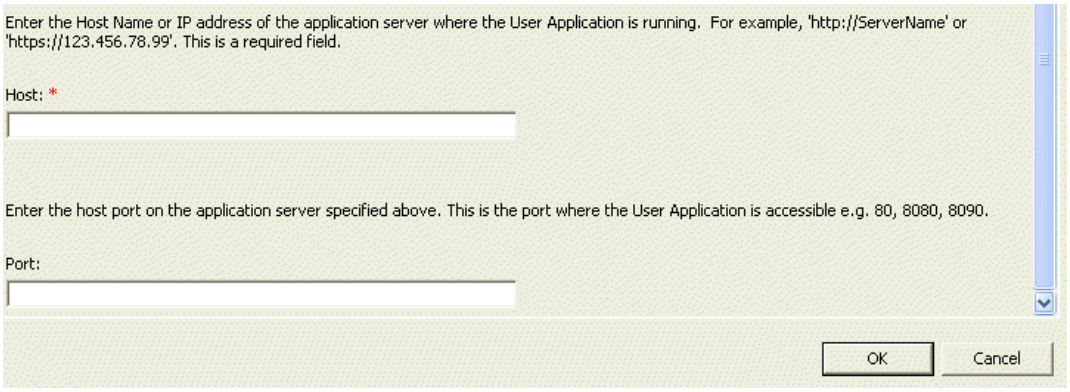
3 Especifique cómo el asistente debe gestionar la validación de las entradas, haciendo clic en Sí o No.



.

.

.



4 Complete el panel como se muestra a continuación:

Propiedad	Datos que se deben especificar
Nombre del controlador	◆ Nombre de un controlador existente (el controlador del conjunto de controladores especificado durante la instalación de la aplicación de usuario). ◆ Nombre de un controlador nuevo.
ID de autenticación	El DN del administrador de la aplicación de usuario.
Contraseña de aplicación/Reintroducir la contraseña	La contraseña del administrador de la aplicación de usuario (arriba)
Contexto de la aplicación	Nombre del contexto de la aplicación de usuario (especificado en el momento de la instalación; por ejemplo, IDM).
Host	Nombre de host o dirección IP del servidor de aplicación en el que se implanta la aplicación de usuario del Gestor de identidades. Esta información se utiliza: ◆ Para iniciar flujos de trabajo en el servidor de aplicación para conectarse a flujos de trabajo de acceso (terminar, retraer, etc.). ◆ Para actualizar las definiciones de los datos en caché.
Puerto	Puerto del host anterior.

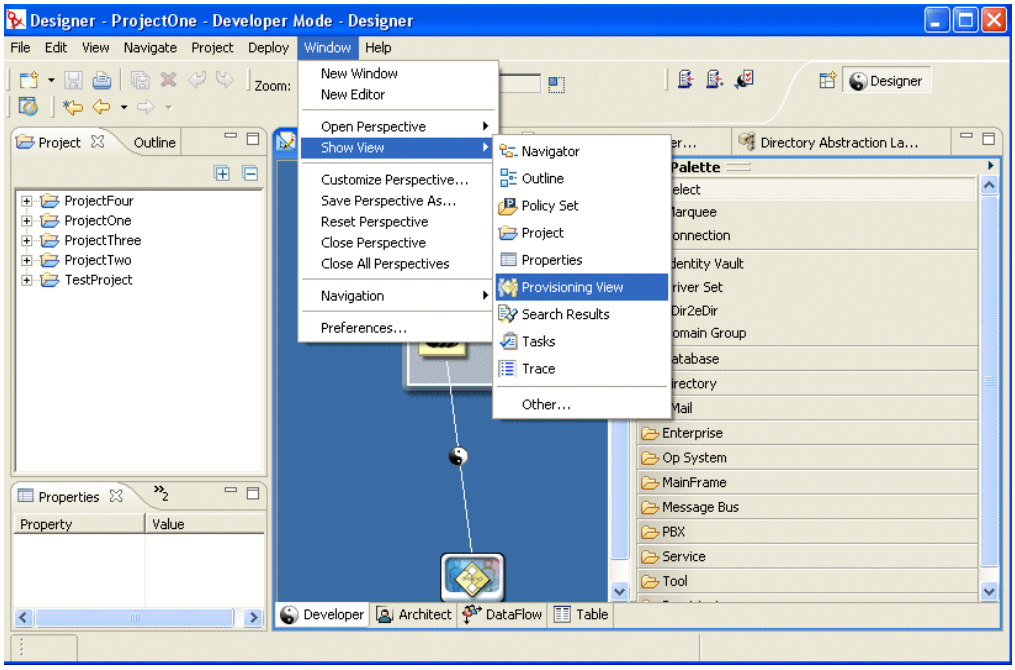
5 Haga clic en *Aceptar*.

4.2.2 Acceso a la vista de provisión

Para acceder a la vista de provisión.

1 Seleccione uno de los métodos siguientes:

- Seleccione *Ventana>Mostrar vista>Vista de provisión*.



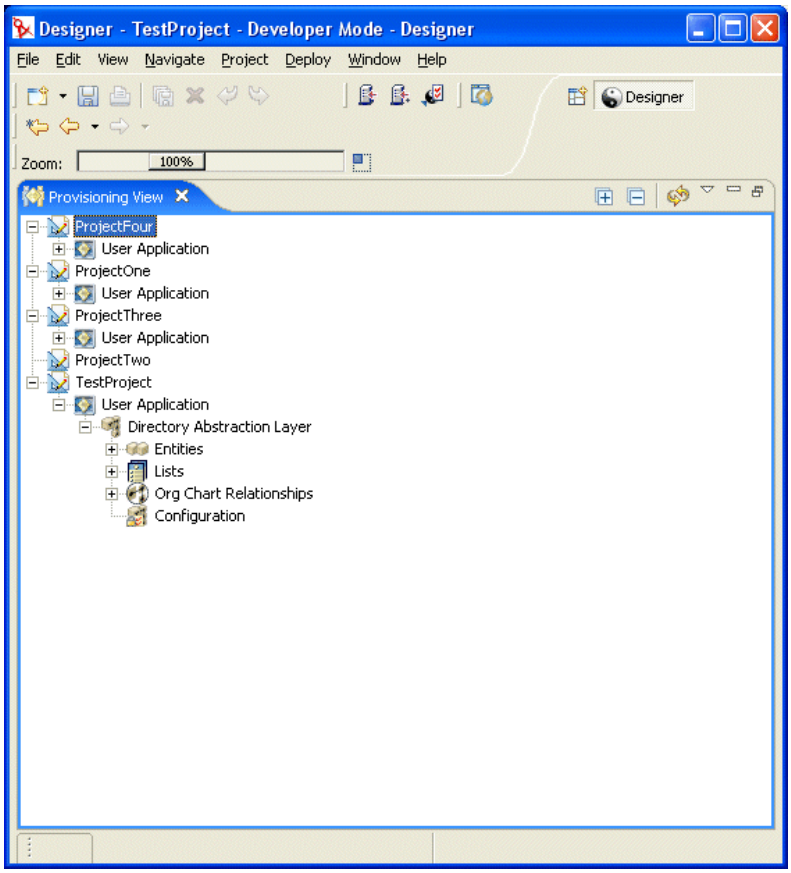
- Abra la carpeta *Provisión* y seleccione *Vista de provisión*.
- Haga clic en *Aceptar*.

o

- Seleccione el icono de la aplicación de usuario, haga clic con el botón derecho del ratón y seleccione *Aplicación>Mostrar la vista de provisión*.

En la vista de provisión, verá el proyecto que acaba de crear junto con los proyectos de provisión restantes que se encuentran en el mismo espacio de trabajo.

Sugerencia: Si no ve en la vista las aplicaciones que espera, *podría* deberse a que el proyecto está dañado. En dicho caso, deberá volver a crearlo.



Acerca de la vista de provisión

La vista de provisión proporciona un acceso persistente a las funciones de provisión. Si hace doble clic en un elemento de dicha vista, se abrirá el editor del elemento. Utilice la vista de provisión para ejecutar las acciones siguientes con las definiciones del nivel de abstracción del directorio:

- *Importe* una o varias definiciones de objetos del repositorio seguro de identidades.
- *Valide* la estructura de las definiciones de datos.
- *Implante* las definiciones en el repositorio seguro de identidades especificada en el proyecto.
- *Cree y suprima* definiciones del nivel de abstracción del directorio.

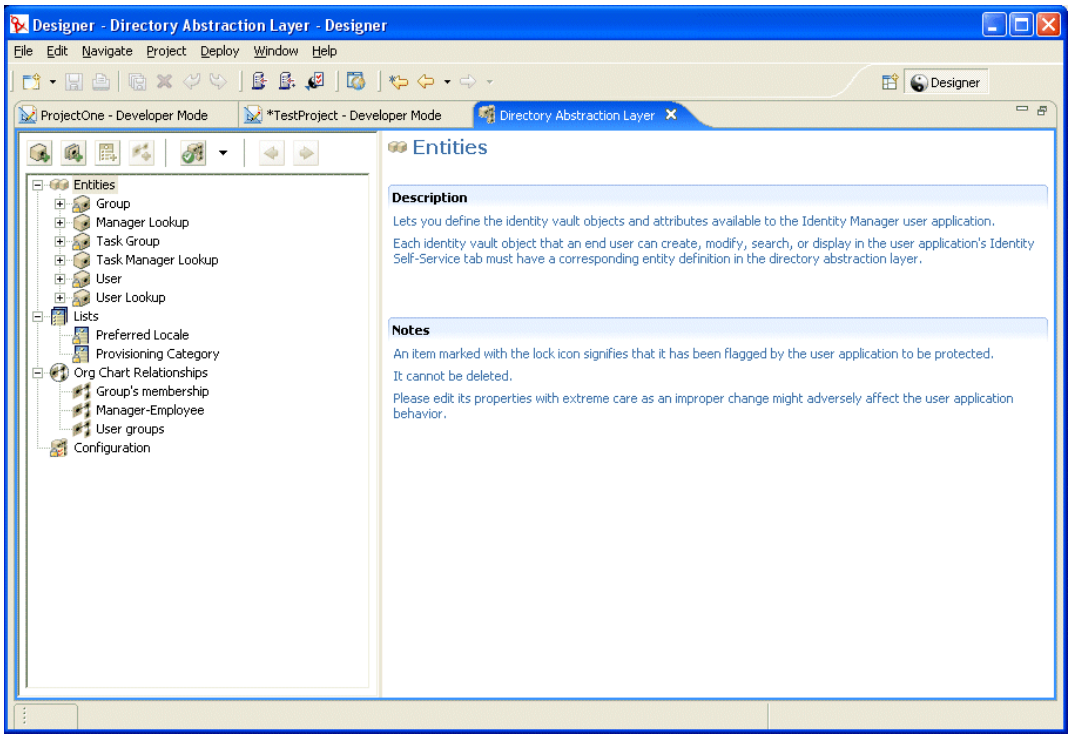
Si desea obtener más información, consulte Sección 4.8, “Importación, validación e implantación de las definiciones del nivel de abstracción del directorio”, en la página 111.

4.2.3 Inicio del editor del nivel de abstracción del directorio

Para abrir el editor del nivel de abstracción del directorio:

1. Con la *Vista de provisión* abierta, desplácese hasta el nodo del nivel de abstracción del directorio.
2. Haga doble clic en dicho nodo.

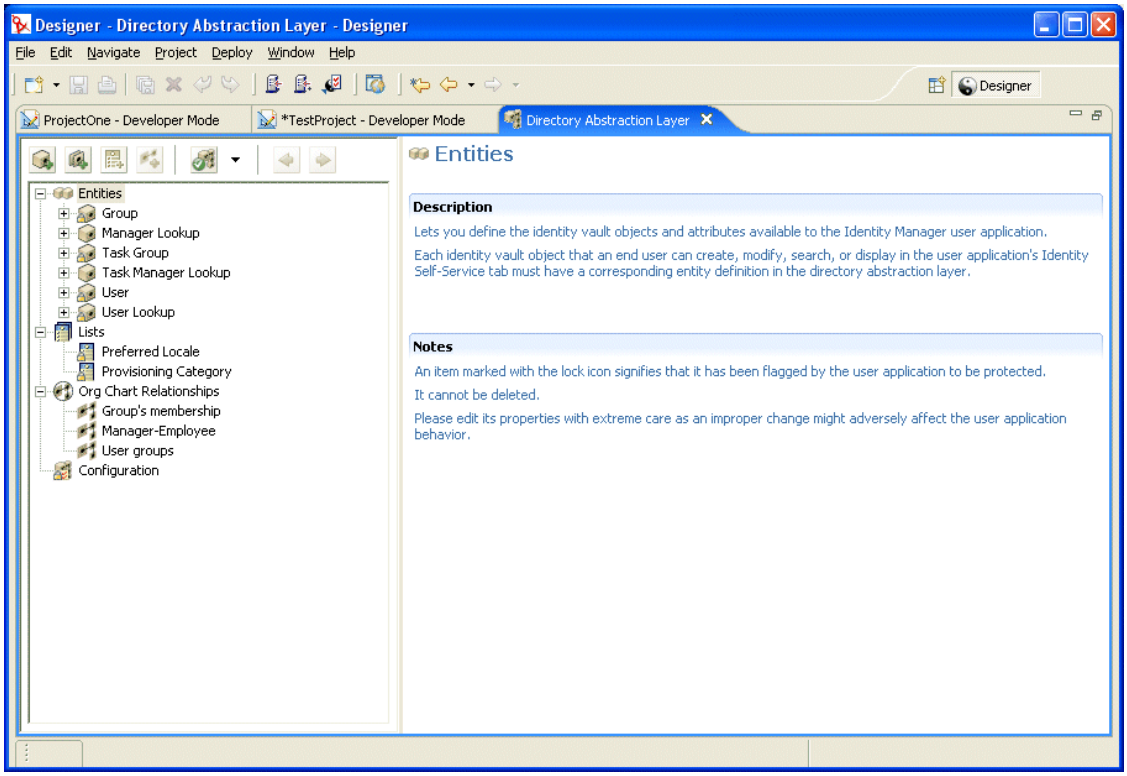
Verá un árbol que contiene entidades, listas, relaciones del organigrama corporativo y configuración.



Acerca del editor del nivel de abstracción del directorio

El editor del nivel de abstracción del directorio proporciona una forma gráfica de definir un conjunto de archivos XML que forman el nivel de abstracción del directorio. Dicho editor es una herramienta basada en Eclipse a la que se puede acceder desde la *vista de provisión* de un proyecto del Gestor de identidades.

Cuando abra por primera vez el editor del nivel de abstracción del directorio, verá un conjunto base de objetos del nivel de abstracción que se crea automáticamente cada vez que se crea un proyecto de provisión nuevo:



Los nodos del editor del nivel de abstracción del directorio son:

Elemento	Descripción
Entidades	Las entidades representan los objetos del repositorio seguro de identidades configurados para este proyecto y disponibles para la aplicación de usuario. Existen dos tipos de entidades: ◆ **Las entidades que se asignan desde el esquema**. Dichas entidades representan objetos que existen en el repositorio seguro de identidades y que se exponen directamente a los usuarios a través de la aplicación de usuario. Normalmente, los usuarios pueden crear, buscar y modificar los atributos de estos tipos de objetos. ◆ **Entidades que representan las relaciones LDAP**. También llamadas DNLookup. Dichas entidades representan búsquedas indexadas y se utilizan para dar soporte a determinados tipos de atributos que se desea exponer. Las entidades DNLookup proporcionan información acerca de las relaciones entre objetos LDAP. Dichas entidades son utilizadas por: ◆ El portlet del organigrama corporativo para determinar las relaciones. ◆ Los portlets de la lista de búsqueda, creación e información para proporcionar listas de selección emergentes y contextos de DN. Si desea obtener más información, consulte Sección 4.3.3, “Definición de entidades”, en la página 88.
Listas	Permite definir el contenido de las listas globales. Las listas globales: ◆ Están asociadas a un atributo. Cuando el atributo se muestra en la aplicación de usuario, está como lista desplegable. ◆ Se utilizan para mostrar las categorías utilizadas por el módulo auxiliar de configuración de peticiones de provisión en iManager. Si desea obtener más información, consulte Sección 4.4, “Funcionamiento con listas”, en la página 104.
Relaciones de los organigramas corporativos	Utilizado por la acción Organigrama corporativo de la pestaña Autoservicio de identidades de la aplicación de usuario. Permite asignar relaciones jerárquicas entre entidades del esquema. Si desea obtener más información, consulte Sección 4.5, “Funcionamiento con relaciones de los organigramas corporativos”, en la página 106.
Configuración	Parámetros de configuración general. Si desea obtener más información, consulte Sección 4.6, “Trabajo con los ajustes de configuración”, en la página 110.

Donde los archivos XML se almacenan localmente El editor del nivel de abstracción del directorio genera un archivo XML único por cada entidad, lista o relación. Los archivos se

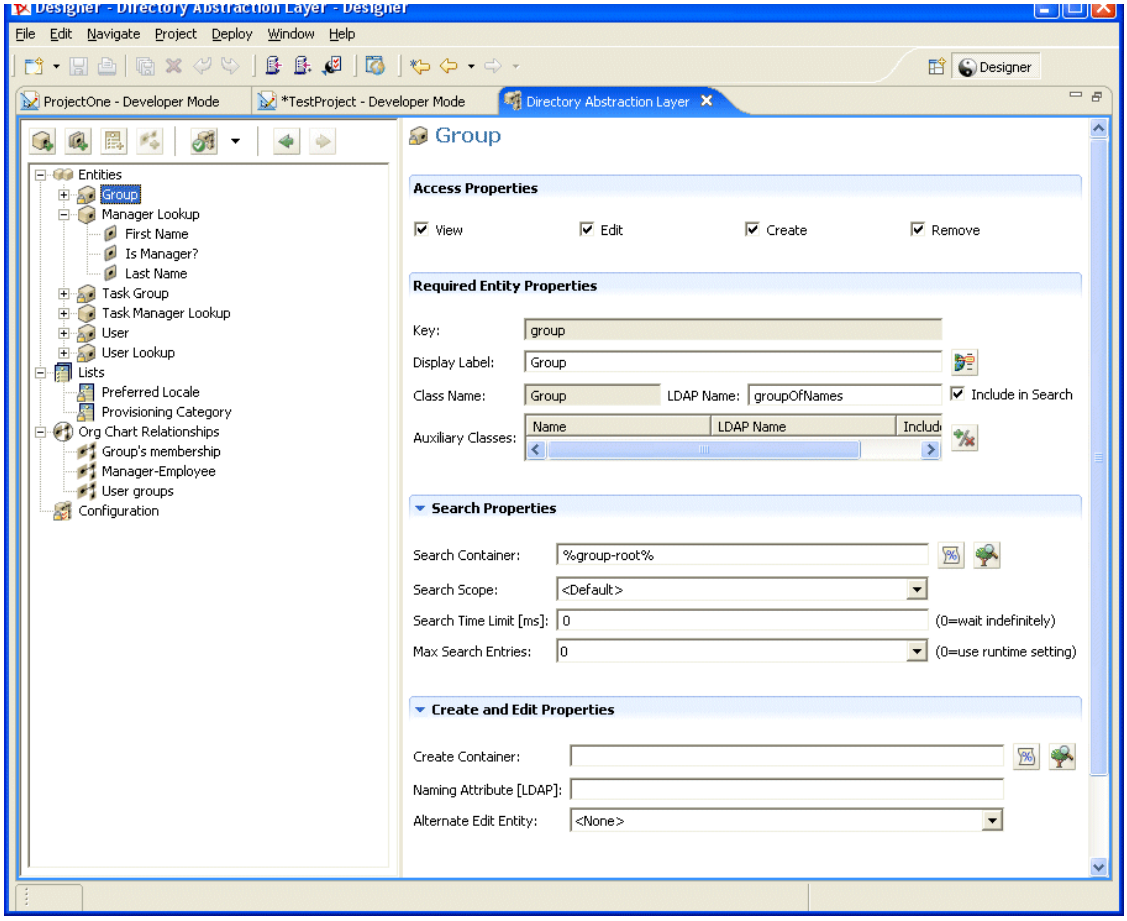
almacenan en la carpeta */*Provisioning\AppConfig\DirectoryModel del proyecto. El nombre del archivo se basa en la clave del objeto. Incluyen:

Directorio	Descripción
ChoiceDefs	Contiene los archivos que definen las listas globales. Los archivos tienen la extensión .choice.
EntityDefs	Contiene los archivos que definen las entidades y atributos. Los archivos tienen la extensión .entity.
RelationshipDefs	Contiene los archivos que definen las relaciones disponibles en el portlet del organigrama corporativo. Estos archivos tienen la extensión .relation.

Utilice las funciones del editor del nivel de abstracción del directorio para añadir nuevas definiciones que modelen su propio esquema de repositorio seguro de identidades. Utilice las funciones de la *vista de provisión* para implantar las nuevas definiciones en el repositorio seguro de identidades.

Utilización del editor del nivel de abstracción del directorio

El editor del nivel de abstracción del directorio está dividido en dos paneles. El panel de la izquierda muestra una vista del contenido del nivel de abstracción del directorio. Si selecciona un elemento del panel izquierdo, el panel derecho mostrará los atributos y valores del elemento seleccionado.



4.3 Funcionamiento de las entidades y los atributos

Todo objeto del repositorio seguro de identidades que desea que los usuarios busquen, muestren o editen en la aplicación de usuario del Gestor de identidades, debe estar definido como *entidad* en el nivel de abstracción del directorio. Por ejemplo, para utilizar el objeto inetOrgPerson del repositorio seguro de identidades de la aplicación de usuario, deberá crear una definición de entidad para él.

4.3.1 Pasos necesarios para añadir entidades

Siga los pasos que indicamos a continuación, para añadir entidades en el nivel de abstracción del directorio:

Paso	Tarea	Para más información
1	Decida qué objetos del repositorio seguro de identidades va a utilizar en la aplicación de usuario	Sección 4.3.2, “Análisis de las necesidades de datos”, en la página 87
2	Utilice el editor del nivel de abstracción del directorio para definir los objetos del repositorio seguro de identidades del nivel de abstracción del directorio	Sección 4.3.3, “Definición de entidades”, en la página 88
3	Utilice la vista de provisión para dar validez a las definiciones de datos	Sección 4.8, “Importación, validación e implantación de las definiciones del nivel de abstracción del directorio”, en la página 111
4	Implante las definiciones en el repositorio seguro de identidades	Sección 4.8.3, “Acerca de la implantación”, en la página 114
5	Actualice el caché del servidor de aplicación para que incluya las nuevas definiciones del nivel de abstracción	Capítulo 13, “Configuración del almacenamiento en caché”, en la página 219
6	Pruebe la aplicación de usuario del Gestor de identidades para asegurarse de que los cambios se visualizan correctamente	

4.3.2 Análisis de las necesidades de datos

Para modelar los datos del repositorio seguro de identidades del nivel de abstracción del directorio, necesitará saber:

- Las *partes del directorio* que desea que estén disponibles para la aplicación de usuario del Gestor de aplicaciones.

Por ejemplo, la lista de objetos que el usuario puede buscar y visualizar. Compruebe esta lista comparándola con el conjunto básico de definiciones del nivel de abstracción para determinar qué necesita añadir.

- La *estructura del esquema* incluidas las extensiones personalizadas y las clases auxiliares
- La *estructura de los datos* incluido:
  - Qué es obligatorio y qué es opcional

- Reglas de validación
- Relaciones entre objetos (referencias de DN)
- Cómo se definen los atributos (por ejemplo, un atributo que representa un número de teléfono puede tener varios valores para el hogar, la oficina y el inalámbrico)

- Quién verá los datos

  ¿Se trata de un sitio público o privado?

Una vez disponga de esta información, podrá utilizarla para asignar los objetos del repositorio seguro de identidades a las entidades del nivel de abstracción.

Nota: Las ACL de eDirectory se pueden aplicar a todos los objetos del nivel de abstracción. Los derechos efectivos sobre objetos y atributos se basan en el usuario autenticado establecido en la entrada a la aplicación.

4.3.3 Definición de entidades

Según lo que quiera exponer en la aplicación de usuario, tendrá que definir dos tipos de entidades:

- *Entidades que se asignan desde el esquema*. Dichas entidades representan objetos que existen en el repositorio seguro de identidades y que están expuestos directamente a los usuarios en la aplicación de usuario. Cuando defina este tipo de entidad, expondrá todos los atributos con los que desea que los usuarios trabajen. Ejemplos de este tipo de entidad: usuario, grupo y grupo de tareas. También se puede crear más de una definición de entidad para el mismo objeto, si desea exponer diferentes conjuntos de atributos a diferentes tipos de usuarios. Si desea obtener más información, consulte "Creación de varias definiciones de identidad para un único objeto" en la página 88.
- *Entidades que representan relaciones LDAP*. Este tipo de entidad es conocido como DNLookup y la aplicación de usuario la utiliza para:
  - Cumplimentar una lista con los resultados de una búsqueda de nombre completo entre las entidades relacionadas
  - Mantener una integridad de referencia en los atributos de referencia de DN durante las actualizaciones y supresiones

  El portlet del organigrama corporativo utiliza las entidades que admiten DNLookup para determinar las relaciones; también las utilizan los portlets de búsqueda, creación e información para proporcionar listas de selección emergentes y contextos de DN. Ejemplos de este tipo de entidad: búsquedas de supervisores, búsquedas de supervisores de tareas y búsquedas de usuarios. Si desea obtener más información, consulte "Utilización de los tipos de control de DNLookup" en la página 100.

Creación de varias definiciones de identidad para un único objeto

Puede crear más de una definición de entidad que represente el mismo objeto del repositorio seguro de identidades, pero que proporcione una vista diferente de los datos. Dentro de las definiciones de entidad puede:

- *Definir diferentes atributos* por cada definición de entidad

O

- *Definir los mismos atributos*, pero especificar diferentes propiedades de acceso que controlen cómo se buscan, ven, editan u ocultan los atributos

---

Nota: La definición de una entidad puede incluir opcionalmente un filtro para ocultar determinadas entidades del conjunto de resultados.

Por consiguiente, puede utilizar diferentes definiciones de una entidad en diferentes partes de la interfaz de usuario. Por ejemplo, supongamos que desea crear un directorio de empleados; uno para un sitio público y otro para un sitio interno. En el sitio público quiere indicar el nombre y apellidos y un número de teléfono, mientras que en el interno, desea indicar información adicional como el cargo, supervisores, etc. A continuación, indicamos cómo debe efectuarse:

1. Cree dos definiciones de entidad (con claves diferentes).

   Ambas definiciones de entidad exponen el mismo objeto del repositorio seguro de identidades, pero una clave de la definición de entidad es información pública del personal, mientras que la otra es información interna del personal.

2. Dentro de cada definición de entidad, defina un conjunto de atributos diferente: uno para la información pública del personal y otro para la información interna.
3. Utilice la pestaña Administración del portal de la aplicación de usuario del Gestor de identidades para crear una instancia del portlet para la página pública y otra para la página interna.

   Si desea obtener más información acerca de cómo crear instancias del portlet, consulte el Capítulo 9, “Administración de portlets”, en la página 179.

Procedimientos para crear definiciones de entidades

Una vez haya determinado las entidades y atributos que desea exponer, empiece a añadirlos al nivel de abstracción del directorio utilizando el editor. Seguirá una serie de pasos como los que indicamos a continuación:

Paso	Operaciones que puede realizar	Consulte este procedimiento
1.	Decida con qué conjunto de archivos desea empezar.	
	◆ Desea añadir el conjunto básico de definiciones	Sección 4.3.1, “Pasos necesarios para añadir entidades”, en la página 87
	◆ Desea empezar por las definiciones que ya están implantadas	Sección 4.8.1, “Acerca de la importación”, en la página 112
1a.	Algunas de las entidades que desea utilizar no forman parte del esquema básico de eDirectory. Las extensiones del esquema de eDirectory no aparecerán automáticamente en la lista del editor de objetos y atributos seleccionables. Esto significa que tendrá que actualizar el archivo del esquema local del diseñador para incluir estos objetos y atributos personalizados.	“Para actualizar la lista de elementos del esquema disponibles:” en la página 90
2.	Añada una o varias entidades al nivel de abstracción del directorio	“Añadir entidades” en la página 90

Paso	Operaciones que puede realizar	Consulte este procedimiento
3.	Añada atributos a las entidades	“Adición de atributos” en la página 93

Actualización de la lista de elementos del esquema disponibles

Para actualizar la lista de elementos del esquema disponibles:

1. Con el proyecto del Gestor de identidades abierto, seleccione el repositorio seguro de identidades, haga clic con el botón derecho del ratón y seleccione *Operaciones en directo>Importar esquema*.
2. Seleccione *Importar desde eDirectory* y suministre las especificaciones para el host de eDirectory.
3. Haga clic en *Siguiente*.
4. Seleccione las clases y atributos que desee importar y haga clic en *Finalizar*.

Añadir entidades

Una entidad se puede añadir a través del asistente para añadir entidades (descrito a continuación) o haciendo clic en el botón *Añadir entidad* de la barra de herramientas del editor.

Nota: Cuando utilice el botón Añadir entidad, el sistema le solicitará que seleccione la clase de objeto de la entidad que desea crear. El editor añadirá automáticamente los atributos necesarios a la entidad. A continuación, podrá utilizar el diálogo Añadir atributo para completar la definición de entidad.

Para añadir una entidad utilizando el asistente para añadir entidades:

1. Lance el asistente para añadir entidades ejecutando uno de los métodos siguientes:

   Desde la *Vista de provisión*:

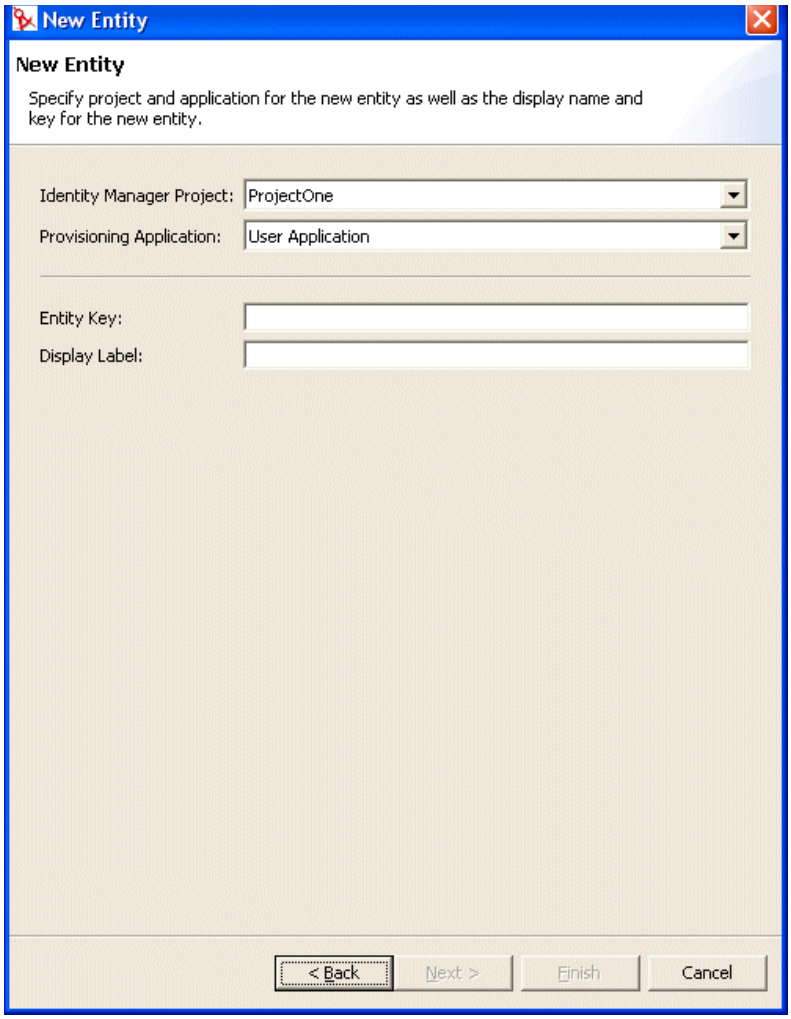
   - Seleccione el nodo *Entidades*, haga clic con el botón derecho del ratón y seleccione *Nuevo*.
   - Seleccione *Archivo>Nuevo>Provisión*. Seleccione *Entidad del nivel de abstracción del directorio*. Haga clic en *Siguiente*.

   En el editor del nivel de abstracción del directorio:

   - Seleccione el nodo *Entidades*, haga clic con el botón derecho del ratón y seleccione *Asistente para nuevos atributos de la entidad*.

     Se mostrará el diálogo Entidad nueva.

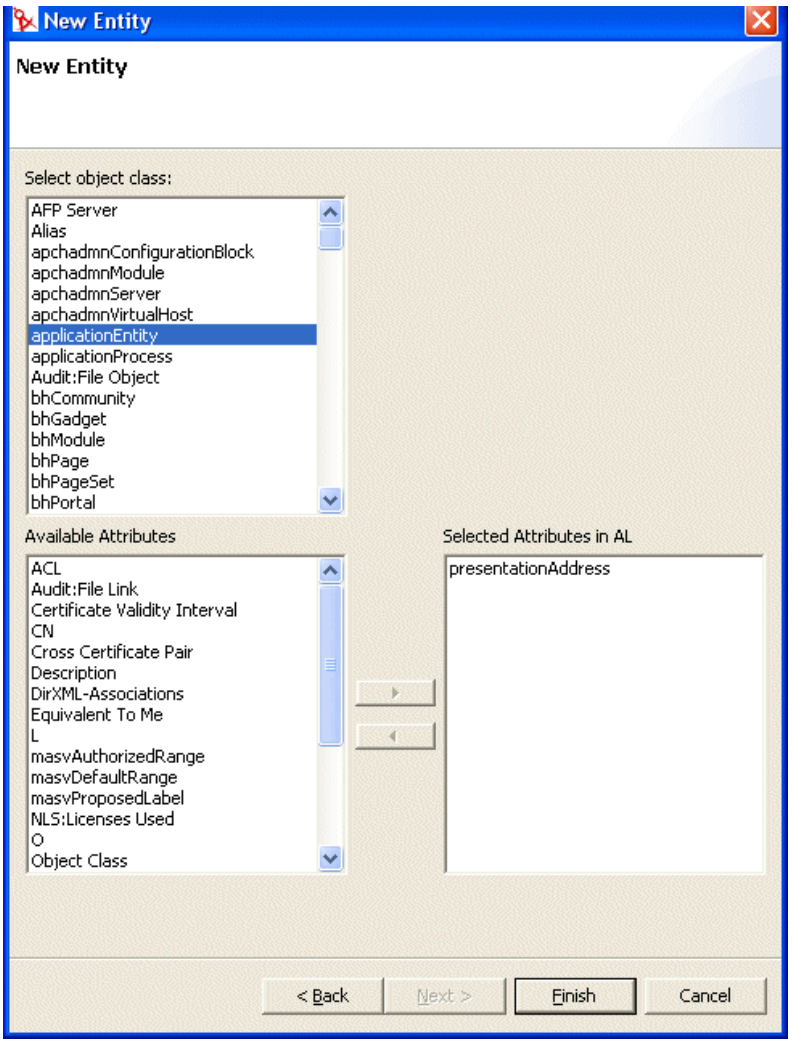
   Nota: Si se inicia desde el menú Archivo, el diálogo contendrá campos que no aparecen cuando se lanza siguiendo alguno de los otros métodos. A continuación, lo mostramos.



2 Complete el panel como se muestra a continuación:

Campo	Descripción
Aplicación de provisión y proyecto del Gestor de identidades	Seleccione la aplicación de provisión y el proyecto del Gestor de identidades donde desea añadir la entidad y los atributos. **Nota:** Estos campos se visualizan cuando se lanza el asistente desde el menú Archivo.
Clave de entidad	Identificador exclusivo de la entidad.
Etiqueta de visualización	La cadena que se muestra siempre que se hace referencia a la entidad en la interfaz de usuario.

3 Haga clic en *Siguiente*. Se mostrará el diálogo Entidad nueva:



4 Seleccione la clase de objeto para la entidad que desea crear y, a continuación, seleccione los atributos en la lista Atributos disponibles

---

Sugerencia: Si la clase de objeto de la entidad que desea crear no se muestra en la lista de clases de objetos disponibles, es posible que deba actualizar el archivo local de esquema del diseñador. Siga los pasos descritos en "Para actualizar la lista de elementos del esquema disponibles:" en la página 90.

---

5 Haga clic en *Finalizar*.

Se mostrará la hoja de propiedades para editarla.

Si desea obtener más información, consulte "Referencia de la propiedad de una entidad" en la página 94.

Nota: Para que el atributo esté disponible para la aplicación de usuario, debe implantar la entidad que contiene el atributo.

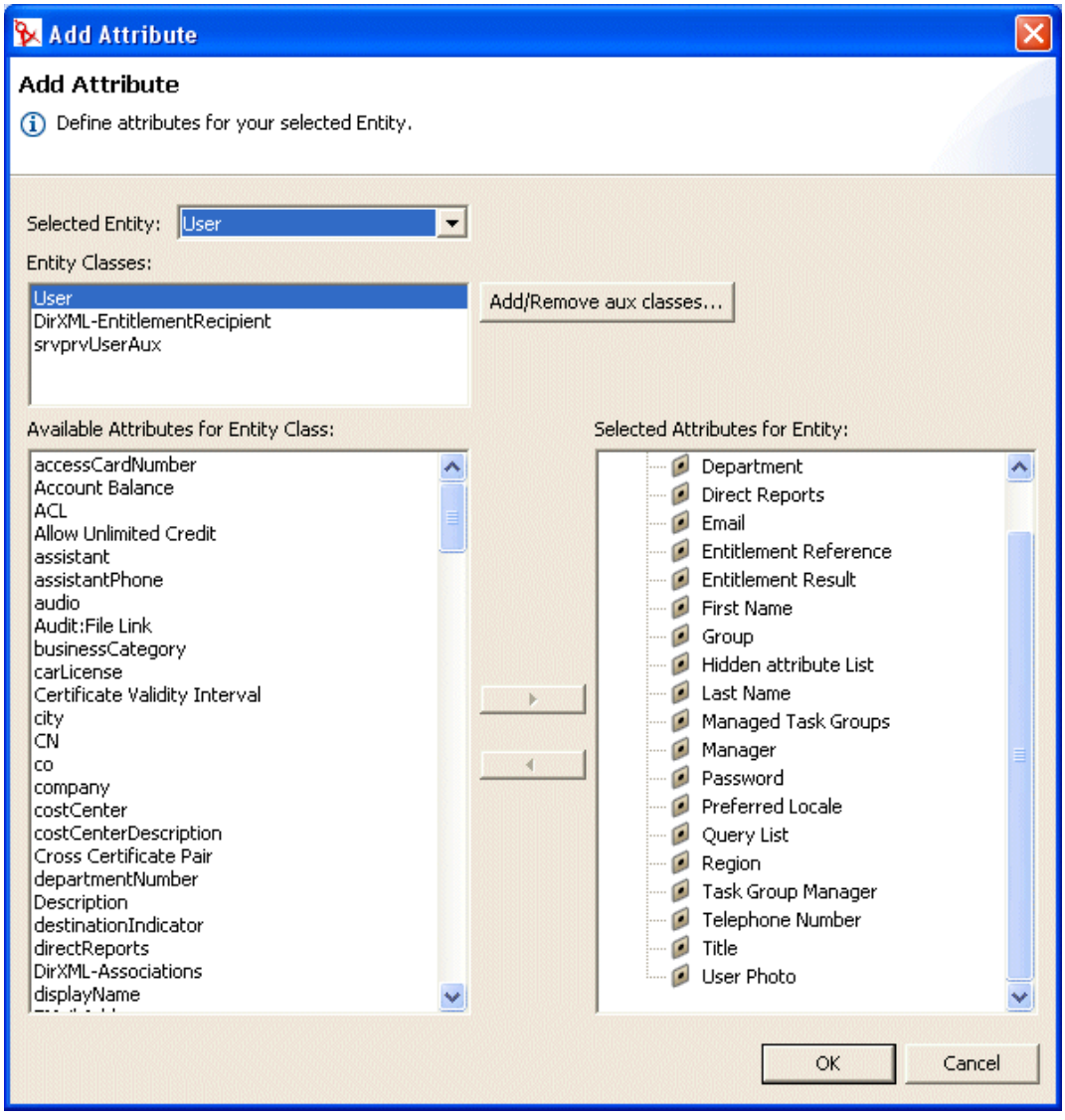
Adición de atributos

Para añadir un atributo:

1. Seleccione una entidad.
2. Añada un atributo:
   - Haciendo clic con el botón derecho y seleccionando *Añadir atributo*.

   o
   - Haciendo clic en el icono *Añadir atributo*.

   El sistema le solicitará lo siguiente:



3. Seleccione el atributo en la lista *Atributos disponibles para la clase de entidad* y añádalo a la lista *Atributos seleccionados para la entidad* .

Sugerencia: Si el atributo que desea crear no se muestra en la lista de atributos disponibles para la clase de entidad, es posible que deba actualizar el archivo local de esquema del diseñador. Siga los pasos descritos en "Para actualizar la lista de elementos del esquema disponibles:" en la página 90.

4 Haga clic en *Aceptar*.

Se mostrará la hoja de propiedades para editarla.

Si desea obtener más información, consulte "Referencia de la propiedad de un atributo" en la página 97.

Nota: Para que el atributo esté disponible para la aplicación de usuario, debe implantarlo.

Referencia de la propiedad de una entidad

Puede definir los tipos de propiedades siguientes en las entidades:

- "Propiedades de acceso de la entidad" en la página 94
- "Propiedades obligatorias de la entidad" en la página 94
- "Propiedades de búsqueda de la entidad" en la página 95
- "Propiedades de creación y edición de entidades" en la página 96
- "Propiedades de gestión de contraseñas" en la página 96

Propiedades de acceso de la entidad

Las *propiedades de acceso* controlan cómo la aplicación de usuario interactúa con la entidad. Incluyen:

Propiedad	Descripción
Crear	**Seleccionado**: la aplicación de usuario puede crear este objeto.
Editar	**Deseleccionado**: la aplicación de usuario no puede cambiar este objeto, sin tener en cuenta las ACL subyacentes. **Seleccionado**: este objeto se puede cambiar, pero las ACL del repositorio seguro de identidades deberán utilizarse para determinarlo.
Ver	**Seleccionado**: la aplicación de usuario puede visualizar este objeto.
Eliminar	**Seleccionado**: la aplicación de usuario puede suprimir este objeto.

Propiedades obligatorias de la entidad

Las propiedades *obligatorias* de la entidad son:

Nombre de propiedad	Descripción
Clave	Identificador exclusivo de esta entidad. Define la forma en que la aplicación de usuario hará referencia a este objeto.
Etiqueta de visualización	Define cómo se muestra el objeto en la interfaz de usuario.

Nombre de propiedad	Descripción
Nombre de clase	El nombre de clase de los Servicios del Directorio de Novell (NDS).
Nombre LDAP	El nombre de la clase de objeto LDAP.
Buscar	**Seleccionado**: se puede buscar esta entidad. Las entidades utilizadas en las consultas por los portlets de identidad (como la lista de búsqueda entidades o el organigrama corporativo de entidades) deben estar seleccionadas (true).
Clases auxiliares	Una lista de cero o más clases auxiliares para esta entidad. Si va a añadir clases auxiliares, deberá especificar el nombre LDAP de la clase auxiliar, el nombre NDS y si se pueden o no buscar.

Propiedades de búsqueda de la entidad

Las *propiedades de búsqueda de la entidad* son:

Nombre de propiedad	Descripción
Buscar en contenedor	Nombre completo del nodo LDAP o contenedor donde se inicia la búsqueda (la raíz de búsqueda). Por ejemplo: `ou=sample,o=ourOrg` Puede desplazarse por el repositorio seguro de identidades para seleccionar el contenedor o utilizar uno de los parámetros predefinidos descritos en “Uso de parámetros predefinidos” en la página 97.
Ámbito de búsqueda	Especifica dónde se realizará la búsqueda en relación con la raíz de búsqueda. Los valores son: **<Por defecto>**: este ámbito de búsqueda equivale a seleccionar Contenedores y subcontenedores. **Contenedor**: la búsqueda se realiza en el DN de la raíz de búsqueda y todas las entradas del nivel raíz de búsqueda. **Contenedor y subcontenedores**: la búsqueda se realiza en el DN de la raíz de búsqueda y en todos los subcontenedores. Equivale a seleccionar **<Por defecto>.** **Objeto**: limita la búsqueda al objeto especificado. Esta búsqueda se realiza para verificar la existencia del objeto especificado.
Límite de tiempo de búsqueda[ms]	Especifique un valor en milisegundos o especifique 0 para indicar sin límite de tiempo.

Nombre de propiedad	Descripción
Máximo de entradas de búsqueda	Especifique el número máximo de entradas que desea que la búsqueda devuelva. Especifique 0 si desea utilizar el valor de tiempo de ejecución. Recomendaciones: Para obtener una mayor eficiencia, defina **entre 100 y 200** **No** defina más de 1000

Propiedades de creación y edición de entidades

Las *propiedades de creación y edición de entidades* son:

Nombre de propiedad	Definición
Crear contenedor	El nombre del contenedor donde se creará una entidad nueva de este tipo. Puede desplazarse por el repositorio seguro de identidades para seleccionar el contenedor o utilizar uno de los parámetros predefinidos descritos en “Uso de parámetros predefinidos” en la página 97. Si no se especifica este valor, el portlet de creación solicitará al usuario que especifique un contenedor para el objeto nuevo. El portlet utilizará la raíz de búsqueda especificada en la definición de la entidad como base y permitirá que el usuario profundice desde ese punto. Si no se ha especificado ninguna raíz de búsqueda en la definición de entidad, utilizará el DN de raíz especificado durante la instalación de la aplicación de usuario.
Atributo Denominación	El atributo Denominación de la entidad (el nombre completo relativo (RDN)). Este valor sólo es necesario para las entidades en las que se ha seleccionado el parámetro de acceso Create.
Entidad de edición alternativa	Los atributos de la entidad de edición se muestran en el modo de edición del portlet de información. Seleccione una entidad en la lista desplegable o <Ninguno> si el portlet Información no va a mostrar esta entidad.

Propiedades de gestión de contraseñas

Las *propiedades de gestión de contraseñas* son:

Nombre de propiedad	Definición
Atributo de la contraseña	Seleccione el atributo donde se almacenará la contraseña de esta entidad.
Contraseña obligatoria cuando se crea un atributo	**Seleccionado**: significa que es obligatorio introducir una contraseña cuando se crea esta entidad.

Uso de parámetros predefinidos

El editor del nivel de abstracción del directorio permite utilizar parámetros predefinidos para determinados valores. Los parámetros son:

Parámetro predefinido	Descripción
%driver-root%	Representa el DN del controlador de provisión. Este valor se especifica durante la configuración de la aplicación del usuario, en la instalación o en una configuración posterior. Se almacena en la configuración de dominio de la aplicación de usuario.
%user-root%	Representa el DN del contenedor de usuarios. Este valor se especifica durante la configuración de la aplicación del usuario, en la instalación o en una configuración posterior. Se almacena en la configuración de dominio de la aplicación de usuario.
%group-root%	Representa el DN del contenedor de grupos. Este valor se especifica durante la configuración de la aplicación del usuario, en la instalación o en una configuración posterior. Se almacena en la configuración de dominio de la aplicación de usuario.

Referencia de la propiedad de un atributo

Puede definir los tipos de propiedades siguientes en los atributos:

- “Propiedades de acceso de los atributos” en la página 97
- “Propiedades obligatorias del atributo” en la página 98
- “Propiedades de formato y de filtro del atributo” en la página 99
- “Propiedades de control de la IU del atributo” en la página 99

Propiedades de acceso de los atributos

Las *propiedades de acceso de los atributos* son:

Nombre	Descripción
Editar	**Seleccionado**: la aplicación de usuario puede editar o modificar este atributo. Incluso si está seleccionado (true), es posible que el atributo siga sin poderse editar si los derechos efectivos de las ACL del repositorio seguro de identidades subyacente lo evitan.
Habilitar	**Deseleccionado**: la aplicación de usuario no puede utilizar este atributo. Equivale a eliminar la entrada del archivo.

Nombre	Descripción
Ocultar	Controla si la casilla de verificación Ocultar de la aplicación de usuario está habilitada o inhabilitada. Dicha casilla permite que los usuarios controlen si la aplicación mostrará un atributo (como su fotografía). **Deseleccionado**: la casilla de verificación Ocultar está inhabilitada para este atributo, por lo que el usuario no podrá seleccionar si lo ocultará. **Seleccionado**: la casilla de verificación Ocultar puede habilitarse en la aplicación de usuario. No obstante, los usuarios que hayan entrado deberán cumplir también los puntos siguientes. Deberán: ◆ Ser propietarios del atributo o bien un administrador de la aplicación de usuario. ◆ Tener derechos de Trustee para actualizar el atributo srvprvHideAttributes en el repositorio seguro de identidades. Si no se cumplen dichos requisitos, la casilla de verificación Ocultar se inhabilitará en la interfaz de usuario, incluso aunque este valor esté seleccionado (true). **Sugerencia:** Cuando un usuario oculta un atributo que contiene una imagen, los usuarios que han visto la imagen podrán seguir viéndola hasta que el caché del navegador se actualice.
Multivalor	Especifica si este atributo puede tener varios valores como, por ejemplo, un número de teléfono. **Seleccionado**: el atributo puede tener varios valores.
Lectura	**Seleccionado**: la aplicación de usuario puede consultar este atributo. La mayoría de los atributos deberían tenerlo seleccionado (true), pero en el caso de algunos atributos como, la contraseña, debería estar deseleccionado.
Requerir	**Seleccionado**: el atributo debe suministrarse.
Buscar	**Seleccionado**: la aplicación de usuario puede buscar en este atributo. Los atributos que se utilizarán en las consultas de los portlets de identidad (como la lista de búsqueda de entidades o el organigrama corporativo de la entidad) deben estar seleccionados. **Sugerencia:** Si un atributo que se utiliza en una búsqueda también está indexado en eDirectory, la búsqueda será más rápida.
Ver	**Seleccionado**: la aplicación de usuario puede mostrar este atributo. En la mayoría de casos debería ser cierto, pero en el caso de algunos atributos como la contraseña, probablemente estará deseleccionado.

Propiedades obligatorias del atributo

Nombre	Descripción
Clave	Identificador exclusivo del atributo.
Etiqueta de visualización	Etiqueta que se visualiza en la aplicación de usuario.
Nombre de atributo	El nombre NDS de este atributo.

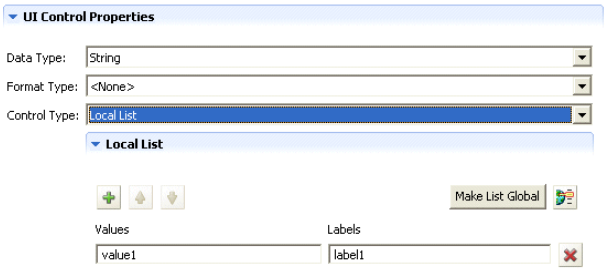
Nombre	Descripción
Nombre LDAP	El nombre LDAP de este atributo.

Propiedades de formato y de filtro del atributo

Nombre	Descripción
Filtro: Atributo WHERE	Permite especificar un filtro LDAP en la búsqueda del repositorio seguro de identidades para este atributo.
Habilitar	**Seleccionado**: habilita el filtro.

Propiedades de control de la IU del atributo

Nombre	Descripción
Tipo de datos	Seleccione un tipo de datos en la lista siguiente: ◆ Binario ◆ Booleano ◆ DN ◆ Número entero ◆ Cadena localizada ◆ Cadena ◆ Hora
Tipo de formato	Utilizado por la aplicación de usuario para dar formato a los datos Los tipos de formato son: ◆ Ninguno ◆ IM de AOL ◆ Correo electrónico ◆ IM de Groupwise ◆ Imagen ◆ Teléfono ◆ IM de Yahoo ◆ URL de imagen ◆ Fecha ◆ DateTime Los tipos de formato dependen de los tipos de datos. Por ejemplo, un tipo de datos de hora sólo se puede asociar a los formato de fecha y de fecha y hora.

Nombre	Descripción
Tipo de control	Los tipos son: **DNLookup**: define que este atributo contiene una referencia de DN. Debe utilizarlo cuando desee: ◆ Cumplimentar una lista con los resultados de una búsqueda de nombre completo entre las entidades relacionadas ◆ Mantener una integridad de referencia en los atributos de referencia de DN durante las actualizaciones y supresiones La aplicación de usuario utiliza esta información para generar elementos especiales de la interfaz de usuario y para realizar búsquedas optimizadas basadas en la definición de DNLookup. Si desea obtener más información, consulte “Utilización de los tipos de control de DNLookup” en la página 100 **Lista global**: muestra este atributo como una lista desplegable cuyo contenido está definido en un archivo que no entra dentro de la definición del atributo. Si desea obtener más información, consulte Sección 4.4, “Funcionamiento con listas”, en la página 104. **Lista local**: muestra este atributo como una lista desplegable cuyo contenido está definido con este atributo. Para definir una lista local: 1. Con el atributo seleccionado, defina el tipo de control como Lista local.  2. Haga clic en el botón Añadir para añadir más valores. Utilice los botones de flecha hacia arriba y hacia abajo para cambiar la posición del elemento dentro de la lista. En la columna Valor, escriba el valor que se escribirá en el repositorio seguro de identidades. Sólo puede incluir minúsculas, números y caracteres de subrayado (_). 3. En la columna Etiquetas, escriba el texto que desee que aparezca en la interfaz de usuario. **Rango**: use el tipo de control Rango con los tipos de datos Número entero para restringir las entradas de usuario en un rango de valores secuencial. Suministrará los valores de principio y fin del rango.

Utilización de los tipos de control de DNLookup

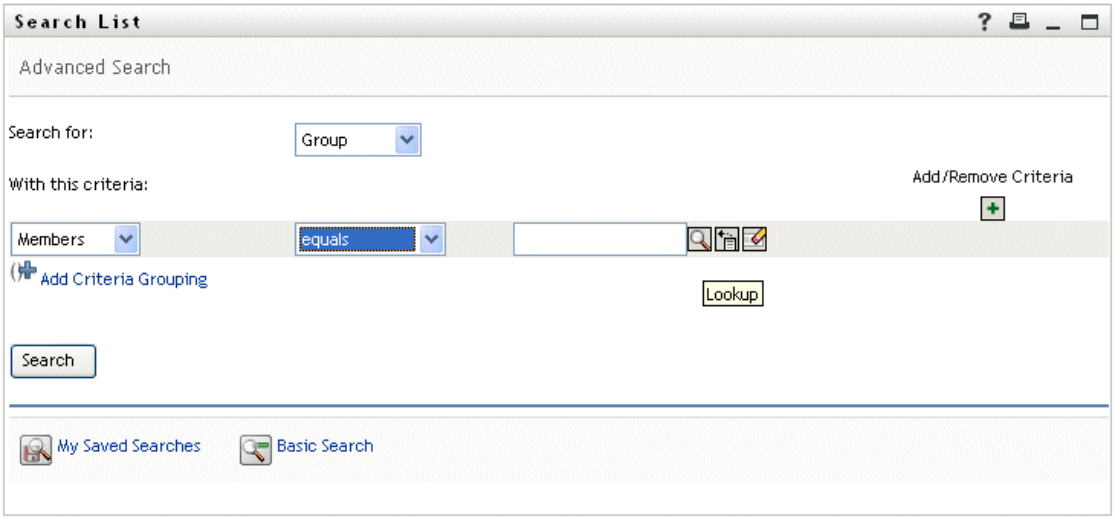
Cuando un tipo de control se define como DNLookup, significa que:

◆ Cuando los usuarios busquen en este atributo, pueden elegir entre una lista de posibles valores.

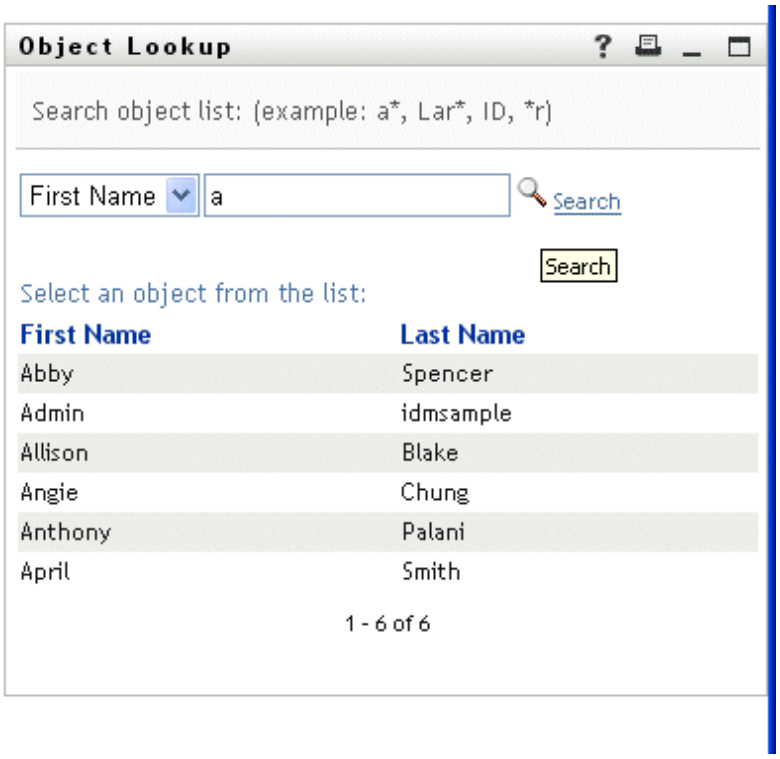
- Cuando este atributo se crea, cumplimenta o suprime, un atributo de una entidad relacionada se actualizará correctamente en función de la acción del usuario (crear, suprimir, actualizar) a fin de mantener la integridad de referencia.

DNLookup para listas de selección

La aplicación de usuario instalada contiene definiciones de entidades para usuarios y grupos. La definición de entidad de usuarios contiene un atributo llamado Grupo que está definido como tipo de control de DNLookup. Esto permite que cualquier portlet de identidad pueda proporcionar una lista de grupos de selección para un usuario determinado. Por ejemplo, supongamos que un usuario decide efectuar una búsqueda en un directorio. Desea encontrar un usuario de un grupo, pero no sabe el nombre de dicho grupo. Tiene la posibilidad de seleccionar Usuario como el objeto que desea buscar e incluir Grupo como criterio de búsqueda, tal como se muestra a continuación:



Dado que Grupo está definido como tipo de control de búsqueda de DN para la entidad Usuario, se mostrará el icono de búsqueda. Si el usuario lo selecciona, aparecerá una lista de posibles grupos:



El usuario puede seleccionar un grupo en la lista.

DNLookup para integridad referencial

Los DNLookup por cuestiones de actualización o de sincronización son importantes, ya que LDAP permite que las relaciones de grupo se asignen en ambas direcciones. Por ejemplo, los datos pueden estar configurados para que:

- El objeto de usuario contiene un atributo de grupo. El atributo de grupo:
- Tiene varios valores
- Muestra una lista de todos los grupos a los que pertenece el usuario
- El objeto Grupo contiene un atributo de usuario. El atributo de usuario:
- Es multivalente
- Muestra una lista de todos los usuarios que pertenecen al grupo

Esto significa que puede tener un atributo en el objeto usuario que muestre todos los grupos a los que pertenece el usuario y en el objeto Grupo tener un atributo DN que incluya todos los miembros de dicho grupo.

Cuando el usuario solicita una actualización, la aplicación de usuario tiene que cumplir la relación y asegurarse de que los atributos de origen y de destino estén sincronizados. En DNLookup, especifique los dos atributos que tienen que estar sincronizados. Puede utilizar esta técnica para proporcionar sincronización entre cualquier objeto que esté relacionado y no sólo los objetos estructurales de grupo. Este tipo de control de DNLookup se crea especificando las propiedades de

DNLookup avanzadas descritas en la referencia *Propiedades de la integridad relacional de DNLookup*.

Referencia de las propiedades de DNLookup

Las propiedades de visualización de DNLookup son:

Campo	Definición
Entidad de búsqueda	Nombre de la entidad donde se efectuará la búsqueda; por ejemplo, la entidad Grupo de tareas contiene un atributo para el Supervisor de tareas. Para cumplimentar este campo, tendrá que saber qué usuarios son Supervisores de tareas.
Entidad de información	Clave de la entidad cuya información desea mostrar si el usuario solicita más información, haciendo clic en un enlace de hipertexto de la aplicación de usuario. Cuando se define un DNLookup, los portlets de identidad pueden proporcionar un enlace de hipertexto que permite que los usuarios muestren la información del objeto enlazado.
Atributos que se visualizarán	Elija uno o varios atributos que se visualizarán cuando la búsqueda haya finalizado.
Realizar una consulta automática	Define cómo se visualizarán los **Atributos que se visualizarán** (arriba). ◆ **Seleccionado**: realiza una consulta automática de la entidad y presenta los resultados en una lista seleccionable. Es posible que esta opción no sea la más adecuada si la cantidad de datos devuelta es grande, ya que esto obligaría al usuario a desplazarse por un conjunto de resultados enorme. ◆ **Deseleccionado**: permite que el usuario especifique los criterios de búsqueda de la consulta de la entidad y que presente los resultados en una lista seleccionable.

Propiedades de la integridad relacional de DNLookup: estas propiedades se utilizan para sincronizar los datos entre dos objetos como grupos y miembros del grupo.

Propiedad	Definición
Atributos de origen que se actualizarán	Nombre del atributo que se actualizará. El atributo debe contener una referencia DN a los **Atributos de destino que se actualizarán**. Obligatorio para sincronizar los atributos en dos objetos diferentes.
Atributos de destino que se actualizarán	Nombre del atributo que debe actualizarse junto con los **Atributos de origen que se actualizarán**. Nombre de atributo LDAP. Obligatorio para sincronizar los atributos en dos objetos diferentes. El atributo debe contener una referencia de DN.
Clases auxiliares de destino, si las hay	Nombre de la clase auxiliar que contiene **los atributos de destino que se actualizarán**.

4.4 Funcionamiento con listas

El nodo de listas permite definir el contenido de las listas globales. La aplicación de usuario del Gestor de identidades utiliza las listas globales para:

- Proporcionar una lista de valores de un atributo. Cuando el atributo se muestra para editarlo en la interfaz de usuario, los posibles valores se muestran como lista desplegable.
- Se utiliza para definir las categorías disponibles en el módulo auxiliar de configuración de peticiones de provisión en iManager. Se trata de una lista especial. Para obtener información detallada, consulte Sección 4.4.2, “Acerca de la lista Categoría de provisión”, en la página 106.

Para crear una lista global nueva:

1 Lance el asistente para listas nuevas según uno de los métodos siguientes:

Desde la *Vista de provisión*:

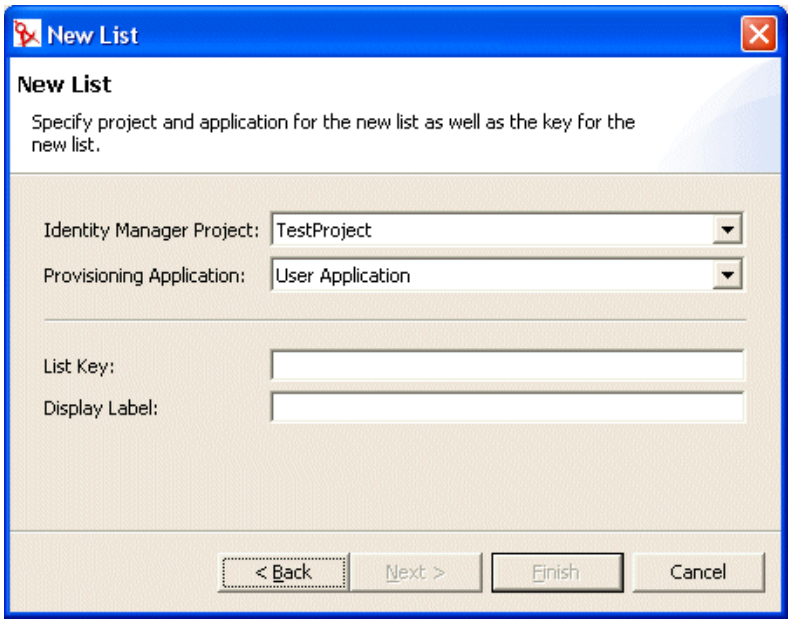
- Seleccione *Archivo>Nuevo>Provisión*. Seleccione *Lista del nivel de abstracción del directorio*. Haga clic en *Siguiente*.
- Seleccione el nodo *Listas*, haga clic con el botón derecho del ratón y seleccione *Nuevo*.

En el *editor del nivel de abstracción del directorio*:

- Haga clic en el botón *Lista nueva*.
- Seleccione el nodo Listas, haga clic con el botón derecho del ratón y seleccione *Añadir lista*.

Se mostrará el diálogo Lista nueva.

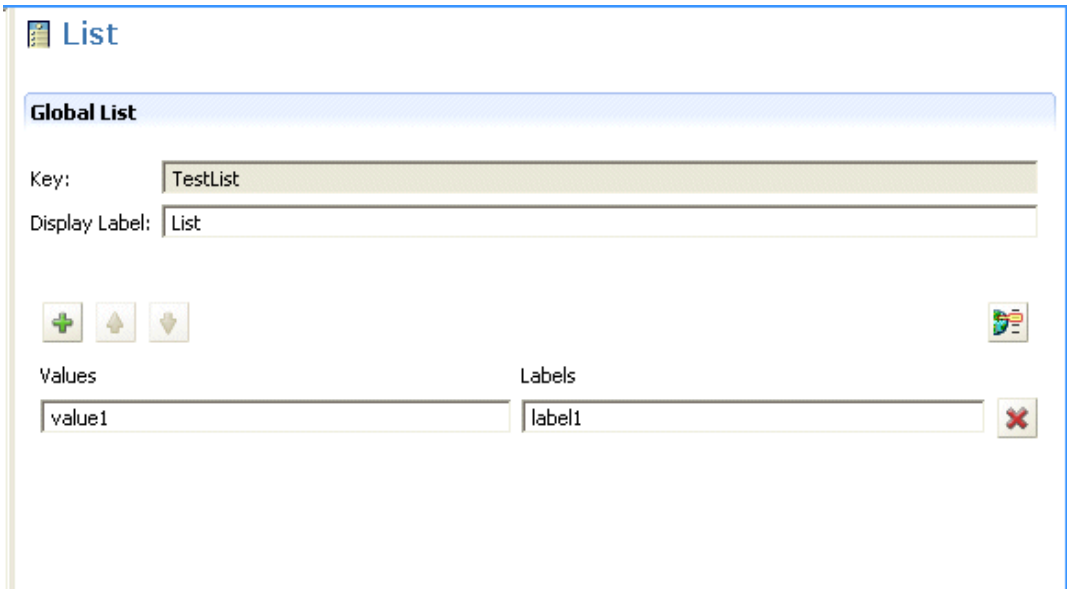
Nota: Si se inicia desde el menú Archivo, el diálogo contendrá campos que no aparecen cuando se lanza siguiendo alguno de los otros métodos.



2 Complete el panel como se muestra a continuación:

Campo	Descripción
Aplicación de provisión y proyecto del Gestor de identidades	Seleccione la aplicación de provisión y el proyecto del Gestor de identidades en que desea añadir la entidad y los atributos. **Nota:** Estos campos se visualizan cuando se lanza el asistente desde el menú Archivo.
Clave de la lista	Identificador exclusivo de la lista.
Etiqueta de visualización	La cadena utilizada siempre que se hace referencia a la lista en la interfaz de usuario.

3 Haga clic en *Finalizar*. Se mostrará la hoja de propiedades Listas globales.



4 Complete estos campos:

Campo	Descripción
Etiqueta de visualización	Nombre de la lista tal como aparece en el diseñador.
Etiquetas	Texto del elemento de la lista que desea que aparezca en la interfaz de usuario.
Valores	Valor del elemento de la lista que desea que se almacene en el repositorio seguro de identidades. Sólo puede incluir minúsculas, números y caracteres de subrayado (_).

Ahora la lista está disponible en el entorno de diseño.

5 Guardar el proyecto.

Nota: Para que la lista esté disponible en el entorno de tiempo de ejecución, debe implantarla.

4.4.1 Acerca de la lista Configuración regional preferida

La lista Configuración regional preferida representa el idioma que se utilizará por defecto en caso de que el idioma del navegador no sea uno de los idiomas admitidos. El contenido de esta lista se muestra en la configuración por defecto de la acción Editar usuario de la aplicación de usuario.

4.4.2 Acerca de la lista Categoría de provisión

La lista Categoría de provisión define el conjunto de categorías que ayudan a organizar los recursos provisionados (derechos) y las peticiones de provisión. Las categorías de esta lista se muestran en:

- *iManager*: módulo auxiliar de configuración de peticiones de provisión
- *aplicación de usuario*: ficha Peticiones y aprobaciones

No se puede cambiar la clave de la lista Petición de provisión, pero se pueden añadir más elementos a la lista o cambiar los valores y etiquetas de categoría existentes.

Para modificar el contenido de la lista Categoría de provisión:

1. Asegúrese de que el proyecto correcto esté abierto en el editor.
2. Haga clic en el nodo Listas.
3. Seleccione *Categoría de provisión*.
4. Utilice el panel de propiedades de la lista global para introducir las modificaciones.

   Nota: El campo Valores se utilizará para cumplimentar la clave de categoría. El campo Valores está restringido al uso de minúsculas, números y caracteres de subrayado (_), ya que estos son los únicos caracteres válidos de la clave de categoría. La clave de categoría se utiliza internamente como identificador de la categoría.

5. Guarde e implante los cambios. No se olvide de actualizar el caché del servidor de la aplicación.

   Una vez los cambios estén implantados, se reflejarán en la aplicación de usuario y en el módulo auxiliar iManager.

4.5 Funcionamiento con relaciones de los organigramas corporativos

El nodo de relaciones del organigrama corporativo permite definir relaciones jerárquicas entre entidades definidas en el nivel de abstracción del directorio. La relación puede existir entre entidades similares (por ejemplo, entre usuario y usuario) o entre entidades diferentes (por ejemplo, entre usuario y dispositivo).

La aplicación de usuario define las siguientes relaciones:

- Relaciones de grupo
- Supervisor-Empleado
- Grupos de usuarios

Para implantar correctamente una relación, todos los componentes (entidades y atributos) de la relación deben estar ya implantados.

Para crear una relación nueva:

1 Una relación nueva se puede crear según cualquiera de los métodos siguientes:

Desde la *Vista de provisión*:

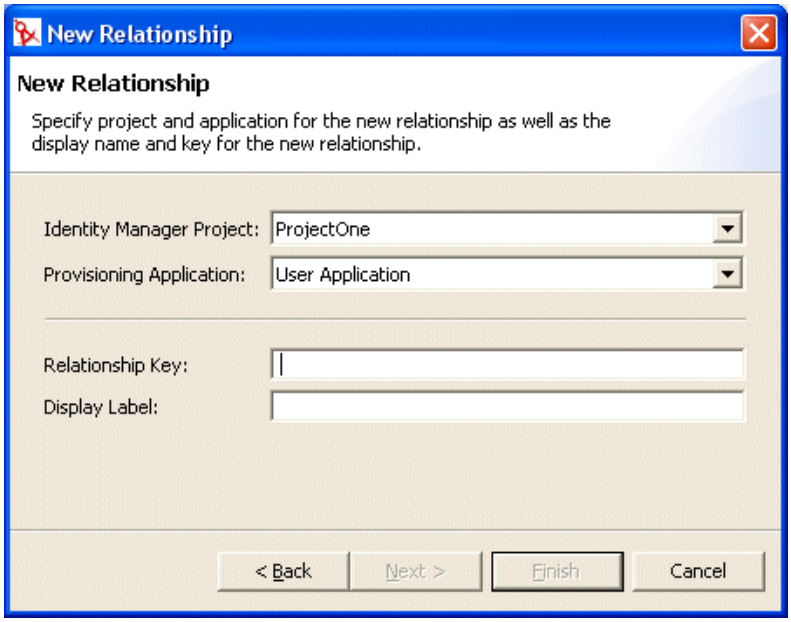
- Seleccione *Archivo>Nuevo>Provisión*. Seleccione *Relación del nivel de abstracción del directorio* y haga clic en *Siguiente*.
- Seleccione el nodo *Relaciones del organigrama corporativo* y haga clic con el botón derecho del ratón y seleccione *Añadir*.

En el *editor del nivel de abstracción del directorio*:

- Haga clic en el botón *Añadir relación*.
- Seleccione el nodo *Relaciones del organigrama corporativo* y haga clic con el botón derecho del ratón y seleccione *Añadir relación*.

Se mostrará el diálogo Relación nueva.

Nota: Si se inicia desde el menú Archivo, el diálogo contendrá campos que no aparecen cuando se lanza siguiendo alguno de los otros métodos.

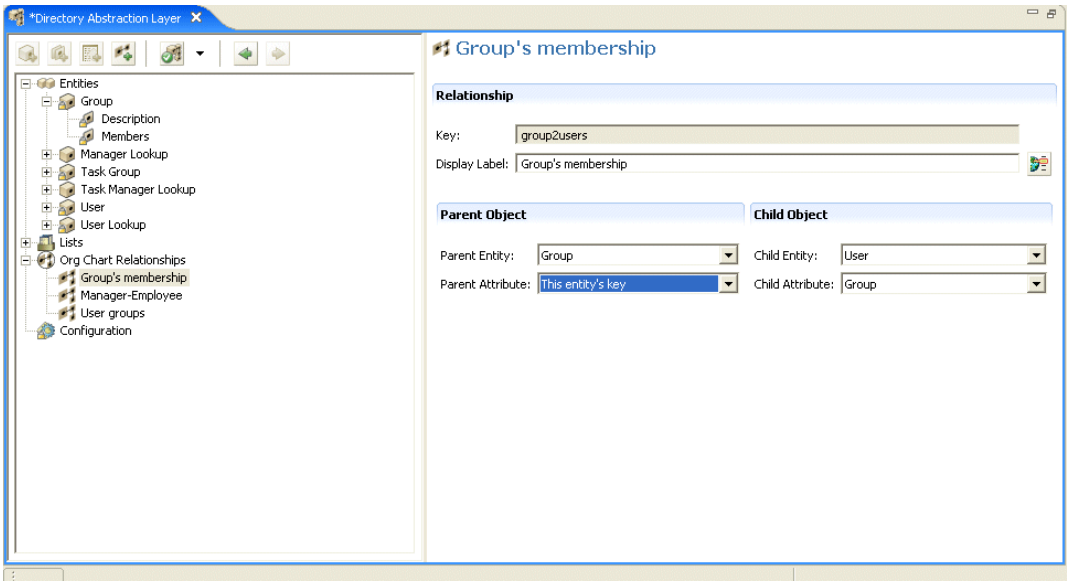


2 Complete el panel como se muestra a continuación:

Campo	Operaciones que puede realizar
Aplicación de provisión y proyecto del Gestor de identidades	Asegúrese de que estén seleccionados el proyecto del Gestor de identidades y las aplicaciones de provisión correctos. **Nota:** Este campo se visualiza cuando se crean relaciones desde el menú Archivo.
Clave de relación	Escriba un valor único para la clave de relación.
Etiqueta de visualización	Escriba la cadena que desea que se visualice siempre que se muestre la relación en la interfaz de usuario del Gestor de identidades.

3 Haga clic en *Finalizar*.

Se creará la relación y la hoja de propiedades se abrirá para editarla.



4.5.1 Referencia de las propiedades de relación

Campo	Descripción
Clave	Identificador único de sólo lectura de la relación. **Sugerencia:** Este valor se especifica en la hoja de preferencias del portlet del organigrama corporativo.

Campo	Descripción
Etiqueta de visualización	Especifique un nombre para visualizarlo cuando otros portlets de identidad le hagan referencia. Por ejemplo, este valor se visualiza cuando los usuarios hacen clic en el icono de selección del organigrama corporativo del portlet de información. Haga clic en **Localizar** para proporcionar la traducción del texto de la etiqueta de visualización.
Entidad Padre	Seleccione una entidad en la lista desplegable. La entidad que seleccione se convertirá en el objeto padre de la jerarquía del organigrama corporativo. Por ejemplo, en una relación de Supervisor-Empleado, la Entidad padre será Usuario. En una relación de Grupo-Miembro, la Entidad padre será Grupo. **Requisitos del nivel de abstracción del directorio**: las entidades de esta lista son un subconjunto de entidades definido en el nivel de abstracción del directorio. Las entidades padre deben tener seleccionada la propiedad de acceso a la vista (true)
Atributo padre	Seleccione un atributo en la lista desplegable. Este atributo se utiliza para encontrar entidades hijo coincidentes. Cuando el valor de este atributo coincide con el valor correspondiente de un atributo de la entidad hijo (véase Atributo hijo más abajo), se puede establecer una relación. **Requisitos del nivel de abstracción del directorio**: esta lista de atributos se rellena utilizando los atributos de entidad padre seleccionados. Sólo incluye los atributos definidos como tipo de control DNLookup
Entidad hijo	Seleccione la entidad que será el objeto hijo de la jerarquía. Por ejemplo, en una relación de Supervisor-Empleado, sería usuario. Por ejemplo, en una relación de Empleado-Recursos, sería Dispositivos. Esta entidad debe contener el atributo relacionado con el atributo padre.
Atributo hijo	Seleccione el atributo correspondiente al atributo padre. Permite especificar el atributo de la entidad hijo que se utilizará para encontrar las entidades padres correspondientes. Cuando el valor de este atributo coincide con el valor correspondiente de un atributo de la entidad padre (véase Atributo padre más arriba), se puede establecer una relación.

Nota: Los grupos dinámicos no son totalmente compatibles con el portlet del organigrama corporativo. Un grupo dinámico no se puede definir como entidad padre de una relación, aunque un grupo dinámico se puede definir como entidad hijo de una relación.

Para suprimir una relación:

1. Seleccione la relación que desee suprimir.
2. Haga clic con el botón derecho del ratón y seleccione *Suprimir*.

4.6 Trabajo con los ajustes de configuración

El nodo Configuración permite definir las propiedades de configuración general de la aplicación de usuario. Incluyen:

Propiedad	Descripción
Por defecto‘Mi perfil’ Entidad	Define la entidad que se visualizará cuando el usuario hace clic en **Mi perfil** en la interfaz de usuario. Este campo sólo puede mostrar entidades cuya clase de objeto sea usuario (o LDAP inetOrgPerson).
Configuración regional por defecto	Define el idioma por defecto que se utilizará para las etiquetas de visualización de la aplicación de usuario. Si el navegador está definido con un idioma incompatible, en su lugar se utilizará esta configuración regional. **Nota:** La configuración regional del navegador anulará la configuración regional por defecto de los idiomas admitidos.
Clases de contenedor	Proporciona a la acción Crear usuario o Grupo el contenido de una lista de selección de clases de contenedor. El usuario selecciona un contenedor en la lista de selección como lugar en el que residirá el objeto que acaba de crear.

4.7 Localización del texto de visualización

El editor del nivel de abstracción del directorio proporciona una forma sencilla de localizar el texto de visualización:

- Etiquetas de visualización de entidades y atributos
- Nombres de las relaciones de los organigramas corporativos
- Elementos de las listas local y global

4.7.1 Idiomas admitidos

El texto de visualización se puede localizar en uno o varios de los idiomas siguientes:

- Inglés
- Francés
- Alemán
- Italiano
- Japonés
- Coreano
- Portugués
- Ruso
- Chino simplificado
- Español

- Chino tradicional

4.7.2 Localización de texto

El editor del nivel de abstracción del directorio proporciona diferentes formas de localizar las definiciones del nivel de abstracción. Puede acceder a los diálogos de localización de las formas siguientes:

Para definir el texto de localización de una	Acción
Todos los elementos localizables del nivel de abstracción del directorio	◆ Haga clic en **Definir la globalización local (**en la barra de herramientas del editor del nivel de abstracción del directorio). Asegúrese de seleccionar el idioma de destino antes de introducir el texto localizado en el campo de destino.
Una entidad, relación o lista específica	◆ En la vista del árbol del editor del nivel de abstracción del directorio, seleccione el objeto que desee localizar. ◆ Haga clic con el botón derecho del ratón y seleccione **Localizar**. Asegúrese de seleccionar el idioma de destino antes de introducir el texto localizado en el campo de destino.
Una etiqueta de visualización única	◆ Seleccione una entidad o atributo específico. ◆ Haga clic en **Localizar la etiqueta de visualización** (al lado del campo Etiqueta de visualización del panel de propiedades).

Los diálogos pueden tener un aspecto diferente, aunque todos contendrán los campos siguientes:

- *Origen*: por lo general, el tipo de objeto (como entidad, lista o relación) y la clave
- *Origen*: texto que se desea traducir (etiqueta de visualización)
- *Idioma de destino*: uno de los idiomas admitidos
- *Texto*: el texto de la traducción

4.8 Importación, validación e implantación de las definiciones del nivel de abstracción del directorio

Importar, validar e implantar las definiciones del nivel de abstracción del directorio son acciones que ejecuta la vista de provisión del diseñador.

- Sección 4.8.1, “Acerca de la importación”, en la página 112
- Sección 4.8.2, “Acerca de la validación”, en la página 114
- Sección 4.8.3, “Acerca de la implantación”, en la página 114

4.8.1 Acerca de la importación

La función de importación permite importar un conjunto de definiciones existentes. La importación es útil cuando:

- Se desea empezar un proyecto nuevo basado en un proyecto implantado.
- Se desea compartir definiciones con otros desarrolladores que trabajen en el mismo proyecto. Por ejemplo, supongamos que otro desarrollador añade un atributo a la entidad de usuario o bien una lista global nueva. Si el desarrollador implanta la nueva definición en el repositorio seguro de identidades, podrá importarlo y asegurarse de que está trabajando en definiciones idénticas.

Para importar definiciones existentes:

1. Abra la *Vista de provisión*.
2. Determine si desea importar:
   - Un conjunto completo de definiciones
   - Un conjunto de un tipo de definición como todas las entidades o todas las relaciones.
   - Un objeto específico (como la entidad de usuario)
3. Para importar:
   - Un objeto específico, selecciónelo en la lista, haga clic con el botón derecho del ratón y seleccione *Importar objeto*.
   - Un conjunto completo de definiciones, seleccione el nodo del nivel de abstracción del directorio y seleccione *Importar todo* o *Importar objeto*.
4. Haga clic en el icono de navegación de eDirectory y desplácese al nodo DirectoryModel, seleccione los objetos que desee importar y haga clic en *Aceptar*.
   - Si los objetos coinciden, se le notificará que no hay diferencia y que no se puede importar.
   - Si los objetos no coinciden, podrá confirmar los objetos que desea importar. Revise los elementos seleccionados para importarlos, introduzca los cambios necesarios y haga clic en *Aceptar*.

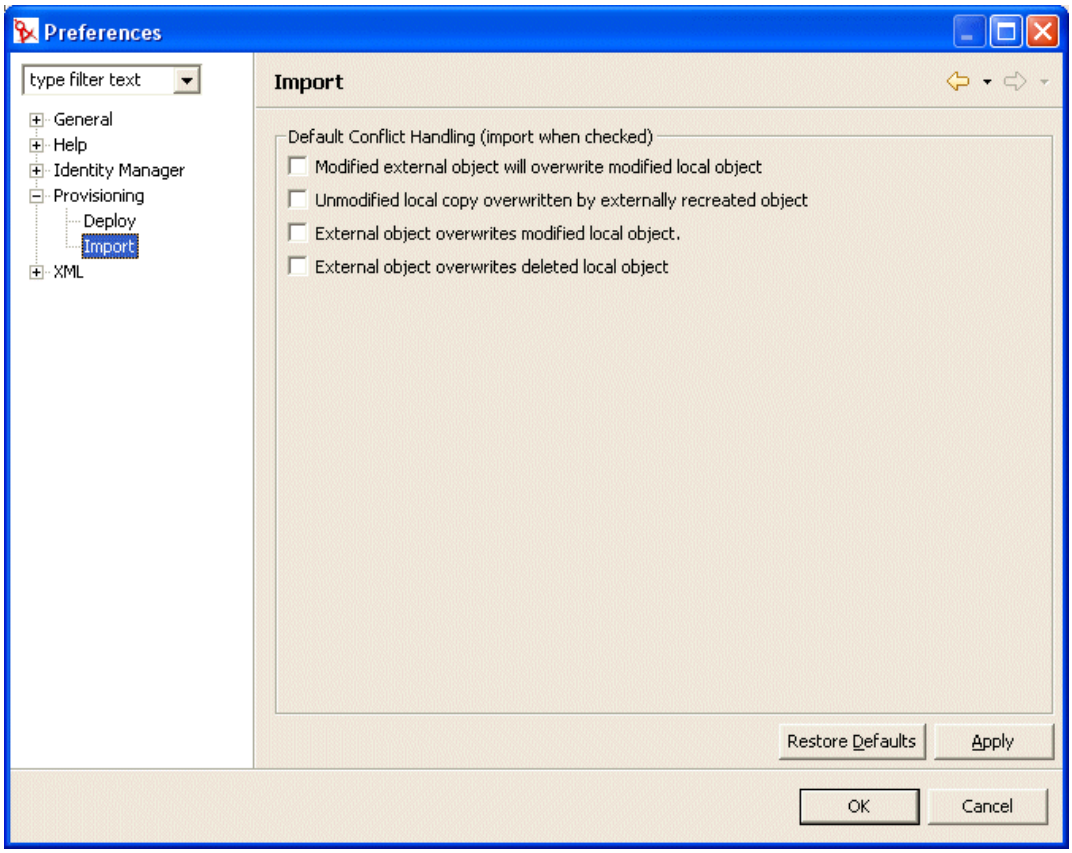
Definición de las preferencias de importación

Las preferencias de importación permiten especificar cómo desea que el diseñador resuelva los conflictos entre los datos del repositorio seguro de identidades y los archivos del nivel de abstracción del directorio local. Estos conflictos pueden surgir debido a que diferentes usuarios y herramientas pueden tener acceso a las definiciones del nivel de abstracción del directorio del repositorio seguro de identidades. Otros administradores o desarrolladores que utilicen herramientas de iManager o su propio proyecto basado en el diseñador local pueden cambiar las definiciones. Cuando surgen conflictos entre las definiciones del sistema de archivos local y el repositorio seguro de identidades, estas preferencias permiten especificar cómo gestionar los conflictos.

Para definir preferencias de importación:

1. Seleccione *Ventana>Preferencias*.

2 Abra el nodo Provisión del árbol y haga clic en *Importar*.



3 Seleccione las preferencias:

Preferencia	Descripción
El objeto externo modificado sobrescribirá el objeto local modificado	Tanto el archivo local como las definiciones del repositorio seguro de identidades contienen cambios. Los cambios locales todavía no se han implantado. Seleccione esta opción si desea identificar el objeto del repositorio seguro de identidades para sobrescribir los cambios efectuados en el archivo local.
Copia local no modificada sobrescrita por un objeto vuelto a crear externamente	El objeto del repositorio seguro de identidades había sido suprimido y se ha vuelto a crear. El conjunto de archivos locales incluye la definición original sin cambios. Seleccione esta opción si desea que la importación sobrescriba la copia local.
El objeto externo sobrescribe el objeto local modificado	El archivo local contiene cambios que no se han implantado en el repositorio seguro de identidades. Seleccione esta opción si desea que los archivos locales se sobrescriban al importar.

Preferencia	Descripción
El objeto externo sobrescribe el objeto local suprimido	Ha definido localmente una definición, pero no ha implantado los cambios. Esto significa que el objeto sigue existiendo en el repositorio seguro de identidades. Seleccione esta opción si desea identificar los objetos del repositorio seguro de identidades que se copiarán en el sistema de archivos local. Si selecciona esta opción, perderá los cambios que no haya implantado.

4.8.2 Acerca de la validación

Las definiciones de datos del nivel de abstracción del directorio se pueden validar en los sistemas de archivos locales antes de intentar implantarlas. La validación:

- Verifica que el XML esté bien formado y cumpla el esquema que define los elementos necesarios para entidades, atributos, listas, relaciones, etc.
- Comprueba todas las entidades para asegurarse de que las referencias a otras entidades y a listas globales sean válidas.

Por ejemplo, cuando valida una entidad y sus atributos, el validador comprueba que todas las referencias a otras entidades efectuadas mediante los campos *Editar entidad*, *DNLookup* y *Entidad de información* hagan referencia a entidades que existan realmente.

- Permite asegurarse de que todas las entidades tengan, como mínimo, un atributo definido.
- Permite asegurarse de que todas las listas locales y globales contengan, como mínimo, un elemento.

Las definiciones se pueden validar selectivamente desde la *Vista de provisión*. Para validar:

- Todos los elementos de un nodo, seleccione el nodo, haga clic con el botón derecho del ratón y seleccione *Validar*.
- Un único objeto de un nodo, seleccione el objeto, haga clic con el botón derecho del ratón y seleccione *Validar*.

Se pueden validar todas las definiciones, haciendo clic con el botón derecho en el botón *Validar nivel de abstracción* de la barra de herramientas del nivel de abstracción del directorio.

Nota: La validación no comprueba en el repositorio seguro de identidades la existencia de objetos.

4.8.3 Acerca de la implantación

Debe implantar las definiciones en un repositorio seguro de identidades, antes de ver los cambios obtenidos en la aplicación de usuario del Gestor de identidades.

Para implantar un conjunto de definiciones en un repositorio seguro de identidades:

1. Guarde todos los cambios que haya efectuado mediante el editor del nivel de abstracción del directorio.

Si no guarda los cambios antes de intentar la implantación, el editor abrirá un diálogo que muestra las definiciones que no se han guardado y le solicitará que guarde los cambios más recientes. Si no los guarda, el objeto seguirá implantado en el servidor, pero no incluirá los cambios que no se hayan guardado. Si elige no guardar los cambios, no significa que la implantación se cancele.

2 Abra la *Vista de provisión*.

3 Decida si desea implantar todos los objetos definidos mediante el editor del nivel de abstracción o un subconjunto.

- Para implantarlos todos:

  Seleccione el nodo raíz, pulse el botón derecho del ratón y seleccione *Implantar todo*.

- Para implantar una entidad, relación, lista o valor de configuración específico:

  Selecciónelo, pulse el botón derecho del ratón y seleccione *objeto*.

Es posible que el sistema le solicite las credenciales del repositorio seguro de identidades. El editor realizará una validación y mostrará los mensajes de validación en un diálogo. Responda a los mensajes de validación seleccionando/deseleccionando los elementos que implantará. Después de efectuar las selecciones de implantación y de enviarlas, se le notificará si la implantación ha sido correcta o no.

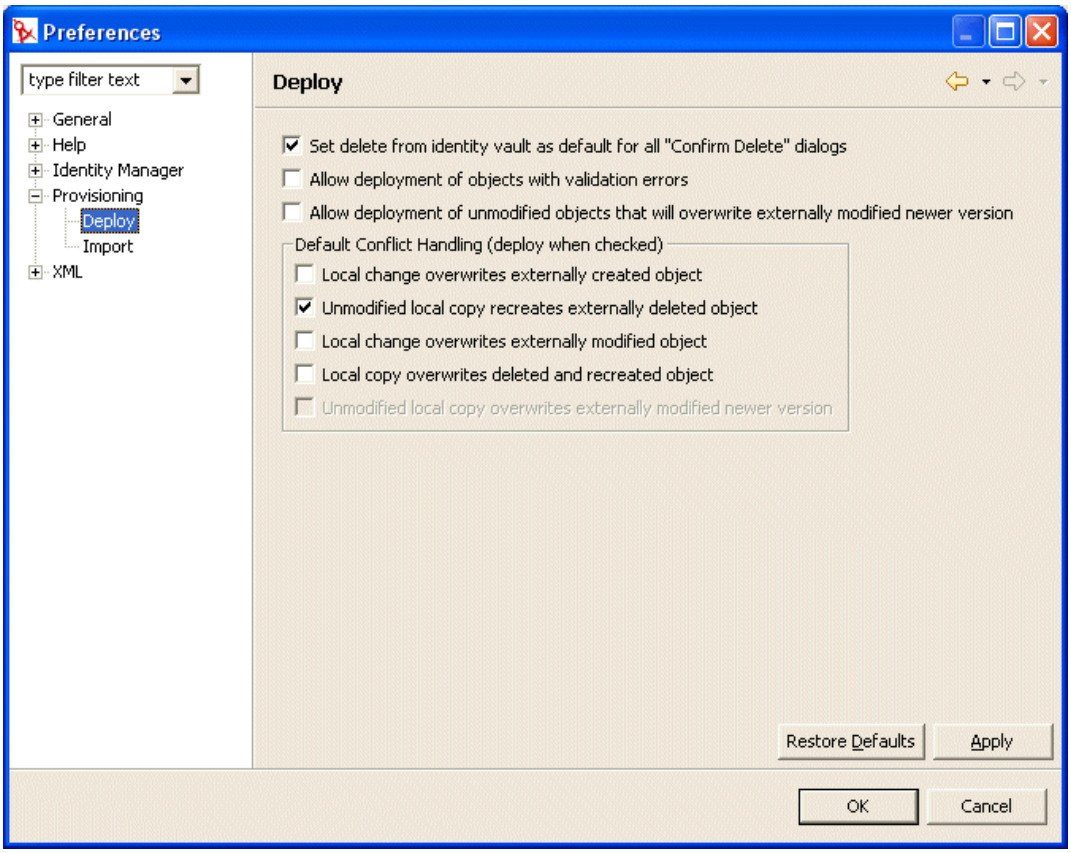
Configuración de las preferencias de implantación

Las preferencias de implantación permiten especificar cómo desea que el diseñador resuelva los conflictos entre los datos del repositorio seguro de identidades y los archivos del nivel de abstracción del directorio local. Pueden producirse conflictos debido a que otros usuarios han implantado cambios en el repositorio seguro de identidades que no se reflejan en las definiciones del sistema de archivos local. Para asegurarse de que los conflictos se gestionan tal como desea, puede definir las preferencias especificando la resolución del conflicto.

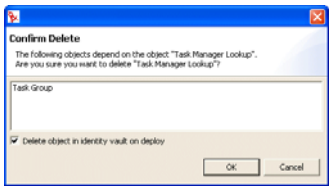
Para definir preferencias de implantación:

1 Seleccione *Ventana>Preferencias*.

2 Abra el nodo Provisión del árbol y haga clic en *Implantar*.



3 Especifique las preferencias de implantación generales:

Preferencia	Descripción
Defina la supresión del repositorio seguro de identidades como el valor por defecto para todos los diálogos de “Confirmar supresión”	Si intenta suprimir un objeto de la vista de provisión o del editor del nivel de abstracción del directorio, el sistema le solicitará que confirme la supresión con un diálogo como el siguiente:  Esta preferencia determina si la casilla de verificación del diálogo de confirmación etiquetada **Suprimir objeto del repositorio seguro de identidades al implantar** se selecciona por defecto. Seleccionar esta preferencia significa que el valor por defecto es suprimir siempre el objeto del repositorio seguro de identidades. El objeto local siempre se suprime.

Preferencia	Descripción
Permitir la implantación de objetos con errores de validación	**Selecciónela**: seleccione esta opción si desea implantar objetos que no han pasado la validación. En el momento de implantar, el diseñador valida las definiciones que se están implantando siguiendo las reglas de validación descritas en Sección 4.8, “Importación, validación e implantación de las definiciones del nivel de abstracción del directorio”, en la página 111. **Deselecciónela**: para evitar la implantación de definiciones que no han pasado la validación.
Permitir la implantación de objetos no modificados que sobrescribirán la versión más nueva modificada externamente	**Selecciónela**: si los archivos locales no se han cambiado, pero sí se han cambiado los objetos del repositorio seguro de identidades. ¿Desea que los archivos locales sobrescriban los archivos del repositorio seguro de identidades? En caso positivo, seleccione esta preferencia. **Deselecciónela**: si desea conservar las versiones más nuevas del repositorio seguro de identidades. Cuando esta opción está seleccionada, puede definir el comportamiento por defecto seleccionando también la preferencia de resolución de conflictos **Una copia local sin modificar sobrescribe la versión más nueva modificada externamente**.

4 Especificación de las preferencias de resolución de conflictos:

Preferencia	Descripción
El cambio local sobrescribe el objeto creado externamente	**Selecciónela**: si desea que el objeto que está implantando sobrescriba el objeto que se encuentra en el repositorio seguro de identidades. **Deselecciónela**: la implantación no se efectúa cuando se produce este conflicto.
La copia local no modificada vuelve a crear un objeto suprimido externamente	**Selecciónela**: si desea que el objeto local que está implantando cree un objeto que ya se había suprimido del repositorio seguro de identidades. **Deselecciónela**: la implantación no se efectúa cuando se produce este conflicto.
El cambio local sobrescribe un objeto modificado externamente	**Selecciónela**: si desea que la definición local esté siempre implantada, incluso si otro usuario ha cambiado el repositorio seguro de identidades. **Deselecciónela**: la implantación no se efectúa cuando se produce este conflicto.
La copia local sobrescribe el objeto suprimido y vuelto a crear	**Selecciónela**: si desea que el objeto local esté siempre implantado, incluso si el objeto repositorio seguro de identidades se ha suprimido o se ha suprimido y vuelto a crear. **Deselecciónela**: la implantación no se efectúa cuando se produce este conflicto.

Preferencia	Descripción
La copia local no modificada sobrescribe la versión más nueva modificada	Sólo se puede definir esta preferencia cuando la preferencia de implantación general **Permitir la implantación de objetos no modificados que sobrescribirán la versión más nueva modificada externamente** está seleccionada. **Selecciónelo**: si los archivos locales no se han cambiado, pero los objetos del repositorio seguro de identidades se han cambiado y el usuario **siempre** quiere que los archivos locales sobrescriban los archivos del repositorio seguro de identidades como comportamiento por defecto. **Deselecciónela**: si desea conservar las versiones más nuevas del repositorio seguro de identidades.

Configuración de las entradas

5

En este capítulo se describen los elementos siguientes:

5.1 Acerca del registro de eventos

La aplicación de usuario del Gestor de identidades implementa el registro mediante *log4j*, un paquete de registro de código abierto distribuido por The Apache Software Foundation. Por defecto, los mensajes de eventos se registran en la *consola del sistema* y en el archivo de registro del servidor de aplicación, en el nivel de registro INFO y superior. También puede configurar la aplicación de usuario para que entre en Novell Audit. Los eventos se registran en *todos* los registradores activados.

Importante: Si va a entrar en Novell Audit, se recomienda que revise la documentación de Novell Audit (http://www.novell.com/documentation/nsureaudit).

5.1.1 Acerca de los valores del nivel de registro

El registro en consola implica que las escrituras sean sincronizadas. Ello implica que el registro puede convertirse tanto en un problema de uso del procesador, como en una obstrucción de simultaneidad. El valor por defecto de la prioridad se puede cambiar a ERROR, modificando el valor en <*installdir*>/jboss/server/IDMProv/conf/log4j.xml. Localice el nodo raíz similar al siguiente:

```
<root> <appender-ref ref="CONSOLE"/> <appender-ref ref="FILE"/> </
root>
```

Cambie el valor de prioridad a:

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

Si asigna un valor a root, se asegurará de que cualquier agregador de registros que no tenga un nivel asignado explícitamente herede el nivel de root. Por defecto, el agregador de archivos no tiene asignado un nivel umbral, por lo que asume el de root. Todos los agregadores incluidos en root que tengan un umbral de nivel han de tener ERROR o WARN. Si el nivel de error definido es superior a WARM, tendrá una repercusión sobre el rendimiento.

5.2 Entrada en un servidor de Novell Audit

Para entrar en un servidor de Novell Audit, siga los pasos que indicamos a continuación:

Paso	Operaciones que puede realizar	Para más información
1	Añada el esquema de aplicación del Gestor de identidades al servidor de Novell Audit como aplicación de registro	Sección 5.2.1, “Adición del esquema de aplicación del Gestor de identidades al servidor de Novell Audit como aplicación de registro”, en la página 120
2	Configure el **agente de la plataforma** Novell Audit en el servidor de la aplicación	El agente de la plataforma se necesita en cualquier cliente que notifique eventos a Novell Audit y se configura mediante el archivo de **configuración logevent**. Dicho archivo proporciona información de configuración que el agente de la plataforma necesita para comunicarse con el servidor de Novell Audit. La ubicación por defecto de este archivo en el servidor de aplicación es: ◆ Linux—/etc/logevent.conf ◆ Windows—/<WindowsDir>/logevent.cfg (Normalmente c:\windows) Asegúrese de especificar la **dirección IP o nombre DNS del servidor Novell Audit** en el valor **LogHost**. Por ejemplo: `LogHost=xxx.xxx.xxx.xxx` Especifique cualquier otro valor que necesite para su entorno. **Importante:** Después de crear o modificar el archivo de configuración logevent, deberá reiniciar el servidor de aplicación JBoss, antes de que dichos cambios entren en vigor. Si desea obtener información acerca de la estructura del archivo de configuración logevent, consulte la sección que trata de la configuración de los agentes de plataforma (http://www.novell.com/documentation/nsureaudit) en el capítulo relativo al sistema de registro de Novell Audit Administration Guide (Novell Audit: Guía de administración).
3	Habilite el registro en Novell Audit	Sección 5.2.2, “Habilitación del registro de Audit”, en la página 121

5.2.1 Adición del esquema de aplicación del Gestor de identidades al servidor de Novell Audit como aplicación de registro

Para configurar Audit para que utilice la aplicación del Gestor de identidades como aplicación de registro, siga los pasos siguientes:

1 Localice el archivo siguiente:

DirXML.lsc

Plataforma	Ubicación
Linux	Postinstalación: /opt/novell/naudit/logschema/dirxml.lsc
Windows	En los medios de instalación: /nt/dirxml/nsure_audit/nauditextensions/lsc/dirxml.lsc

2 Utilice un navegador Web para acceder a *iManager* y entrar como *administrador*.

3 Vaya a *Funciones y tareas> Auditoría y registro* y seleccione *Opciones del servidor de registro*.

4 Desplácese hasta el *contenedor de servicios de registro* del árbol y seleccione el *servidor de registro seguro de auditoría*. A continuación, haga clic en *Aceptar*.

5 Vaya a la pestaña *Aplicaciones de registro*, seleccione el *Nombre de contenedor* adecuado y haga clic en el enlace *Nueva aplicación de registro*.

6 Cuando se abra el diálogo Nueva aplicación de registro, especifique lo siguiente:

Para este valor	Realice la operación siguiente
Nombre de la aplicación de registro	Escriba un nombre que tenga significado para su entorno
Importar archivo LSC	Utilice el botón **Examinar** para seleccionar el archivo **DirXML.lsc**

A continuación, haga clic en *Aceptar*. La pestaña Aplicaciones de registro mostrará el nombre de la aplicación añadida.

7 Haga clic en *Aceptar* para completar la configuración del servidor de Novell Audit.

8 Asegúrese de que el estado de la aplicación de registro esté en ACTIVO. (El círculo situado bajo el estado debe ser de color verde. Si está rojo, haga clic en él para ponerlo en ACTIVO).

9 *Reinicie* el servidor de Novell Audit para activar los valores de la nueva aplicación de registro.

5.2.2 Habilitación del registro de Audit

Para habilitar el registro de Novell Audit en la aplicación de usuario del Gestor de identidades

1 Entre en la aplicación de usuario como usuario Admin.

2 Seleccione la pestaña *Administración*.

3 Seleccione la pestaña *Registro*.

4. Active la casilla de verificación *También enviar los mensajes de registro a la auditoría* (cerca de la parte inferior de la pestaña).
5. Para que los cambios persistan en cualquier reinicio del servidor de aplicación posterior, asegúrese de que *Consolidar los cambios en el registro* esté seleccionado.

5.2.3 Eventos que se registran

La aplicación de usuario del Gestor de identidades registra un conjunto de eventos automáticamente a partir de las peticiones de flujo de trabajo, búsqueda, información y contraseña. Por defecto, la aplicación de usuario del Gestor de identidades registra automáticamente los eventos siguientes en todos los canales de registro activos:

ID del evento	Proceso	Evento	Gravedad
31400	Portlet de información	Delete_Entity	Info
31401		Update_Entity	Info
31410	Portlet de cambio de contraseña	Change_Password_Failure	Error
31411		Change_Password_Success	Info
31420	Portlet de contraseña olvidada	Forgot_Password_Change_Failure	Error
31421		Forgot_Password_Change_Success	Info
31430	Buscar portlet	Search_Request	Info
31431		Search_Saved	Info
31440	Crear portlet	Create_Entity	Info
31520	Flujo de trabajo	Workflow_Error	Error
31521		Workflow_Started	Info
31522		Workflow_Forwarded	Info
31523		Workflow_Reassigned	Info
31524		Workflow_Approved	Info
31525		Workflow_Refused	Info
31526		Workflow_Ended	Info
31527		Workflow_Claimed	Info
31528		Workflow_Unclaimed	Info
31529		Workflow_Denied	Info
3152A		Workflow_Completed	Info
3152B		Workflow_Timedout	Info
3152C		User_Message	Info
31533		Workflow_Retracted	Info

ID del evento	Proceso	Evento	Gravedad
3152D	Provisión	Provision_Error	Error
3152E		Provision_Submitted	Info
3152F		Provision_Success	Info
31530		Provision_Failure	Error
31531		Provision_Granted	Info
31532		Provision_Revoked	Info
31450	Contexto de seguridad	Create_Proxy_Definition_Success	Info
31451		Create_Proxy_Definition_Failure	Error
31452		Update_Proxy_Definition_Success	Info
31453		Update_Proxy_Definition_Failure	Error
31454		Delete_Proxy_Definition_Success	Info
31455		Delete_Proxy_Definition_Failure	Error
31456		Create_Delegatee_Definition_Success	Info
31457		Create_Delegatee_Definition_Failure	Error
31458		Update_Delegatee_Definition_Success	Info
31459		Update_Delegatee_Definition_Failure	Error
3145A		Delete_Delegatee_Definition_Success	Info
3145B		Delete_Delegatee_Definition_Failure	Error
3145C		Create_Availability_Success	Info
3145D		Create_Availability_Failure	Error
3145E		Delete_Availability_Success	Info
3145F		Delete_Availability_Failure	Error

5.2.4 Informes del registro

Si registra eventos en el canal de la base de datos de Novell Audit, podrá ejecutar informes sobre los datos. Existen varias formas de generar informes con los datos registrados en una base de datos de Novell Audit:

- Utilice la aplicación Novell Audit Report para ejecutar sus propios informes o para ejecutar los informes predefinidos descritos en "Informes del registro predefinidos" en la página 124 más abajo.
- Escriba consultas de los datos registrados mediante iManager seleccionando *Auditoría y registro>Consultas*.
- Escriba sus propias consultas SQL de los datos registrados.

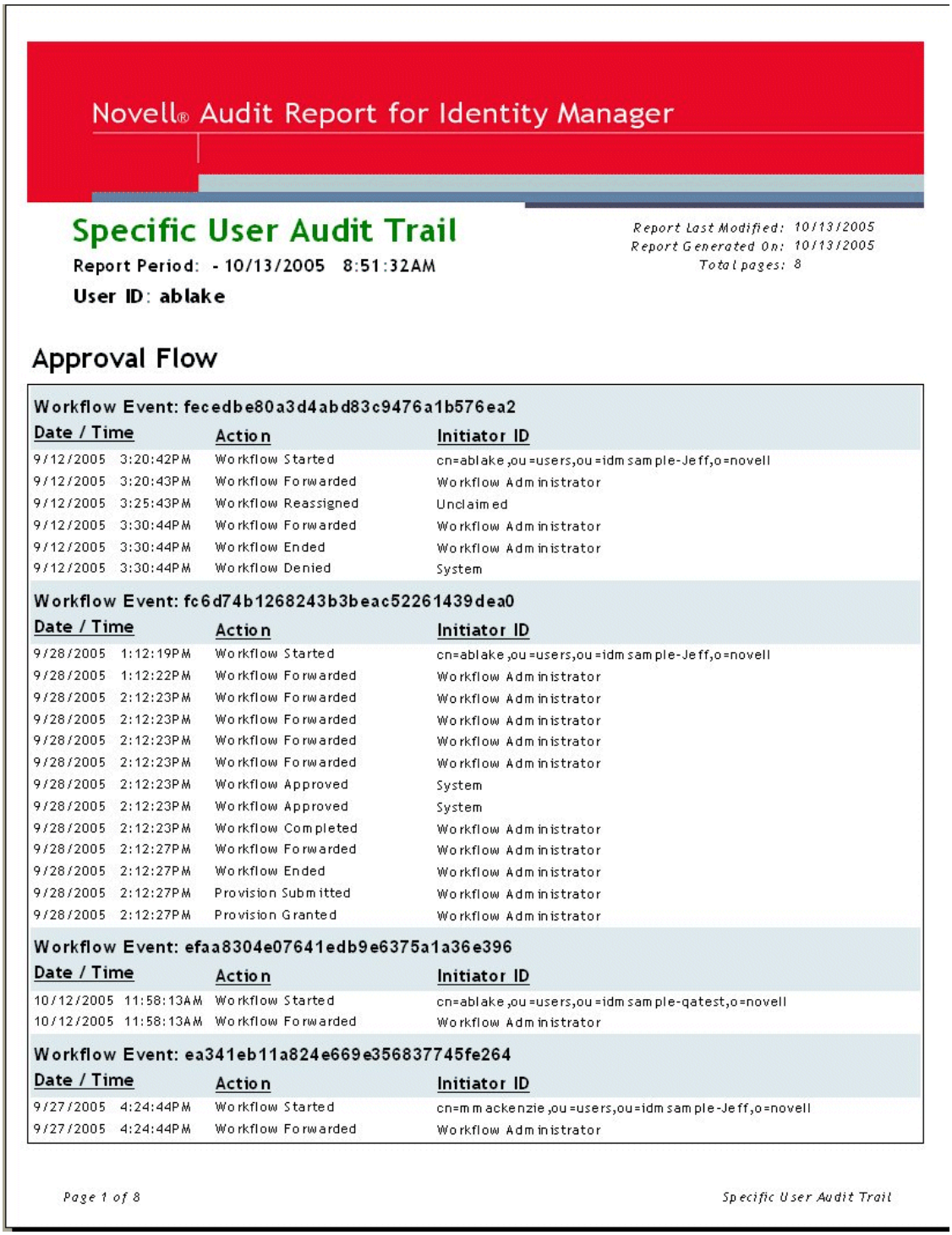
La tabla por defecto de Novell Audit se denomina NAUDITLOG.

Informes del registro predefinidos

Los informes del registro predefinidos se crean en formato (*.rpt*) de Crystal Reports para filtrar los datos registrados en la base de datos de Novell Audit:

Nombre del informe	Descripción
Informe de acciones administrativas	Muestra todas las acciones administrativas iniciadas desde el portal de la aplicación de usuario del Gestor de identidades. Este informe incluye al administrador que inició la acción. Excluye los cambios administrativos efectuados utilizando iManager o el Diseñador para IDM
Informe historial de los flujos de aprobación	Muestra todas las actividades de flujo de aprobación de un tramo horario especificado.
Informe de provisión de recursos	Muestra todas las actividades de provisión, ordenadas por recurso.
Seguimiento de la auditoría de un usuario específico	Muestra toda la actividad relacionada con un usuario. Las actividades pueden ser tanto de provisión como de autoservicio.
Informe de provisión de un usuario específico	Muestra todas las actividades de provisión de un usuario específico.
Informe de provisión de usuarios	Muestra todas las actividades de provisión, ordenadas por usuario.

Informe de ejemplo A continuación, mostramos un ejemplo de seguimiento de la auditoría de un usuario específico



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8

Specific User Audit Trail

Ubicación del archivo de informe Los archivos de informe se encuentran en:

Plataforma	Ubicación
Windows	/nt/dirxml/reports

Puede utilizar estos informes como plantillas para crear informes personalizados en el Diseñador de Crystal Reports o bien puede ejecutar los informes utilizando *Audit Report* (lreport.exe), un programa de Windows suministrado por Novell Audit. Los informes predefinidos realizan consultas en la base de datos de registro por defecto de Novell Audit denominada *naudit* y una tabla de base de datos denominada *auditlog*. Si su base de datos de registro de Novell Audit tiene otro nombre, utilice la opción de menú *Definir ubicación del origen de los datos* del Diseñador de Crystal Reports para sustituir la base de datos *naudit* por la base de datos de su entorno.

Si desea obtener más información, consulte la sección relativa al trabajo con informes en la documentación de Novell Audit (http://www.novell.com/documentation/nsureaudit).

Administración de la aplicación de usuario

III

En estos capítulos se explica cómo configurar y gestionar la aplicación de usuario del Gestor de identidades mediante la pestaña Administración de la interfaz de usuario.

Utilización de la pestaña Administración

6

Este capítulo sirve de introducción a la pestaña Administración de la interfaz de usuario del Gestor de identidades. Aprenderá a utilizar la pestaña Administración para configurar y gestionar la aplicación de usuario del Gestor de identidades. Los temas son:

6.1 Acerca de la pestaña Administración

A la *interfaz de usuario* del Gestor de identidades acceden principalmente usuarios finales que trabajan con las pestañas que ésta proporciona para el autoservicio de identidades y la provisión basada en el flujo de trabajo (con el módulo de provisión del Gestor de identidades). Esta interfaz de usuario basada en navegador también proporciona una pestaña Administración, a la que pueden acceder los administradores para configurar distintas características de la *aplicación de usuario* subyacente del Gestor de identidades.

Por ejemplo, la pestaña Administración se puede utilizar para:

- *Cambiar el tema* utilizado para el aspecto y funcionamiento de la interfaz de usuario
- *Personalizar las funciones de autoservicio de identidades* disponibles para los usuarios finales
- *Especificar qué usuarios tienen permiso* para realizar acciones de administración
- *Gestionar otros datos* acerca de la aplicación de usuario y de su funcionamiento

6.2 Quién puede utilizar la pestaña Administración

Los usuarios habituales de la interfaz de usuario del Gestor de identidades no ven la pestaña Administración. Existen dos tipos de usuarios que pueden verla y acceder a ella:

- *Administrador de la aplicación de usuario*

  Un administrador de la aplicación de usuario tiene permiso para ejecutar todas las funciones de gestión de la aplicación de usuario del Gestor de identidades. Esto incluye acceder a la pestaña Administración de la interfaz de usuario del Gestor de identidades para ejecutar cualquier acción de administración que admita.

  Durante la instalación, se especifica un usuario como administrador de la aplicación de usuario. Después de la instalación, dicho usuario puede utilizar la página *Seguridad* de la pestaña Administración para especificar otros administradores de la aplicación de usuario, según las necesidades.

Para obtener información detallada, consulte Capítulo 11, “Configuración de la seguridad”, en la página 209.

- *Usuarios permitidos por los administradores de la aplicación de usuario*

  Si es preciso, un administrador de la aplicación de usuario puede asignar permisos a uno o varios usuarios para que vean o accedan a páginas específicas de la pestaña Administración. Dichos permisos se asignan utilizando la página *Administrador de páginas* de la pestaña Administración.

  Para obtener información detallada, consulte Capítulo 7, “Administración de páginas”, en la página 135.

6.3 Acceso a la pestaña Administración

Cuando sea un administrador de la aplicación de usuario (u otro usuario permitido) y necesite gestionar la aplicación de usuario del Gestor de identidades, podrá acceder a la pestaña Administración de la interfaz de usuario del Gestor de identidades. Sólo necesita un navegador Web compatible.

Si desea consultar una lista de los navegadores Web compatibles, consulte *Novell Identity Manager: Installation Guide* (Gestor de identidades: Guía de instalación)

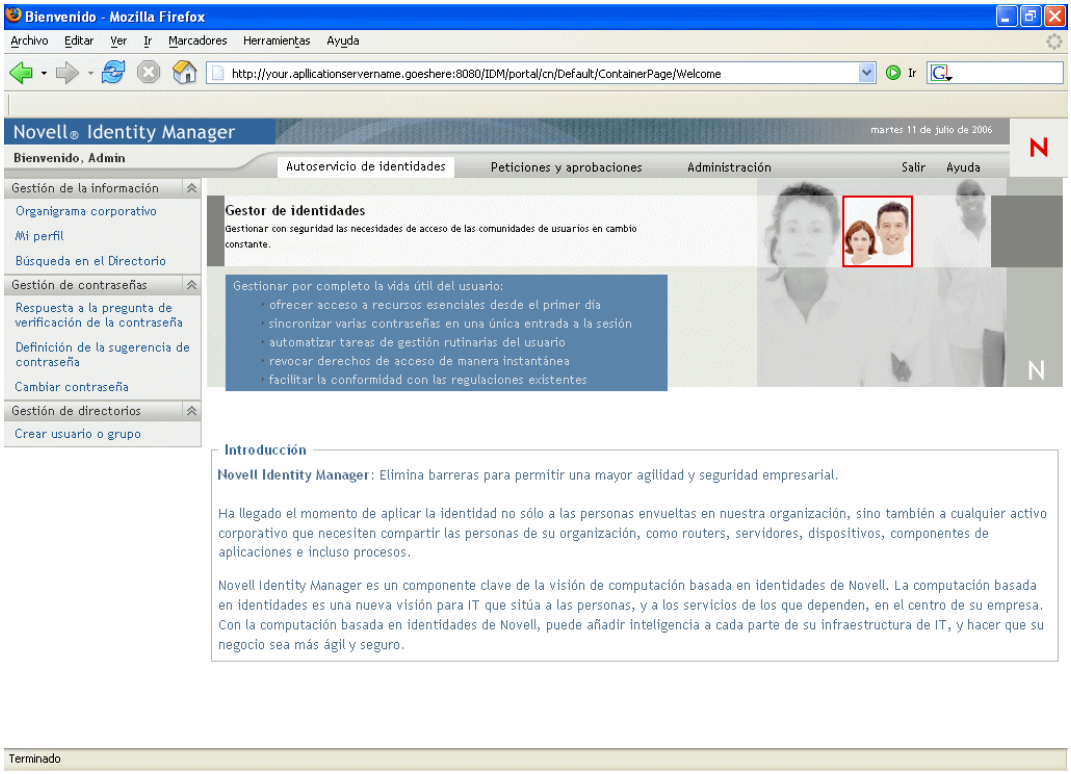
Nota: Para utilizar la interfaz de usuario del Gestor de identidades, asegúrese de que su navegador Web tenga *JavaScript habilitado*.

Para acceder a la pestaña Administración:

1. En el *navegador Web*, vaya a la dirección (URL) de la interfaz de usuario del Gestor de identidades (como está configurada en su sitio). Por ejemplo:

   ```
   http://miservidorapp:8080/IDM
   ```

Se mostrará la *página de bienvenida de invitado* de la interfaz de usuario:

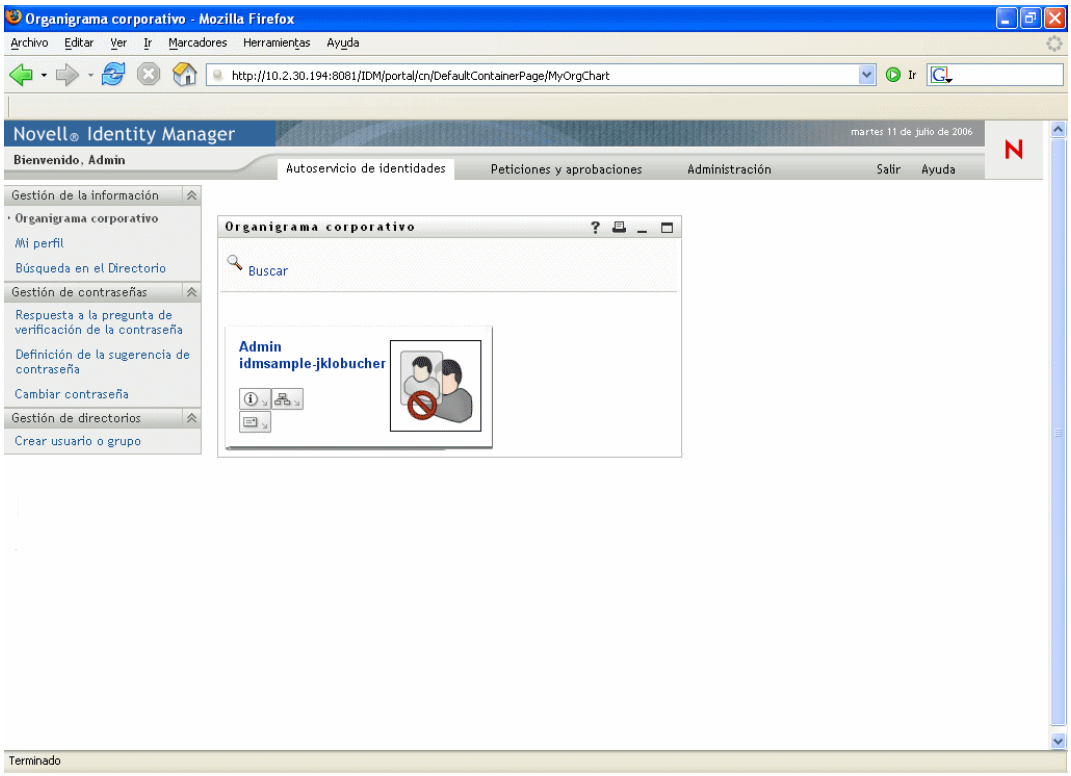


2 Haga clic en el enlace *Entrada* del encabezado de página.

La interfaz de usuario solicita que escriba un nombre de usuario y una contraseña:

3 Entre el nombre de usuario y la contraseña de un *administrador de la aplicación de usuario* (o un usuario con algunos permisos de la pestaña Administración), y haga clic en *Entrada*.

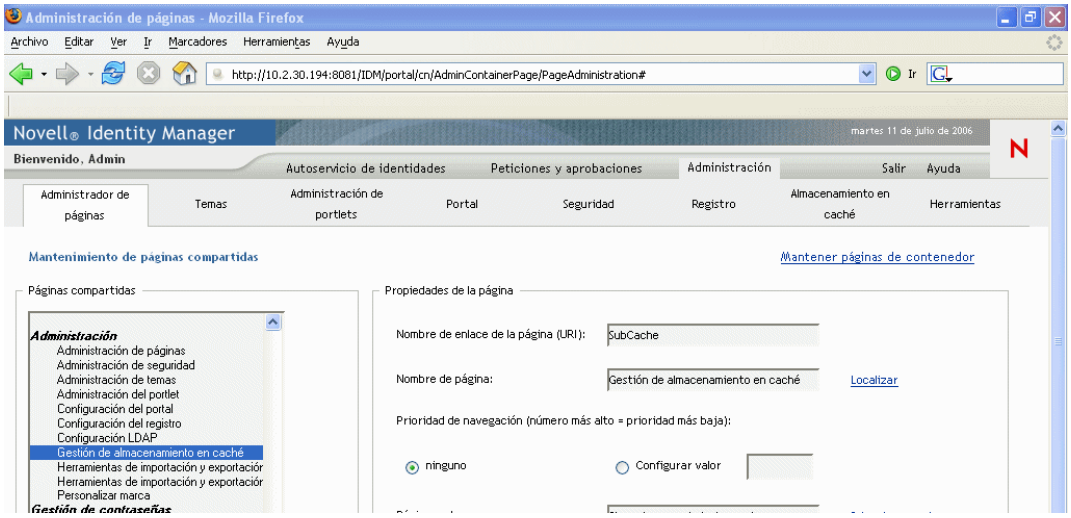
Cuando haya entrado, verá el contenido de la interfaz de usuario apropiado para dicho usuario. Por ejemplo:



Por defecto, se encuentra en la pestaña *Autoservicio de identidades*.

4 Haga clic en la pestaña *Administración*.

La pestaña Administración visualiza un menú de las *acciones de administración* que puede llevar a cabo. Cada opción muestra la página correspondiente de valores y controles. Por defecto, verá la página *Administrador de páginas*:



Para obtener información general acerca de cómo acceder y trabajar en la interfaz de usuario del Gestor de identidades, consulte la guía *Aplicación de usuario del Gestor de identidades: Guía del usuario*.

6.4 Acciones de administración que se pueden efectuar

Cuando esté en la pestaña Administración, podrá utilizar cualquier acción disponible para configurar y gestionar la aplicación de usuario del Gestor de identidades. A continuación, presentamos un resumen:

Acción	Descripción
Administrador de páginas	Controla las páginas que se muestran en la interfaz de usuario del Gestor de identidades y quién tiene permiso para acceder a ellas Para obtener información detallada, consulte Capítulo 7, “Administración de páginas”, en la página 135.
Temas	Controla el aspecto y funcionamiento de la interfaz de usuario del Gestor de identidades Para obtener información detallada, consulte Capítulo 8, “Configuración de temas”, en la página 173.
ADMIN de portlet	Controla los portlets disponibles en la interfaz de usuario del Gestor de identidades y quién tiene permiso para acceder a ellos Para obtener información detallada, consulte Capítulo 9, “Administración de portlets”, en la página 179.
Portal	Controla las características del portal de la aplicación de usuario del Gestor de identidades y especifica cómo se conecta la aplicación de usuario al repositorio seguro de identidades (proveedor de LDAP) Para obtener información detallada, consulte Capítulo 10, “Configuración del portal”, en la página 201.
Seguridad	Especifica quién es el administrador de la aplicación de usuario del Gestor de identidades Para obtener información detallada, consulte Capítulo 11, “Configuración de la seguridad”, en la página 209.
Registro	Controla los niveles de los mensajes de registro que desea que la aplicación de usuario del Gestor de identidades genere y especifica si dichos mensajes (si los hay) se enviarán a Novell Audit. Para obtener información detallada, consulte Capítulo 12, “Configuración del registro”, en la página 213.
Almacenamiento en caché	Gestiona los diversos cachés que mantiene la aplicación de usuario del Gestor de identidades Para obtener información detallada, consulte Capítulo 13, “Configuración del almacenamiento en caché”, en la página 219.

Acción	Descripción
Herramientas	Permite exportar o importar contenido del portal (páginas y portlets) utilizado en la aplicación de usuario del Gestor de identidades Para obtener información detallada, consulte Capítulo 14, “Herramientas para exportar e importar datos del portal”, en la página 229.

Administración de páginas 7

En este capítulo se describe cómo utilizar la página *Administrador de páginas* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general sobre cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

7.1 Acerca de la administración de páginas

Puede utilizar la página Administrador de páginas para controlar las *páginas* visualizadas en la interfaz de usuario del Gestor de identidades y quién tiene *permiso* para acceder a ellas. La interfaz de usuario contiene *dos tipos de páginas*:

Tipo de página	Descripción
Contenedor	Las páginas de contenedor aportan a las páginas compartidas coherencia en el aspecto y funcionamiento, la marca corporativa y la navegación.
Compartidas	Las páginas compartidas aportan un conjunto de contenido coherente que se utiliza para un objetivo específico (como actualizar el perfil de un usuario). Se denominan páginas compartidas, ya que ofrecen servicios que utilizan muchas personas.

Ambos tipos de páginas incluyen contenido en forma de *portlets* (estándar de Java para elementos conectables de la interfaz de usuario).

Para saber más acerca de portlets, consulte Capítulo 9, “Administración de portlets”, en la página 179 y Parte IV, “Referencia de portlet”, en la página 237.

7.1.1 Acerca de las páginas de contenedor

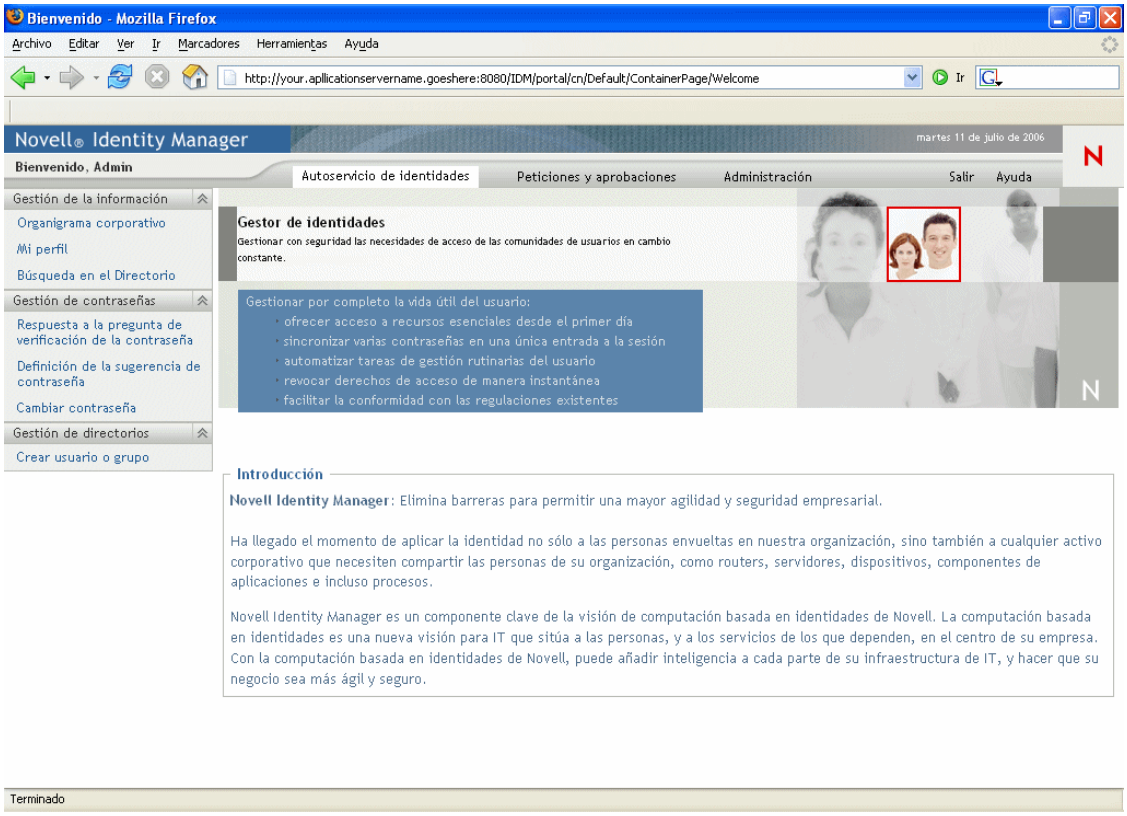
Esta sección sirve de introducción a algunas páginas de contenedor que tienen un papel importante en la interfaz de usuario del Gestor de identidades:

Recuerde que, si así lo desea, puede modificar estas páginas de contenedor. También tiene la opción de añadir sus propias páginas de contenedor.

Para obtener información acerca de cómo trabajar con las páginas de contenedor, consulte Sección 7.2, “Creación y mantenimiento de páginas de contenedor”, en la página 143.

GuestContainerPage

Por defecto, cuando los usuarios llegan a la interfaz de usuario del Gestor de identidades *antes de registrarse*, ven la página de contenedor denominada *GuestContainerPage*. Dicha página de contenedor se visualiza como indicamos a continuación:



Internamente, GuestContainerPage tiene el *diseño* siguiente:

El diseño de GuestContainerPage está dividido en *tres regiones*, que muestran los portlets siguientes:

Portlet	Descripción
HeaderPortlet	Muestra la pestaña de máximo nivel y la información del encabezado de la interfaz de usuario
Navegación de páginas compartidas	Muestra un menú vertical donde el usuario puede seleccionar una página compartida para visualizarla
Controlador de páginas de portal	Muestra la página compartida que el usuario tiene actualmente seleccionada mediante el portlet de navegación de páginas compartidas

Tenga en cuenta que, por defecto, los usuarios sólo ven los elementos siguientes antes de registrarse:

- Un enlace único en el encabezado: *Entrada*
- Una única página compartida: *Bienvenido*

Como el usuario todavía no se ha registrado, el portlet de Navegación de páginas compartidas sólo muestra las páginas compartidas que entran dentro de la categoría *Páginas para invitados (GUEST)*

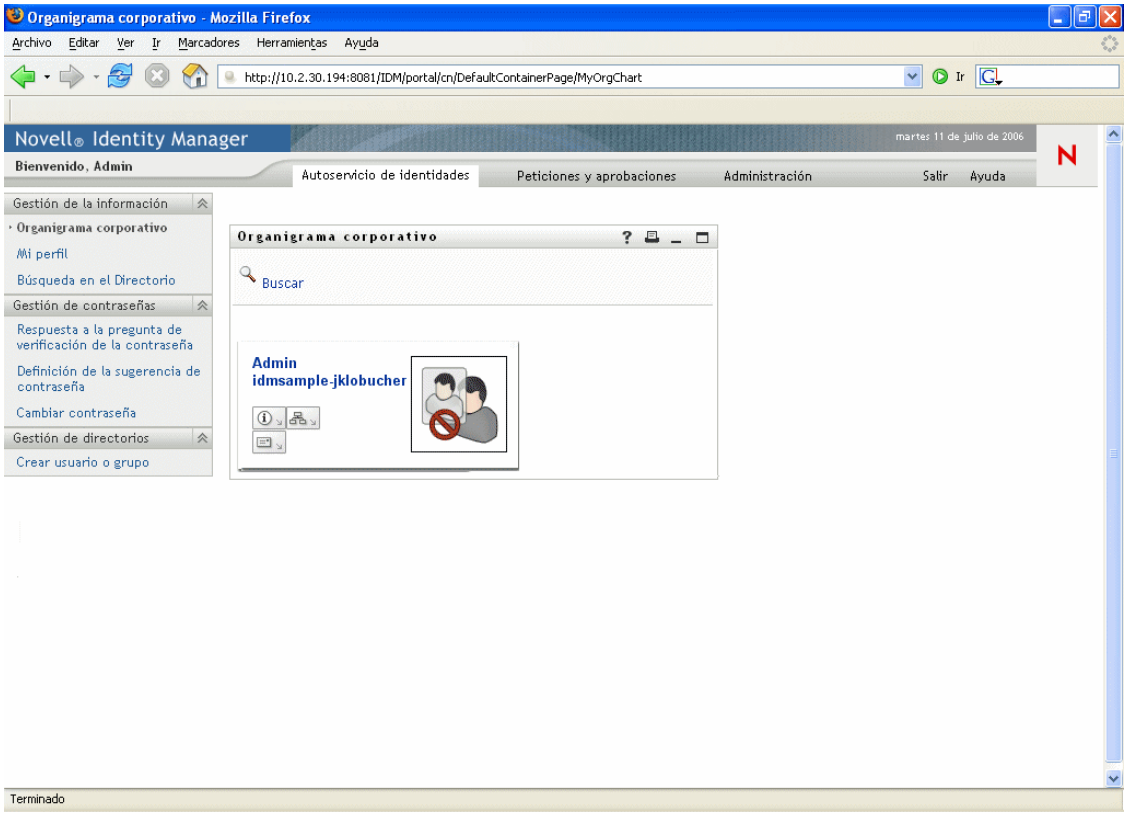
y filtra todas las categorías restantes. Por defecto, Bienvenido es la única página de la categoría de Páginas de invitado.

Después de registrarse, el portlet de Navegación de páginas compartidas filtra la categoría Páginas para invitados (GUEST). Y, en su lugar, muestra otras categorías de páginas compartidas (tal como se ha especificado en sus preferencias).

Para obtener más información acerca del portlet de Navegación de páginas compartidas, consulte Capítulo 15, “Acerca de los portlets”, en la página 239.

DefaultContainerPage

Por defecto, *después de que los usuarios se registran en* la interfaz de usuario del Gestor de identidades, van a la página de contenedor denominada *DefaultContainerPage*. Dicha página de contenedor se visualiza como indicamos a continuación:



Internamente, DefaultContainerPage tiene el *diseño* siguiente:

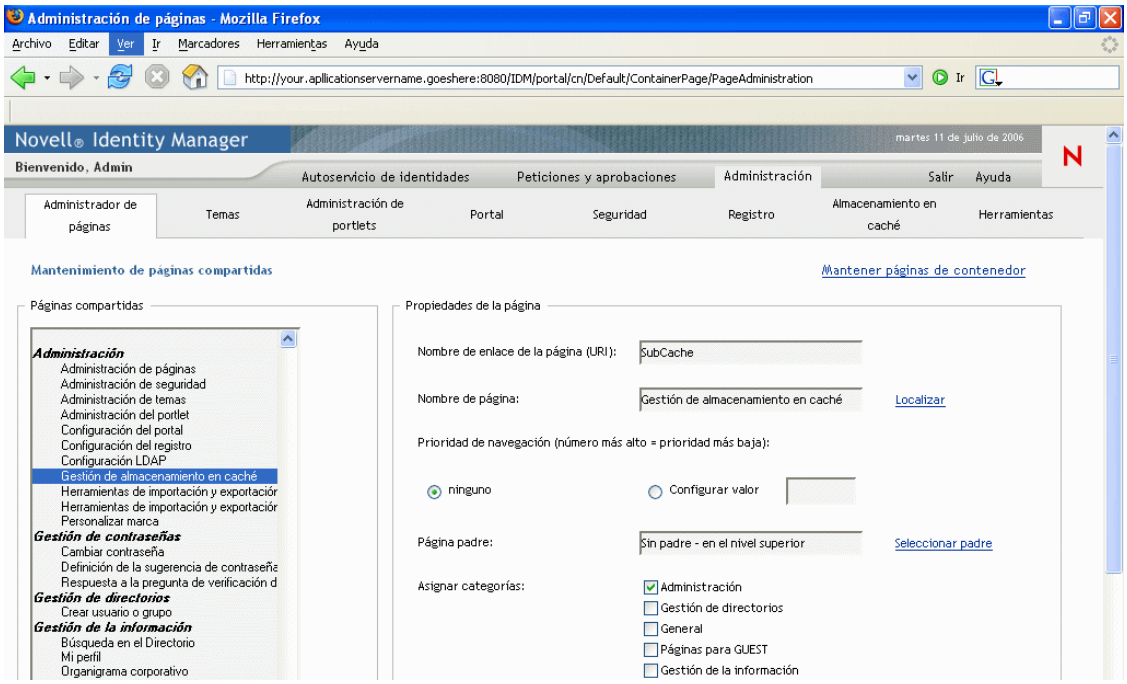
El diseño de DefaultContainerPage está dividido en *tres regiones*, que muestran los portlets siguientes:

Portlet	Descripción
HeaderPortlet	Muestra la pestaña de máximo nivel y la información del encabezado de la interfaz de usuario
Navegación de páginas compartidas	Muestra un menú vertical donde el usuario puede seleccionar una página compartida a visualizar
Controlador de páginas de portal	Muestra la página compartida que el usuario tiene actualmente seleccionada mediante el portlet Navegación de páginas compartidas
Advertencia de tiempo límite de la sesión	Muestra un mensaje de alerta siempre que la sesión de un usuario está a punto de llegar al tiempo límite

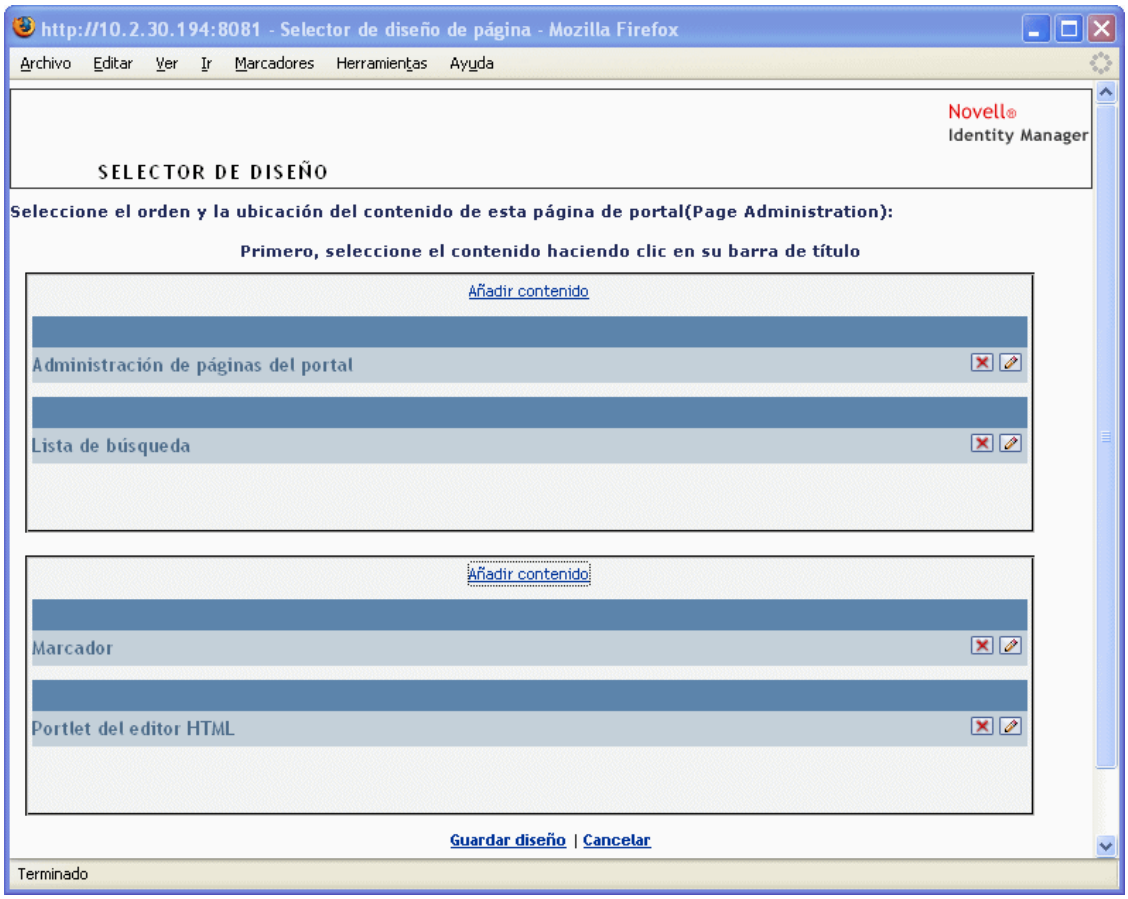
Recuerde que, después del registro del usuario, *DefaultContainerPage abre automáticamente la pestaña Autoservicio de identidades* en HeaderPortlet.

Página de contenedor de ADMIN

Por defecto, cuando los administradores de la aplicación de usuario (y otros usuarios autorizados) *hacen clic en la pestaña Administración* de la interfaz de usuario del Gestor de identidades, van a la página de contenedor denominada *Página de contenedor ADMIN*. Dicha página de contenedor se visualiza como indicamos a continuación:



Internamente, la página de contenedor ADMIN tiene el *diseño* siguiente:



El diseño de la página de contenedor ADMIN está dividido en *dos regiones*, que muestran los portlets siguientes:

Portlet	Descripción
HeaderPortlet	Muestra la pestaña de máximo nivel y la información del encabezado de la interfaz de usuario
Visualización de la lista ADMIN	Muestra un segundo nivel de pestañas donde el usuario puede seleccionar una acción de administración para ejecutarla
Controlador de páginas de portal	Muestra una página compartida que corresponde a la pestaña seleccionada actualmente por el usuario mediante el portlet Visualización de la lista ADMIN
Advertencia de tiempo límite de la sesión	Muestra un mensaje de alerta siempre que la sesión de un usuario está a punto de llegar al tiempo límite

7.1.2 Acerca de las páginas compartidas

La interfaz de usuario del Gestor de identidades incluye un gran número de páginas compartidas que proporcionan la mayor parte del contenido de sus páginas de contenedor. Si es preciso, dichas

páginas compartidas se pueden modificar. También tiene la opción de añadir sus propias páginas compartidas.

Para obtener información acerca de cómo trabajar con páginas compartidas, consulte Sección 7.3, “Creación y mantenimiento de páginas compartidas”, en la página 152.

Página compartida normal

Echemos un vistazo a una de las páginas compartidas. *Organigrama corporativo* es la *página compartida por defecto* que DefaultContainerPage muestra después de que los usuarios entren en la interfaz de usuario del Gestor de identidades:

Internamente, Organigrama corporativo tiene el *diseño* siguiente:

El organigrama corporativo está formado sólo por *una región*, que muestra sólo un portlet (el portlet *Organigrama corporativo*).

7.1.3 Excepción en el uso de páginas

En este capítulo, acaba de ver cómo estas pestañas de máximo nivel de la interfaz de usuario del Gestor de identidades están basadas en páginas:

- La *pestaña Autoservicio de identidades* utiliza *DefaultContainerPage*
- La *pestaña Administración* utiliza la *Página de contenedor ADMIN*

No obstante, tenga en cuenta que la *pestaña Peticiones y aprobaciones* está basada en otra arquitectura y *no se puede manipular* mediante el Administrador de páginas.

7.2 Creación y mantenimiento de páginas de contenedor

El proceso de crear y mantener páginas de contenedor implica los pasos siguientes:

1. *Crear* una página de contenedor nueva o *seleccionar* una página de contenedor ya existente, tal como se describe en Sección 7.2.1, “Creación de páginas de contenedor”, en la página 144.

2. *Añadir contenido* (en forma de portlets) a la página, tal como se describe en Sección 7.2.2, “Adición de contenido a una página de contenedor”, en la página 147.

   Es posible que también desee *suprimir contenido* de la página, tal como se describe en Sección 7.2.3, “Supresión de contenido de una página de contenedor”, en la página 148.

3. *Seleccionar un diseño de portal*, tal como se describe en Sección 7.2.4, “Modificación del diseño de una página de contenedor”, en la página 149.

4. *Arreglar el orden y la posición* del contenido en el diseño seleccionado, tal como se describe en Sección 7.2.5, “Organización del contenido de la página de contenedor”, en la página 150.

5. *Visualizar la nueva página* directamente introduciendo la URL de la página de contenedor en el navegador, tal como se describe en Sección 7.2.6, “Visualización de una página de contenedor”, en la página 152.

Páginas de contenedor y diseños Las páginas de contenedor no están estrechamente vinculadas a los diseños de portal. Esto significa que puede cambiar los diseños de las páginas de contenedor sin perder contenido de la página. Cuando se aplica un diseño nuevo a la página de contenedor, todos los portlets que se hayan añadido a la página se visualizarán automáticamente con el nuevo diseño. Es posible que deba ajustar con mayor precisión la colocación de contenido en el diseño nuevo.

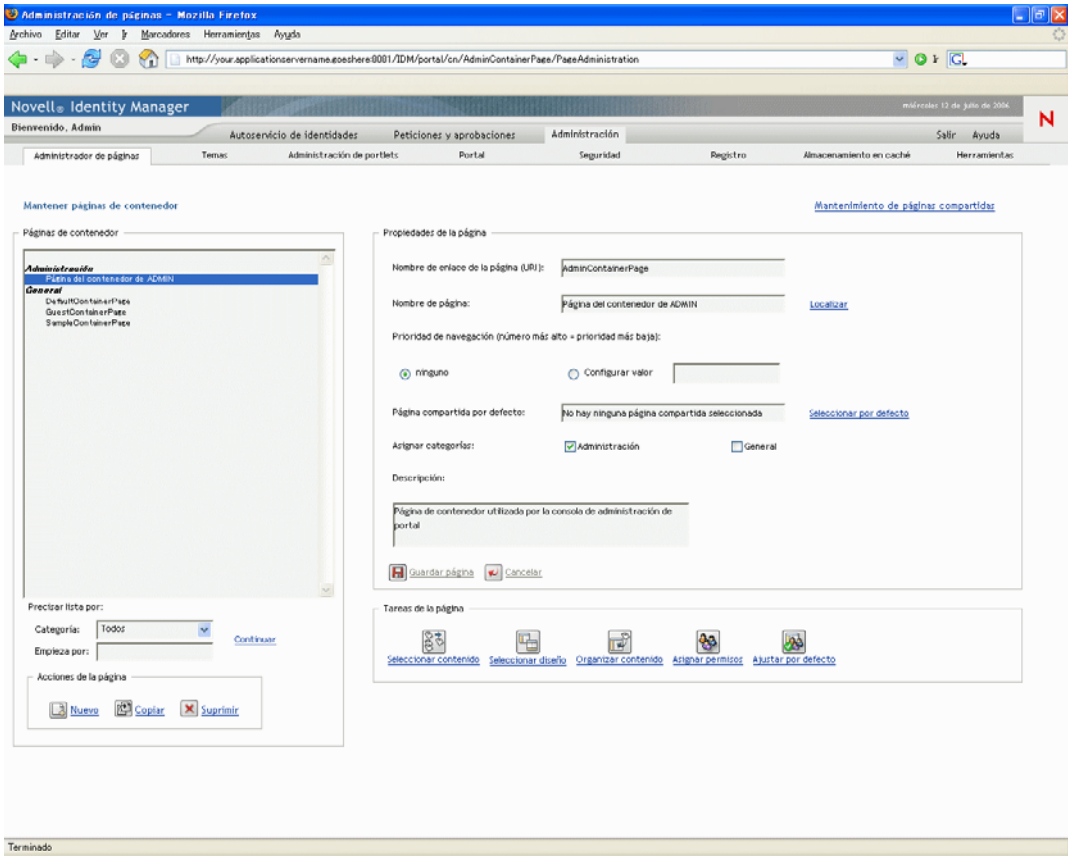
7.2.1 Creación de páginas de contenedor

Las páginas de contenedor se pueden crear a partir de cero o bien copiando páginas existentes. En esta sección se describen ambos procedimientos.

Para crear una página de contenedor a partir de cero:

1. En la página Administrador de páginas, seleccione *Mantenimiento de páginas de contenedor*.

Se visualizará el panel Mantenimiento de páginas de contenedor:



2 Seleccione la acción de la página *Nuevo* (en la sección inferior izquierda del panel).

Se creará una página de contenedor sin título ni categoría.

3 Especifique las *propiedades de página* de la página de contenedor:

Propiedad	Operaciones que puede realizar
Nombre de enlace de la página (URI)	Especifique el nombre URI de la página (tal como aparecerá dentro de la URL de la interfaz de usuario). Por ejemplo, si especifica el URI: `MiPáginaContenedor` aparecerá dentro de la URL tal como mostramos a continuación: `http://miservidorapp:8080/IDM/portal/cn/`**`MiPáginaContenedor`**

Propiedad	Operaciones que puede realizar
Nombre de página	Especifique el nombre de visualización de la página. Por ejemplo: `Mi página de contenedor` Puede hacer clic en **Localizar** para especificar las versiones localizadas de este nombre en otros idiomas.
Prioridad de navegación	Especifique una de las opciones siguientes: ◆ **Ninguno** : si no necesita asignar ninguna prioridad a esta página de contenedor. ◆ **Configurar valor** : para asignar una prioridad a esta página de contenedor, en relación a otras páginas de contenedor. La prioridad debe ser un número entero comprendido entre -1 y 9999, en el que -1 es la prioridad más alta y 9999 es la más baja. Definir valores de prioridad es útil si se desea asegurar un orden determinado cuando las páginas se indican por prioridad o bien si se desea asegurar una selección concreta, cuando hay varias páginas por defecto (en caso de que un usuario pertenezca a varios grupos).
Página compartida por defecto	Consulte Sección 7.6, “Selección de una página compartida por defecto para una página de contenedor”, en la página 170.
Asignar categorías	Seleccione cero o más de las categorías siguientes a las que desee que la página pertenezca: ◆ Administración ◆ General La asignación de categorías es útil si se desea asegurar una organización adecuada, cuando las páginas se enumeran por categoría o si se desea asegurar un subconjunto adecuado cuando las páginas se filtran por categoría.
Descripción	Escriba texto que describa la página.

4 Haga clic en *Guardar página* (en la parte inferior de la sección de propiedades de la página).

Para crear una página de contenedor copiando una página existente:

1 En la página Administrador de páginas, seleccione *Mantenimiento de páginas de contenedor*.

Se visualizará el panel Mantenimiento de páginas de contenedor (tal como se muestra en el procedimiento anterior).

2 En la lista de páginas de contenedor, *seleccione* la página que desee copiar.

Sugerencia: Si la lista es larga, puede *precisarla* (por categoría o texto de inicio) para encontrar más fácilmente la página deseada.

3 Seleccione la acción de la página *Copiar* (en la sección inferior izquierda del panel).

Se creará una página de contenedor nueva con el nombre *Copia de nombre_página_original*.

4 Especifique las *propiedades de página* de la página de contenedor (tal como se describe en el procedimiento anterior).

5 Haga clic en *Guardar página* (en la parte inferior de la sección de propiedades de la página).

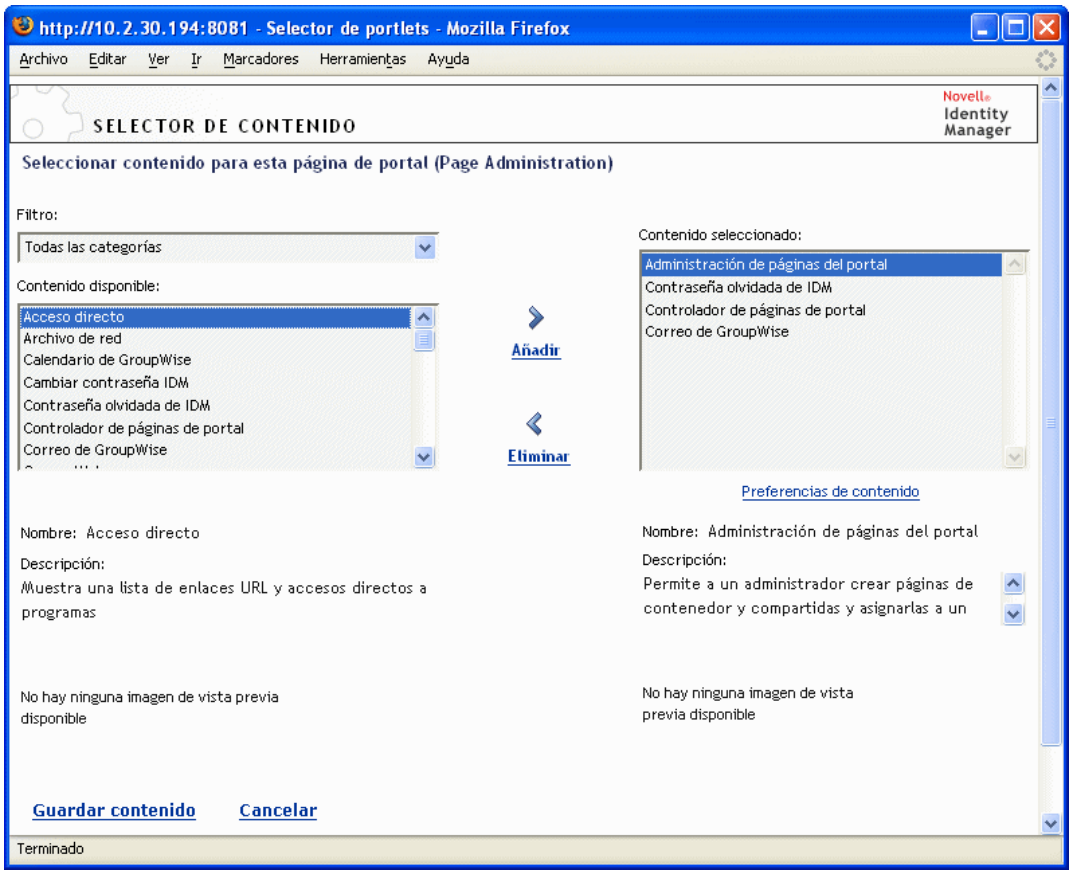
7.2.2 Adición de contenido a una página de contenedor

Después de crear una página de contenedor, el paso siguiente consiste en añadir contenido seleccionando portlets para colocarlos en la página. Puede utilizar portlets creados anteriormente con la aplicación de usuario del Gestor de identidades u otros portlets que haya registrado.

Para añadir contenido a una página de contenedor:

1 Abra una página nueva o ya existente en el panel Mantenimiento de páginas de contenedor y haga clic en la tarea de la página *Seleccionar contenido* (en la parte inferior del panel).

El *Selector de contenido* se visualizará en una ventana del navegador nueva:



2 Si desea visualizar una categoría específica del contenido disponible, seleccione la categoría en el menú desplegable *Filtro*.

3 Seleccione uno o varios portlets en la lista de *Contenido disponible*.

Sugerencia: Mantenga pulsada la tecla *Control* para seleccionar en la lista varios portlets que no sean contiguos; utilice la tecla *Mayús* para realizar varias selecciones contiguas.

4. Haga clic en *Añadir* para mover las opciones a la lista de *Contenido seleccionado*.
5. Puede hacer clic en *Preferencias de contenido* para editar las preferencias de cualquier portlet que haya seleccionado para su página de contenedor. Los valores de preferencia que especifique entrarán en vigor para la instancia del portlet que aparezca en la página.
6. Haga clic en *Guardar contenido*.

   Ahora que ha elegido el contenido de la página de contenedor, puede seleccionar un diseño nuevo, tal como se describe en Sección 7.2.4, "Modificación del diseño de una página de contenedor", en la página 149 u ordenar el contenido del diseño actual, tal como se describe en Sección 7.2.5, "Organización del contenido de la página de contenedor", en la página 150.

7.2.3 Supresión de contenido de una página de contenedor

En el transcurso de la creación de páginas de contenedor, es posible que desee suprimir contenido eliminando portlets de una página. Puede utilizar el selector de contenido o el selector de diseño, tal como se describe en los procedimientos siguientes.

Para suprimir contenido de una página de contenedor utilizando el selector de contenido:

1. Abra una página del panel Mantenimiento de páginas de contenedor y haga clic en la tarea de la página *Seleccionar contenido* (en la parte inferior del panel).

   El *selector de contenido* se visualizará en una ventana del navegador nueva (tal como se muestra en el procedimiento anterior).
2. Seleccione el portlet que desee suprimir en la lista Contenido seleccionado y haga clic en *Eliminar*.

   Se eliminará el portlet de la página.
3. Haga clic en *Guardar contenido*.

Para suprimir contenido de una página de contenedor utilizando el selector de diseño:

1. Abra una página en el panel Mantenimiento de páginas de contenedor y haga clic en la tarea de la página *Organizar contenido* (en la parte inferior del panel).

El *selector de diseño* se visualizará en una ventana del navegador nueva y mostrará los portlets de dicha página:

2 Haga clic en el botón *X* en el caso de un portlet que desee eliminar.

3 Cuando el sistema le solicite una confirmación , haga clic en *Aceptar*.

Se eliminará el portlet de la página.

4 Haga clic en *Guardar diseño*.

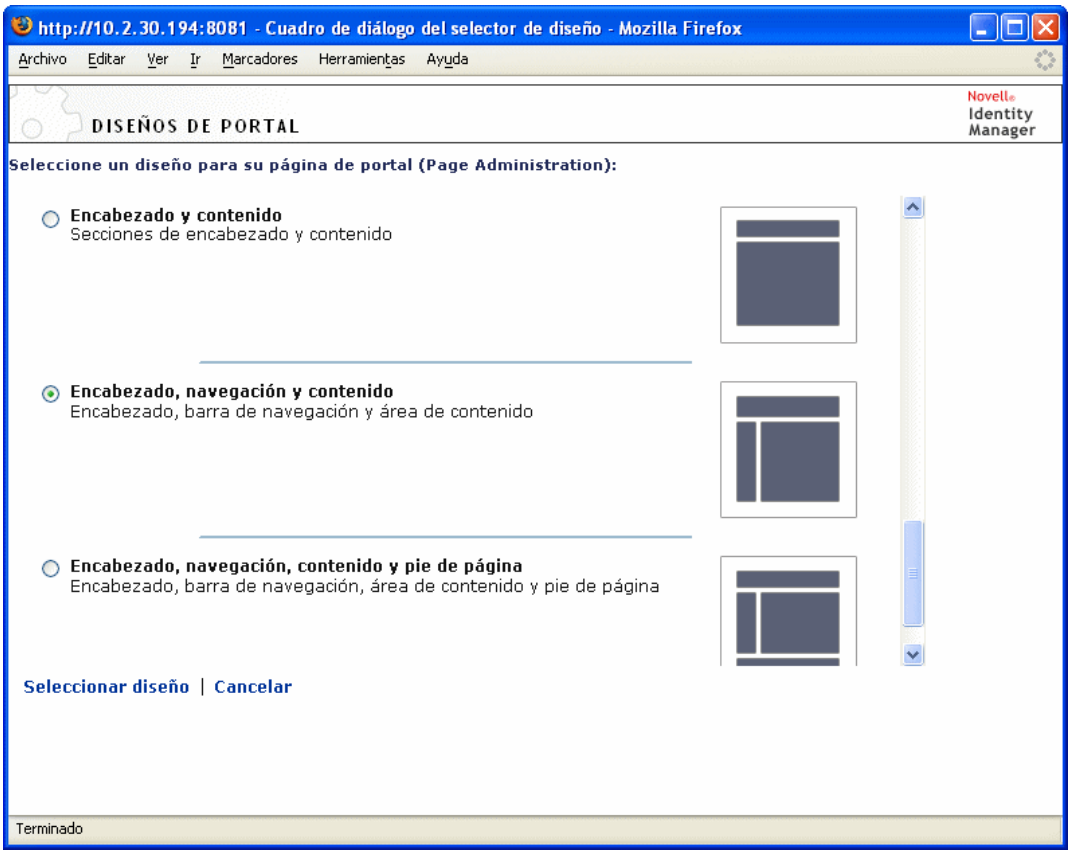
7.2.4 Modificación del diseño de una página de contenedor

Cuando modifique el diseño de una página de contenedor, el contenido existente se desplazará para acomodar el nuevo diseño. En algunos casos, es posible que tenga que ajustar con precisión el resultado final.

Para modificar el diseño de una página de contenedor:

1 Abra una página del panel Mantenimiento de páginas de contenedor y haga clic en la tarea de la página *Seleccionar diseño* (en la parte inferior del panel).

La lista *Diseños de portal* se visualizará en una ventana del navegador nueva:



2 *Desplácese* por las opciones y *seleccione* el diseño que desee.

3 Haga clic en *Seleccionar diseño*.

7.2.5 Organización del contenido de la página de contenedor

Después de decidir el contenido y diseño de la página de contenedor, puede colocar el contenido en el diseño seleccionado, añadir otros portlets en ubicaciones específicas o suprimir portlets.

Para ordenar el contenido de una página de contenedor:

1 Abra una página en el panel Mantenimiento de páginas de contenedor y haga clic en la tarea de la página *Organizar contenido* (en la parte inferior del panel).

El *selector de diseño* se visualizará en una ventana del navegador nueva y mostrará los portlets de dicha página:

2 Si desea *añadir un portlet* a la página, ejecute los pasos siguientes:

2a Haga clic en *Añadir contenido* en la trama de diseño deseada.

El *selector de portlet* se visualizará en una ventana del navegador nueva.

2b Si desea visualizar una categoría específica del contenido disponible, seleccione la categoría en el menú desplegable *Filtro*.

2c Seleccione el portlet que desee en la lista de *Contenido disponible*.

2d Haga clic en *Seleccionar contenido*.

El selector de portlets se cerrará y el portlet seleccionado aparecerá en la trama de diseño de destino del selector de diseños.

3 Si desea *mover un portlet* a otra ubicación del diseño, siga los pasos siguientes específicos para el navegador:

Navegador	Operaciones que puede realizar
Internet Explorer	1. Mover el cursor sobre la barra de título del portlet hasta que el cursor cambie y se convierta en una mano. 2. Con el botón izquierdo del ratón pulsado, arrastre el portlet hasta el lugar deseado del diseño.

Navegador	Operaciones que puede realizar
Mozilla	1. Haga clic en el portlet que desee mover. 2. Haga clic dentro de la trama de diseño de destino. El portlet se moverá hasta el destino.

4 Si desea *eliminar un portlet* del diseño, ejecute los pasos siguientes:

4a Haga clic en el botón *X* del portlet que desee eliminar.

4b Cuando el sistema le solicite una confirmación, haga clic en *Aceptar*.

Se eliminará el portlet del diseño.

5 Si desea *editar las preferencias* de un portlet, ejecute los pasos siguientes:

5a Haga clic en el botón *lápiz* del portlet que desee editar.

Las *preferencias de contenido* del portlet se visualizarán en el navegador.

5b *Cambie* los valores de preferencia según sus necesidades.

Los valores de preferencia que especifique entrarán en vigor para la instancia del portlet que aparezca en la página.

5c Haga clic en *Guardar preferencias*.

6 Haga clic en *Guardar diseño* para registrar los cambios y cerrar el selector de diseños.

7.2.6 Visualización de una página de contenedor

Puede visualizar su página yendo a la URL de la página de contenedor en el navegador.

Para visualizar una página de contenedor:

- En el *navegador Web*, vaya a la URL siguiente:

```
http://servidor:puerto/contexto-war-IDM/portal/cn/nombre-página-contenedor
```

Por ejemplo, para visualizar la página de contenedor denominada *MiPáginaContenedor*:

```
http://miservidorapp:8080/IDM/portal/cn/MiPáginaContenedor
```

7.3 Creación y mantenimiento de páginas compartidas

El proceso de crear y mantener páginas compartidas implica los pasos siguientes:

1 *Crear* una página compartida nueva o *seleccionar* una página compartida ya existente, tal como se describe en Sección 7.3.1, “Creación de páginas compartidas”, en la página 153.

2. *Añadir contenido* (en forma de portlets) a la página, tal como se describe en Sección 7.3.2, “Adición de contenido a una página compartida”, en la página 157.

   Es posible que también desee *suprimir contenido* de la página, tal como se describe en Sección 7.3.3, “Supresión de contenido de una página compartida”, en la página 158.

3. *Seleccionar un diseño de portal*, tal como se describe en Sección 7.3.4, “Modificación del diseño de una página compartida”, en la página 159.

4. *Arreglar el orden y posición* del contenido en el diseño seleccionado, tal como se describe en Sección 7.3.5, “Organización del contenido de la página compartida”, en la página 160.

5. *Visualizar la nueva página* directamente introduciendo la URL de la página compartida en el navegador, tal como se describe en Sección 7.2.6, “Visualización de una página de contenedor”, en la página 152.

Páginas compartidas y diseños Las páginas compartidas no están estrechamente vinculadas a los diseños de portal. Esto significa que puede cambiar los diseños de las páginas compartidas sin perder ningún contenido de página. Cuando se aplica un diseño nuevo, todos los portlets que se hayan añadido a la página se visualizarán automáticamente utilizando el nuevo diseño. Es posible que tenga que ajustar con precisión la colocación de contenido en el diseño nuevo.

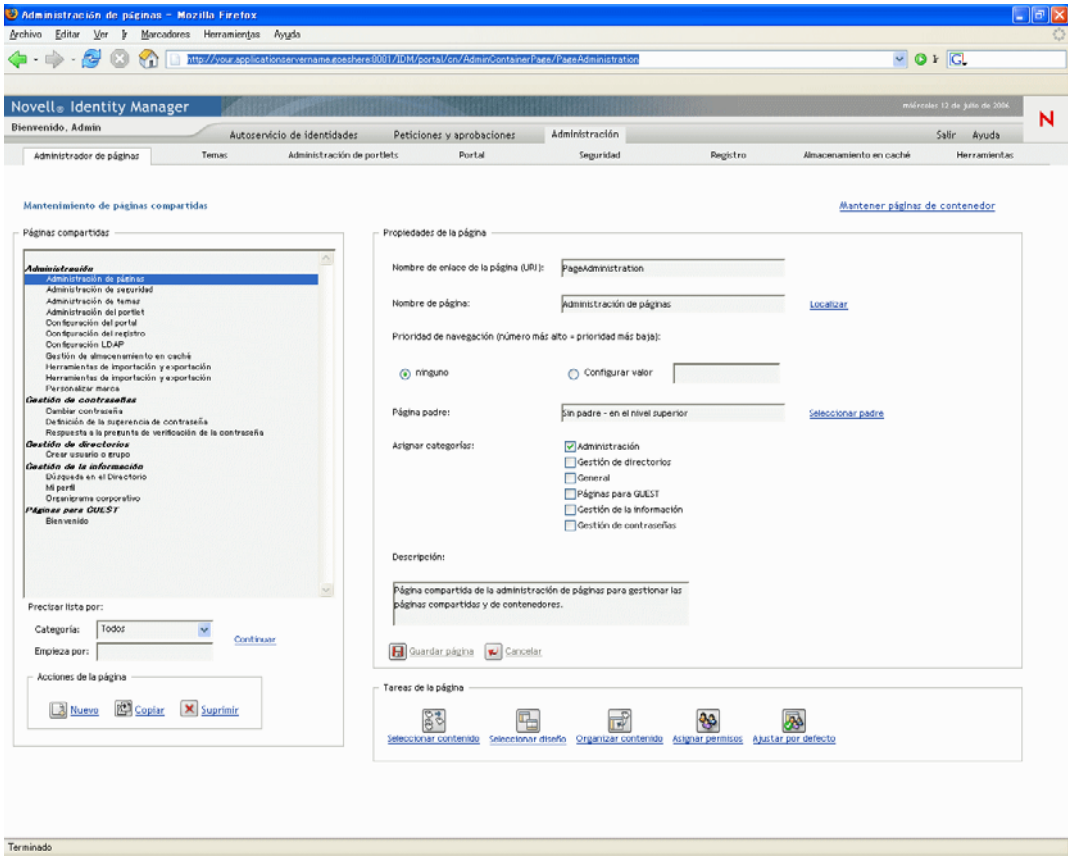
7.3.1 Creación de páginas compartidas

Las páginas compartidas se pueden crear a partir de cero o bien copiando páginas existentes. En esta sección se describen ambos procedimientos.

Para crear una página compartida a partir de cero:

1. En la página Administrador de páginas, seleccione *Mantenimiento de páginas compartidas*.

Se visualizará el panel Mantenimiento de páginas compartidas:



2 Seleccione la acción de la página *Nuevo* (en la sección inferior izquierda del panel).

Se creará una página compartida sin título ni categoría.

3 Especifique las *propiedades de página* de la página compartida:

Propiedad	Operaciones que puede realizar
Nombre de enlace de la página (URI)	Especifique el nombre URI de la página (tal como aparecerá dentro de la URL de la interfaz de usuario). Por ejemplo, si especifica el URI: `MiPáginaCompartida` aparecerá dentro de la URL tal como mostramos a continuación: `http://miservidorapp:8080/IDM/portal/cn/MiPáginaContenedor/`**`MiPáginaCompartida`**

Propiedad	Operaciones que puede realizar
Nombre de página	Especifique el nombre de visualización de la página. Por ejemplo: `Mi Página Compartida` Puede hacer clic en **Localizar** para especificar las versiones localizadas de este nombre en otros idiomas.
Prioridad de navegación	Especifique una de las opciones siguientes: ◆ **Ninguna**: si no necesita asignar ninguna prioridad a esta página compartida. ◆ **Configurar valor** : para asignar una prioridad a esta página compartida, en relación a otras páginas compartidas. La prioridad debe ser un número entero comprendido entre -1 y 9999, en el que -1 es la prioridad más alta y 9999 es la más baja. Definir valores de prioridad es útil cuando se desea asegurar un orden determinado cuando las páginas se indican por prioridad o si se desea asegurar una selección concreta, cuando hay varias páginas por defecto (en caso de que un usuario pertenezca a varios grupos).
Página padre	Si desea que esta página compartida sea hija de otra página compartida, haga clic en **Seleccionar padre**. Asegúrese de que tanto la página padre como la página hijo pertenezcan a las **mismas categorías** (para evitar problemas de visualización). En el tiempo de ejecución, el usuario final verá esta relación cuando utilice el portlet Navegación de páginas compartidas. Cuando visualice la lista de páginas compartidas, verá las entradas de los hijos bajo la de los padres. (Tenga en cuenta que las páginas hijo no heredan el contenido, ni las preferencias, ni los valores de sus páginas padre. Por otra parte, las páginas padre no visualizan automáticamente el contenido de las páginas hijo junto con su propio contenido).

Propiedad	Operaciones que puede realizar
Asignar categorías	Seleccione cero o más de las categorías siguientes a las que desee que la página pertenezca: ◆ Administración ◆ Gestión del directorio ◆ General ◆ Páginas para invitados (GUEST) ◆ Gestión de la información ◆ Gestión de contraseñas La asignación de categorías es útil si se desea garantizar una organización adecuada, cuando las páginas se enumeran por categoría o si se desea asegurar un subconjunto adecuado cuando las páginas se filtran por categoría. **Nota: Páginas para invitados (GUEST)** es una categoría especial utilizada para identificar las páginas compartidas que pueden visualizarse antes de que el usuario entre (y no después). Para obtener más información, consulte la sección relativa al portlet de navegación de páginas compartidas en Capítulo 15, “Acerca de los portlets”, en la página 239.
Descripción	Escriba texto que describa la página.

4 Haga clic en *Guardar página* (en la parte inferior de la sección de propiedades de la página).

Para crear una página compartida copiando una página existente:

1 En la página Administrador de páginas, seleccione *Mantenimiento de páginas compartidas*.

Se visualizará el panel Mantenimiento de páginas compartidas (tal como se muestra en el procedimiento anterior).

2 En la lista de páginas compartidas, *seleccione* la página que desee copiar.

Sugerencia: Si la lista es larga, puede *precisarla* (por categoría o texto de inicio) para encontrar más fácilmente la página deseada.

3 Seleccione la acción de la página *Copiar* (en la sección inferior izquierda del panel).

Se creará una página compartida nueva con el nombre *Copia de nombre_página_original*.

4 Especifique las *propiedades de página* de la página compartida (tal como se describe en el procedimiento anterior).

5 Haga clic en *Guardar página* (en la parte inferior de la sección de propiedades de la página).

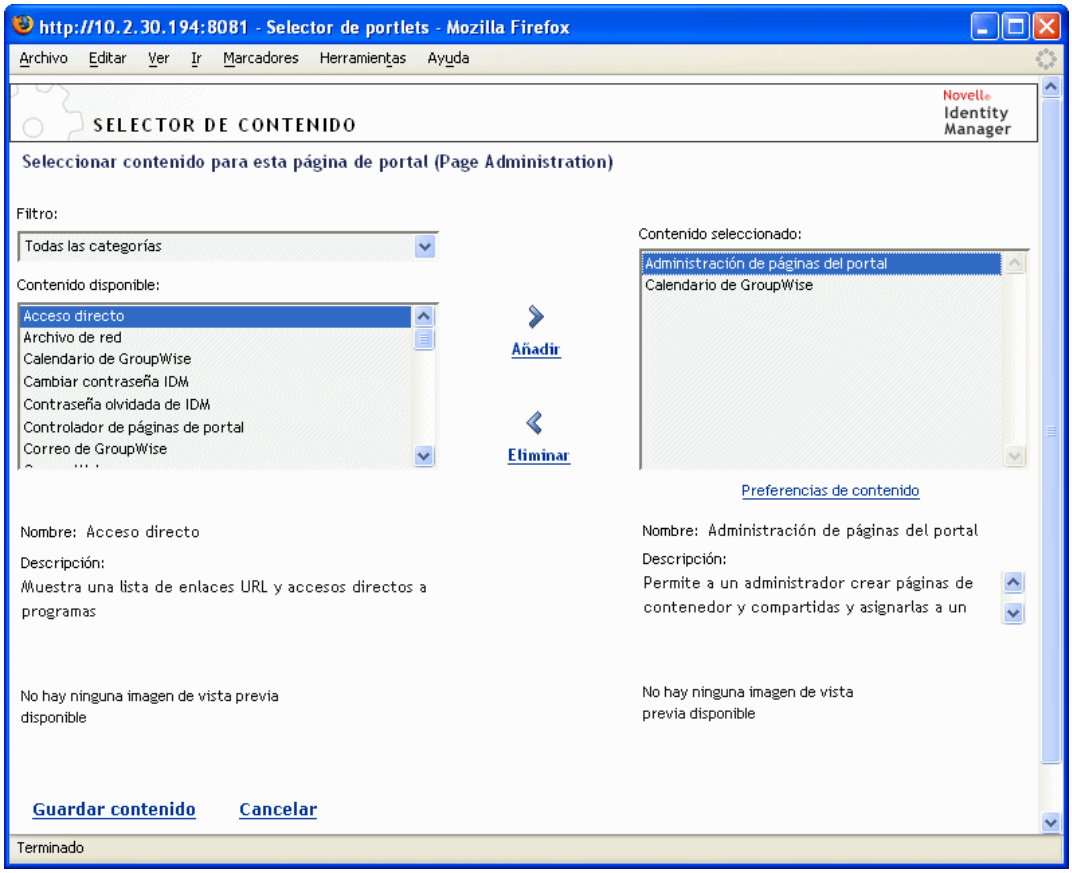
7.3.2 Adición de contenido a una página compartida

Después de crear una página compartida, el paso siguiente consiste en añadir contenido seleccionando portlets para colocarlos en la página. Puede utilizar portlets creados anteriormente con la aplicación de usuario del Gestor de identidades u otros portlets que haya registrado.

Para añadir contenido a una página compartida:

1 Abra una página nueva o ya existente en el panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Seleccionar contenido* (en la parte inferior del panel).

El *Selector de contenido* se visualizará en una ventana del navegador nueva:



2 Si desea visualizar una categoría específica del contenido disponible, seleccione la categoría en el menú desplegable *Filtro*.

3 Seleccione uno o varios portlets en la lista de *Contenido disponible*.

Sugerencia: Mantenga pulsada la tecla *Control* para seleccionar en la lista varios portlets que no sean contiguos; utilice la tecla *Mayús* para realizar varias selecciones contiguas.

4 Haga clic en *Añadir* para mover las opciones a la lista de *Contenido seleccionado*.

5 Puede hacer clic en *Preferencias de contenido* para editar las preferencias de cualquier portlet que haya seleccionado para su página compartida. Los valores de preferencia que especifique tendrán vigor para la instancia del portlet que aparezca en la página.

6 Haga clic en *Guardar contenido*.

Ahora que ha elegido el contenido de la página compartida, puede seleccionar un diseño nuevo, tal como se describe en Sección 7.3.4, “Modificación del diseño de una página compartida”, en la página 159 u ordenar el contenido del diseño actual, tal como se describe en Sección 7.3.5, “Organización del contenido de la página compartida”, en la página 160.

7.3.3 Supresión de contenido de una página compartida

En el transcurso de la creación de páginas compartidas, es posible que desee suprimir contenido eliminando portlets de una página. Puede utilizar el Selector de contenido o el Selector de diseño, tal como se describe en los procedimientos siguientes.

Para suprimir contenido de una página compartida utilizando el Selector de contenido:

1 Abra una página del panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Seleccionar contenido* (en la parte inferior del panel).

El *Selector de contenido* se visualizará en una ventana del navegador nueva (tal como se muestra en el procedimiento anterior).

2 Seleccione el portlet que desee suprimir en la lista Contenido seleccionado y haga clic en *Eliminar*.

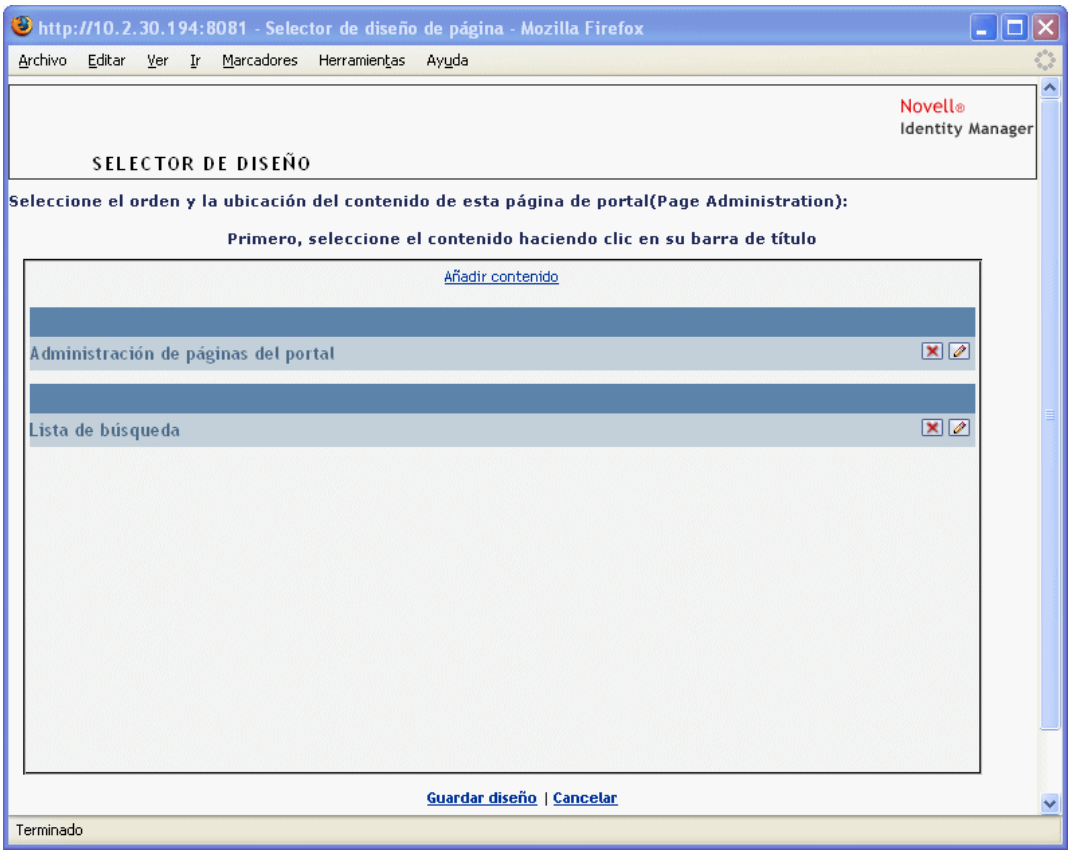
Se eliminará el portlet de la página.

3 Haga clic en *Guardar contenido*.

Para suprimir contenido de una página compartida utilizando el Selector de diseño:

1 Abra una página del panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Organizar contenido* (en la parte inferior del panel).

El *Selector de diseño* se visualizará en una ventana del navegador nueva y mostrará los portlets de dicha página:



2 Haga clic en el botón *X* en el caso de un portlet que desee eliminar.

3 Cuando el sistema le solicite una confirmación, haga clic en *Aceptar*.

Se eliminará el portlet de la página.

4 Haga clic en *Guardar diseño*.

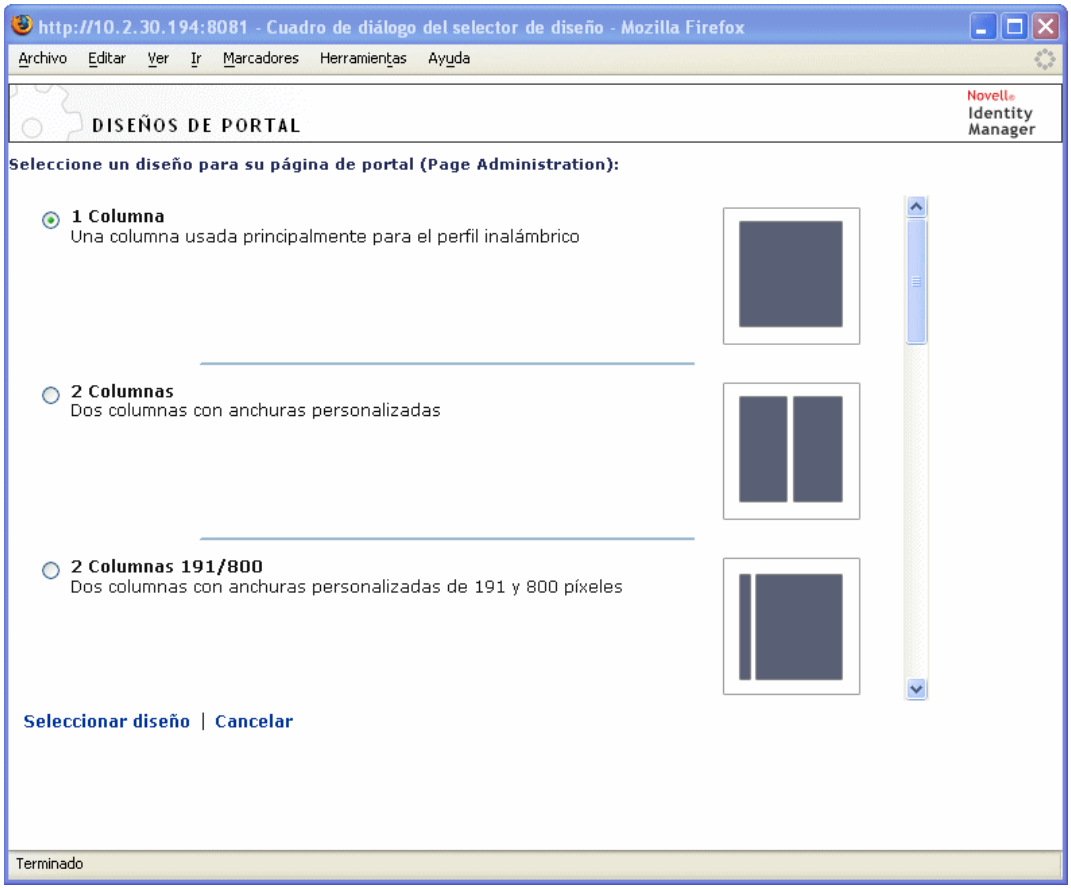
7.3.4 Modificación del diseño de una página compartida

Cuando modifique el diseño de una página compartida, el contenido existente se desplazará para acomodar el nuevo diseño. En algunos casos, es posible que deba ajustar con precisión el resultado final.

Para modificar el diseño de una página compartida:

1 Abra una página del panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Seleccionar diseño* (en la parte inferior del panel).

La lista *Diseños de portal* se visualizará en una ventana del navegador nueva:



2 *Desplácese* por las opciones y *seleccione* el diseño que desee.

3 Haga clic en *Seleccionar diseño*.

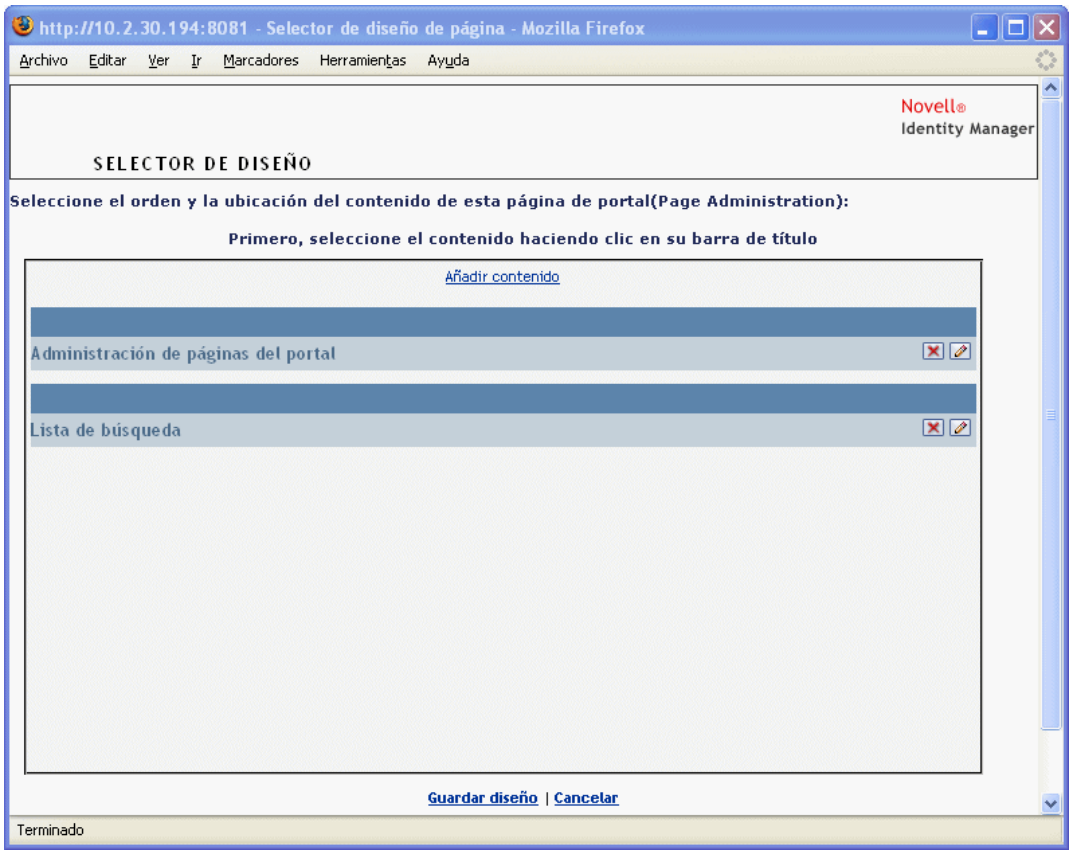
7.3.5 Organización del contenido de la página compartida

Después de decidir el contenido y diseño de la página compartida, puede colocar el contenido en el diseño seleccionado, añadir otros portlets en ubicaciones específicas o suprimir portlets.

Para organizar el contenido de una página compartida:

1 Abra una página del panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Organizar contenido* (en la parte inferior del panel).

El *Selector de diseño* se visualizará en una ventana del navegador nueva y mostrará los portlets de dicha página:



2 Si desea *añadir un portlet* a la página, ejecute los pasos siguientes:

2a Haga clic en *Añadir contenido* en la trama de diseño deseada.

El *Selector de portlet* se visualizará en una ventana del navegador nueva.

2b Si desea visualizar una categoría específica del contenido disponible, seleccione la categoría en el menú desplegable *Filtro*.

2c Seleccione el portlet que desee en la lista de *Contenido disponible*.

2d Haga clic en *Seleccionar contenido*.

El selector de portlets se cerrará y el portlet seleccionado aparecerá en la trama de diseño de destino del Selector de diseños.

3 Si desea *mover un portlet* a otra ubicación del diseño, siga los pasos siguientes específicos para el navegador:

Navegador	Operaciones que puede realizar
Internet Explorer	1. Mover el cursor sobre la barra de título del portlet hasta que el cursor cambie y se convierta en una mano. 2. Con el botón izquierdo del ratón pulsado, arrastre el portlet hasta el lugar deseado del diseño.

Navegador	Operaciones que puede realizar
Mozilla	1. Haga clic en el portlet que desee mover. 2. Haga clic dentro de la trama de diseño de destino. El portlet se moverá hasta el destino.

4 Si desea *eliminar un portlet* del diseño, ejecute los pasos siguientes:

4a Haga clic en el botón *X* del portlet que desee eliminar.

4b Cuando el sistema le solicite una confirmación, haga clic en *Aceptar*.

Se eliminará el portlet del diseño.

5 Si desea *editar las preferencias* de un portlet, ejecute los pasos siguientes:

5a Haga clic en el botón *lápiz* del portlet que desee editar.

Las *preferencias de contenido* del portlet se visualizarán en el navegador.

5b *Cambie* los valores de preferencia según sus necesidades.

Los valores de preferencia que especifique tendrán vigor para la instancia del portlet que aparezca en la página.

5c Haga clic en *Guardar preferencias*.

6 Haga clic en *Guardar diseño* para registrar los cambios y cerrar el Selector de diseños.

7.3.6 Visualización de una página compartida

Puede visualizar su página yendo a la URL de la página compartida en el navegador.

Para visualizar una página compartida:

- En el *navegador Web*, vaya a la URL siguiente:

```
http://servidor:puerto/contexto-war-IDM/portal/pg/nombre-página-compartida
```

Por ejemplo, para visualizar la página denominada *MiPáginaCompartida*:

```
http://miservidorapp:8080/IDM/portal/pg/MiPáginaCompartida
```

7.4 Asignación de permisos para las páginas

Se pueden asignar permisos a otros usuarios, grupos y contenedores para que trabajen con páginas de contenedor y páginas compartidas específicas. Se puede asignar dos niveles de seguridad de permiso:

Permiso	Descripción	Puede asignarse para
Ver	Permite a un usuario, grupo o contenedor acceder a la página y verla en una lista de páginas disponibles	**Páginas de contenedor** y **páginas compartidas**
Propiedad	Permite a un usuario, grupo o contenedor modificar el contenido y diseño de la página y asignar permiso para ver o de propiedad a otros usuarios, grupos y contenedores	**Páginas compartidas**

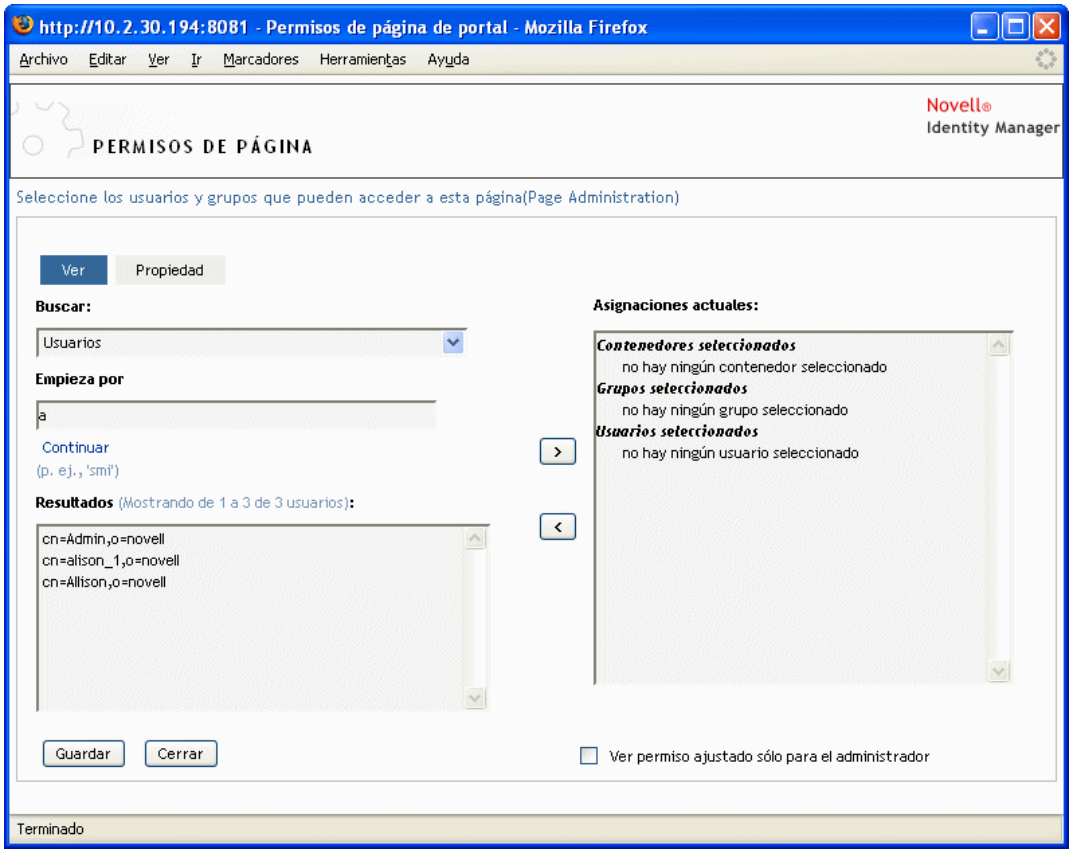
7.4.1 Asignación del permiso Ver la página

Cuando se asigna a los usuarios permiso Ver para una página de contenedor o una página compartida, los usuarios pueden acceder a la página y verla en una lista de páginas disponibles.

Para asignar el permiso Ver para páginas de contenedor o páginas compartidas:

1 Abra una página en el panel Mantenimiento de páginas de contenedor o el panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Asignar permisos* (en la parte inferior del panel).

El diálogo *Permisos de página* se visualizará en una ventana del navegador nueva:



2 Vaya a la pestaña *Ver*.

3 Especifique los *valores de búsqueda* siguientes:

Valor	Operaciones que puede realizar
Buscar	Seleccione una de las opciones siguientes en el menú desplegable: ◆ Usuarios ◆ Grupos ◆ Contenedores

Empieza por	Si desea:
	◆ **Encontrar todos** los objetos disponibles de su tipo especificado (usuario, grupo o contenedor), deje este valor en blanco.
	◆ **Encontrar un subconjunto** de los objetos, introduzca los caracteres de inicio de los valores CN. (No se distinguirá entre mayúsculas y minúsculas. No se admiten comodines).
	Por ejemplo, si busca grupos que empiezan por `S`, los resultados de la búsqueda disminuirán y obtendrá una respuesta similar a la siguiente:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Si busca grupos que empiezan por `Se` obtendrá:
	`cn=Service,ou=groups,o=MyOrg`

4 Haga clic en *Continuar*.

Los resultados de la búsqueda aparecerán en la lista *Resultados*.

5 *Seleccione* los usuarios, grupos o contenedores que desee asignar a la página y, a continuación, haga clic en el botón *Añadir* (>).

Sugerencia: Mantenga pulsada la tecla *Control* para realizar varias selecciones.

6 Habilite o inhabilite el *bloqueo de páginas* tal como se indica a continuación:

Si desea continuar	Realice la operación siguiente
Bloquear la página para que sólo los administradores de la aplicación de usuario la puedan ver.	Active **Permiso de visualización definido sólo para el administrador**
Permitir que todos los usuarios, grupos y contenedores asignados vean la página	Desactive **Permiso de visualización definido sólo para Admin** **Nota:** Si desactiva este valor, pero no hay ningún usuario, grupo o contenedor asignado explícitamente a la página, **todos tendrán permiso para ver** esta página.

7 Haga clic en *Guardar* y, a continuación, en *Cerrar*.

7.4.2 Asignación de propietarios de páginas compartidas

Los usuarios que son propietarios de páginas compartidas pueden modificar el contenido de las páginas de su propiedad y cambiar las preferencias de los portlets contenidos en dichas páginas.

Para asignar un permiso de propiedad sobre páginas compartidas:

1 Abra una página en el panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Asignar permisos* (en la parte inferior del panel).

El diálogo *Permisos de página* se visualizará en una ventana del navegador nueva (tal como se muestra en el procedimiento anterior).

2 Vaya a la pestaña *Propiedad*.

3 Especifique los *valores de búsqueda* siguientes:

Valor	Operaciones que puede realizar
Buscar	Seleccione una de las opciones siguientes en el menú desplegable: ◆ Usuarios ◆ Grupos ◆ Contenedores

Valor	Operaciones que puede realizar

Empieza por	Si desea:
	◆ **Encontrar todos** los objetos disponibles de su tipo especificado (usuario, grupo o contenedor), deje este valor en blanco.
	◆ **Encontrar un subconjunto** de los objetos, introduzca los caracteres de inicio de los valores CN. (No se distinguirá entre mayúsculas y minúsculas. No se admiten comodines).
	Por ejemplo, si busca grupos que empiezan por `S`, los resultados de la búsqueda disminuirán y obtendrá una respuesta similar a la siguiente:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Si busca grupos que empiezan por `Se` obtendrá:
	`cn=Service,ou=groups,o=MyOrg`

4 Haga clic en *Continuar*.

Los resultados de la búsqueda aparecerán en la lista *Resultados*.

5 *Seleccione* los usuarios, grupos o contenedores que desee asignar a la página y, a continuación, haga clic en el botón *Añadir* (>).

Sugerencia: Mantenga pulsada la tecla *Control* para realizar varias selecciones.

6 Habilite o inhabilite el *bloqueo de páginas* tal como se indica a continuación:

Si desea continuar	Realice la operación siguiente
Bloquear la página para que sólo los administradores de la aplicación de usuario puedan trabajar con ella.	Active **Permiso de propiedad definido sólo para el administrador**
Permitir que todos los usuarios, grupos y contenedores asignados trabajen con la página	Desactive **Permiso de propiedad definido sólo para el administrador** **Nota:** Si desactiva este valor, pero no hay ningún usuario, grupo o contenedor asignado explícitamente a la página, **todos tendrán permiso de propiedad sobre** esta página.

7 Haga clic en *Guardar* y, a continuación, en *Cerrar*.

7.4.3 Habilitación del acceso del usuario a la página Crear usuario o grupo

Por defecto, sólo los administradores de la aplicación de usuario pueden ver y utilizar la página *Crear usuario o grupo*, que es una página compartida de la *pestaña Autoservicio de identidades* de la interfaz de usuario del Gestor de identidades. No obstante, si es preciso, un administrador de la aplicación de usuario puede *asignar permisos a uno o varios usuarios* para que vean también dicha página. Por ejemplo, determinadas personas con cargos administrativos o de gestión pueden necesitar la capacidad para crear usuarios, grupos o grupos de tareas.

Para que dichos usuarios puedan acceder a la página Crear usuario o grupo:

1 En el panel *Mantenimiento de páginas compartidas*, abra la página denominada *Crear usuario o grupo*.

2 Utilice la tarea de página *Asignar permisos* para dar *permiso de visualización* a los usuarios, grupos o contenedores adecuados sobre la página compartida Crear usuario o grupo.

3 Pase de Administrador de páginas a *ADMIN de portlet* y abra el registro de portlets denominado *CreatePortlet* (que se utiliza en la página Crear usuario o grupo).

4 Utilice el panel *Seguridad* para dar a los usuarios, grupos o contenedores adecuados *permisos de Lista y Ejecución* sobre el registro de portlet CreatePortlet.

   Si desea obtener más información acerca de cómo asignar permisos para portlets, consulte el Capítulo 9, “Administración de portlets”, en la página 179.

5 Vaya a *iManager* y utilice una cuenta de administrador para *entrar en el árbol* de su repositorio seguro de identidades.

6 Asegúrese de que las personas que vayan a utilizar Crear usuario o grupo tengan *derechos de creación para la propiedad [Derechos de entrada]* en los contenedores donde se crearán los objetos (usuarios, grupos o grupos de tareas).

   Por ejemplo, puede *modificar los Trustees* de un contenedor determinado y añadir los usuarios, grupos o contenedores adecuados como Trustees. A continuación, por cada Trustee, puede asignar los derechos siguientes:

Nombre de propiedad	Derechos asignados	Heredado
[Derechos sobre todos los atributos]	◆ Comparación ◆ Lectura ◆ Escritura	Sí, (seleccionar esta casilla de verificación)
[Derechos de entrada]	◆ Examinar ◆ Crear	Sí, (seleccionar esta casilla de verificación)

   Si no asigna los derechos necesarios en el repositorio seguro de identidades (o si dichos derechos no se pueden derivar), es posible que un usuario final reciba de Crear usuario o grupo un *mensaje de error* como el siguiente:

```
El usuario 'cn=mmackenzie,ou=users,ou=idmsample,o=novell' no está
```

```
autorizado para crear
'cn=MyNewGroup,ou=groups,ou=idmsample,o=novell' o para modificar
los objetos relacionados.
```

Para saber cómo se utiliza la página Crear usuario o grupo (por aquellos que acceden a ella), consulte *Aplicación de usuario del Gestor de identidades: Guía del usuario*.

7.4.4 Habilitación del acceso del usuario a páginas de administración individuales

Por defecto, sólo los administradores de la aplicación de usuario pueden acceder a la *pestaña Administración* de la interfaz de usuario del Gestor de identidades y las *páginas* contenidas en dichas pestaña (Administrador de páginas, Temas, ADMIN de portlet, Portal, Seguridad, Registro, Almacenamiento en caché, Herramientas). No obstante, si es preciso, un administrador de la aplicación de usuario puede *asignar permisos a uno o varios usuarios* para que vean o utilicen páginas específicas de la pestaña Administración. Por ejemplo, puede darse el caso de que un pequeño grupo de usuarios necesite cambiar de temas periódicamente, aunque no sean administradores de la aplicación de usuario.

Para dar acceso a usuarios a páginas de administración individuales:

1. En el panel *Mantenimiento de páginas de contenedor*, abra *Página de contenedor ADMIN*.

   Se trata de la página de contenedor que se utiliza cuando se va a la pestaña Administración de la interfaz de usuario del Gestor de identidades.
2. Utilice la tarea de página *Asignar permisos* para dar *permiso de visualización* a los usuarios, grupos o contenedores adecuados sobre la página de contenedor ADMIN.
3. En el panel *Mantenimiento de páginas compartidas*, abra la página Administración adecuada (una de las páginas compartidas bajo la categoría *Administración*).
4. Utilice la tarea de página *Asignar permisos* para dar *permisos de visualización y propiedad* a los usuarios, grupos o contenedores adecuados para esta página compartida.
5. Asegúrese de que los usuarios, grupos o contenedores especificados tengan *permiso de ejecución por cada portlet* utilizado en una página especificada (si ha restringido dichos portlets).

   Si desea obtener más información acerca de cómo asignar permisos para portlets, consulte el Capítulo 9, “Administración de portlets”, en la página 179.

7.5 Configuración de páginas por defecto para grupos

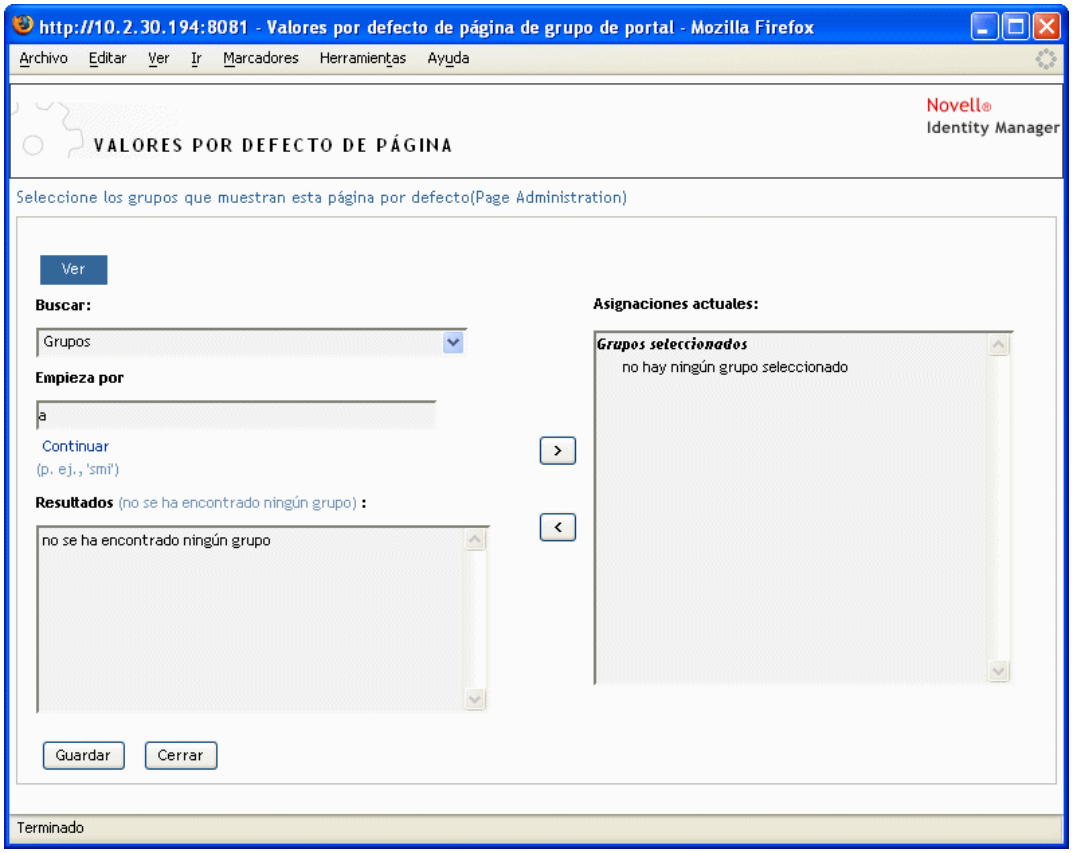
Puede asignar una *página de contenedor por defecto* y una *página compartida por defecto* a cualquier grupo de usuarios autorizado. Estos valores repercuten sobre qué página de contenedor verán dichos usuarios cuando entren y qué página compartida verán en la página de contenedor.

Si los usuarios pertenecen a varios grupos con asignaciones de páginas por defecto, se utilizará la Prioridad de navegación para determinar qué página de contenedor y qué página compartida visualizarán.

Para asignar una página de contenedor o una página compartida por defecto a un grupo:

1 Abra una página en el panel Mantenimiento de páginas de contenedor o el panel Mantenimiento de páginas compartidas y haga clic en la tarea de la página *Ajustar por defecto* (en la parte inferior del panel).

El diálogo *Valores por defecto de página* se visualizará en una ventana del navegador nueva:



2 Especifique los *valores de búsqueda* siguientes:

Valor	Operaciones que puede realizar
Buscar	(Se selecciona automáticamente **Grupos**).

Valor	Operaciones que puede realizar

Empieza por	Si desea:
	◆ **Encontrar todos** los grupos disponibles, deje este valor en blanco.
	◆ **Encontrar un subconjunto** de los grupos, introduzca los caracteres de inicio de los valores CN. (No se distinguirá entre mayúsculas y minúsculas. No se admiten comodines).
	Por ejemplo, si busca grupos que empiezan por `S`, los resultados de la búsqueda disminuirán y obtendrá una respuesta similar a la siguiente:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Si busca grupos que empiezan por `Se` obtendrá:
	`cn=Service,ou=groups,o=MyOrg`

3. Haga clic en *Continuar*.

   Los resultados de la búsqueda aparecerán en la lista *Resultados*.

4. *Seleccione* los grupos para los que esta página será un valor por defecto y, a continuación, haga clic en el botón *Añadir* (>).

   Sugerencia: Mantenga pulsada la tecla *Control* para realizar varias selecciones.

5. Haga clic en *Guardar* y, a continuación, en *Cerrar*.

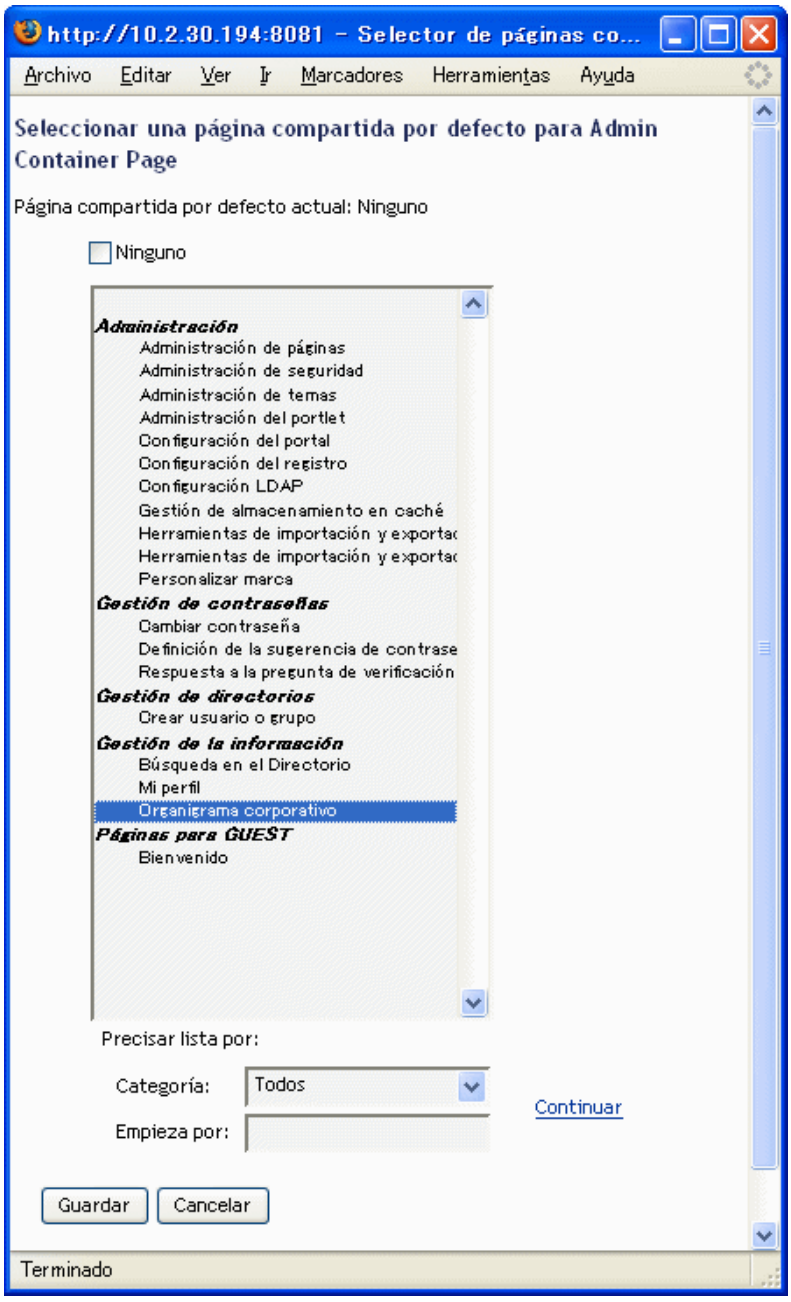
7.6 Selección de una página compartida por defecto para una página de contenedor

Puede asignar una página compartida por defecto a cada una de las páginas de contenedor que tenga. La interfaz de usuario tendrá en cuenta esta asignación de página al determinar qué se visualizará.

Para asignar una página compartida por defecto a una página de contenedor:

1. Abra una página de contenedor en el panel *Mantener páginas de contenedor*.
2. En la sección de propiedades de la página, busque *Página compartida por defecto* y haga clic en *Seleccionar por defecto*.

El diálogo para *seleccionar una página compartida por defecto* se visualizará en una ventana del navegador nueva:



3 Si la lista de páginas compartidas es larga, puede *precisarla* (por categoría o texto de inicio) para encontrar más fácilmente la página deseada.

4 *Seleccione* una página compartida para utilizarla como valor por defecto de la página de contenedor (o active *Ninguno* si no desea valor por defecto).

5 Haga clic en *Guardar* para aceptar la selección y cerrar el diálogo.

6 Haga clic en *Guardar página* (en la parte inferior de la sección de propiedades de la página).

Configuración de temas

8

En este capítulo se describe cómo utilizar la página *Temas* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general sobre cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

8.1 Acerca de la configuración de temas

Puede utilizar la página Temas para controlar el aspecto y funcionamiento de la interfaz de usuario del Gestor de identidades.

Un *tema* es un conjunto de características visuales que se aplican a toda la interfaz de usuario (incluidas las páginas de invitados y de registro, la pestaña Autoservicio de identidades, la pestaña Peticiones y aprobaciones y la pestaña Administración). Siempre hay un tema en efecto para la interfaz de usuario. La página Temas brinda la posibilidad de elegir entre varios temas, en caso de que desee cambiar a otro.

La página Temas también permite:

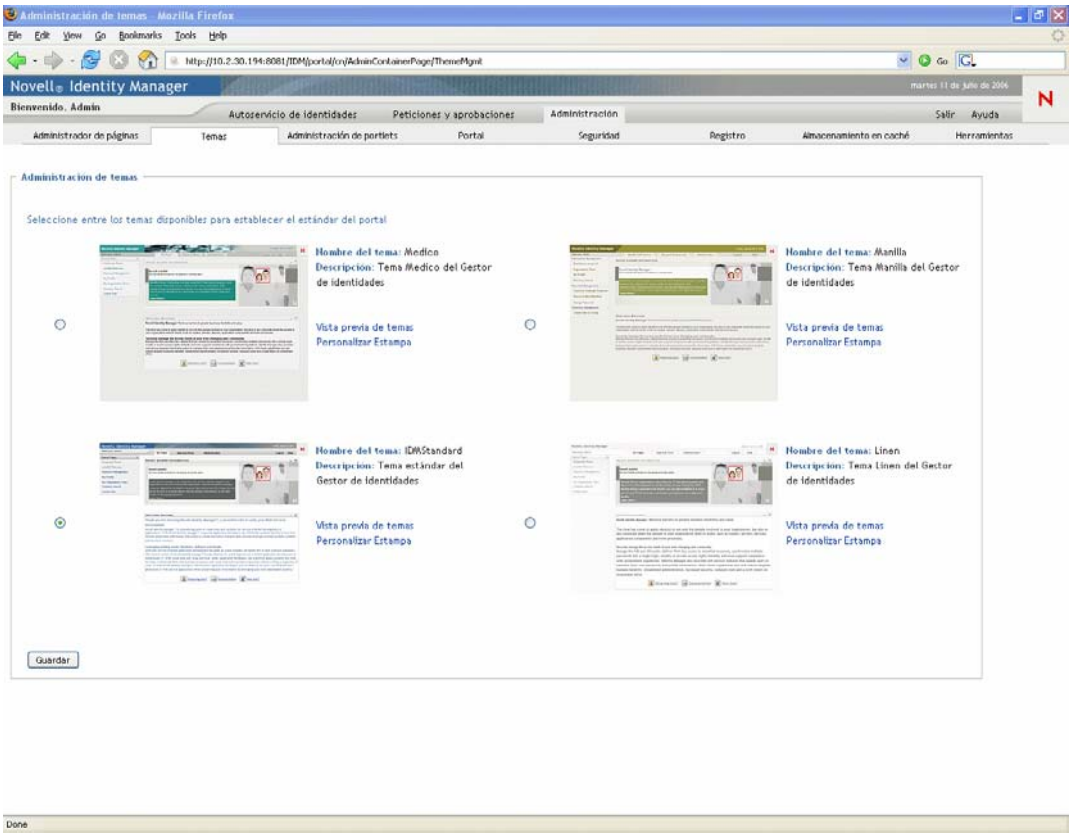
- *Obtener una vista previa* de cada opción de tema para ver qué aspecto tiene
- *Personalizar* cualquier opción de tema para que refleje su propia marca (logotipo, etc.)

8.2 Visualización previa de un tema

Antes de seleccionar un tema, puede obtener una vista previa de cómo cambiará la apariencia de la interfaz de usuario del Gestor de identidades.

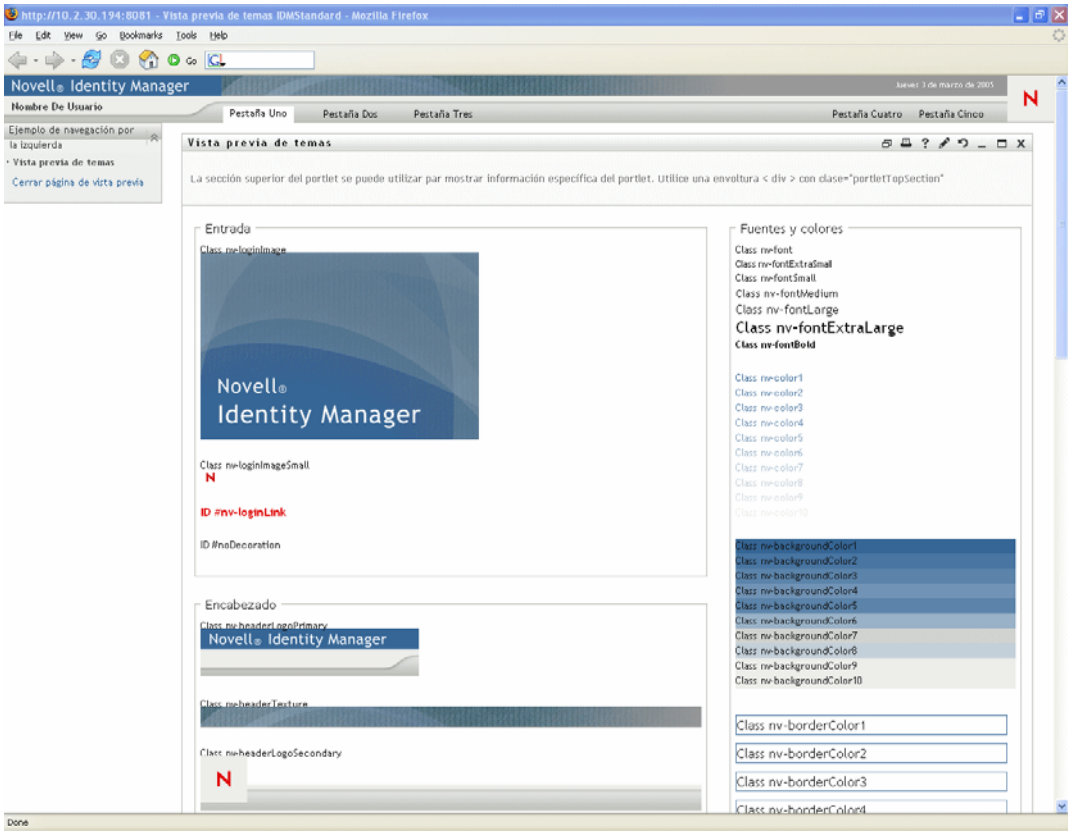
Para obtener una vista previa de un tema:

1 Vaya a la página *Temas*:



2 Encuentre un tema que le interese y haga clic en el enlace *Vista previa de temas*.

La vista previa del tema se visualizará en una ventana del navegador nueva:



3 *Desplácese* por la vista previa para ver las características de este tema.

4 Cuando haya acabado, haga clic en *Cerrar página de vista previa* (en la esquina superior izquierda) o cierre la ventana de vista previa manualmente.

8.3 Selección de un tema

Cuando encuentre un tema que le guste, puede convertirlo en el *tema actual* de la interfaz de usuario del Gestor de identidades.

Para seleccionar un tema:

1 Vaya a la página *Temas*.

2 Haga clic en el *botón circular* del tema que desee.

3 Haga clic en el botón *Guardar*.

El aspecto de la interfaz de usuario cambiará para reflejar el tema deseado.

8.4 Personalización de la marca de un tema

Puede adaptar cualquier tema sustituyéndolo por sus propias *imágenes* y cambiando algunos *valores de color*. Esto le permitirá dar a la interfaz de usuario del Gestor de identidades un aspecto personalizado para que cumpla los requisitos de marca de su compañía u organización.

Para personalizar la marca de un tema:

1. Vaya a la página *Temas*.
2. Encuentre un tema que desee personalizar y haga clic en el enlace *Personalizar marca*.

   La página Temas visualizará la configuración de Personalizar marca para el tema:

3 Especifique *sus personalizaciones* en estos valores (según sus necesidades), incluidos:

- Las imágenes de encabezado
- Los colores del área de navegación
- Las imágenes de entrada

Siga las instrucciones que aparezcan en pantalla para especificar cada valor.

4 Haga clic en el botón *Guardar*.

Si está editando el tema actual, el aspecto de la interfaz de usuario cambiará para reflejar las personalizaciones. (Si desea deshacer todas las personalizaciones del tema, haga clic en el botón *Reajustar*).

Nota: El botón *Vista previa de temas* estará disponible mientras realice las personalizaciones; no obstante, tenga en cuenta que siempre muestra las *características originales* del tema y no mostrará los cambios.

---

5 Cuando haya acabado de trabajar en este tema, haga clic en el botón *Volver al Selector de temas*.

Administración de portlets

9

En este capítulo se describe cómo utilizar la página *ADMIN de portlet* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general sobre cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

9.1 Acerca de la administración de portlets

Puede utilizar la página ADMIN de portlet para controlar los *portlets* disponibles en la interfaz de usuario del Gestor de identidades y quién tiene permiso para acceder a ellos. Los portlets son elementos conectables de la interfaz de usuario (basados en un *estándar de Java*) que proporcionan el contenido de las páginas de la interfaz de usuario (incluidas las páginas de contenedor y las páginas compartidas).

La gestión de portlets implica trabajar con:

Con qué se trabaja	Descripción
Aplicaciones de portlet	WAR compatibles con Java Portlet 1.0 que contienen el descriptor de implantación del portlet portlet.xml y, opcionalmente, otros artefactos de tiempo de ejecución de portlet. Consulte Sección 9.2, “Administración de aplicaciones de portlet”, en la página 180.
Definiciones de portlet	Descriptores (leídos en portlet.xml) que especifican parámetros de configuración del portlet. Existe una definición por cada portlet de una aplicación. Consulte Sección 9.3, “Administración de definiciones de portlet”, en la página 183.
Registros de portlets	Registros de portlets, basados en sus definiciones. Pueden existir múltiples registros del mismo portlet en una única aplicación de portlet. Consulte Sección 9.4, “Administración de portlets registrados”, en la página 187.

Para obtener información acerca de los portlets suministrados con la interfaz de usuario del Gestor de identidades, consulte Parte IV, “Referencia de portlet”, en la página 237. Para obtener información acerca de cómo utilizar portlets en las páginas de contenedor y las páginas compartidas, consulte Capítulo 7, “Administración de páginas”, en la página 135.

9.2 Administración de aplicaciones de portlet

Cuando se instala la aplicación de usuario del Gestor de identidades, *IDM.war* se implanta en el servidor de aplicación y se registra automáticamente como aplicación de portlet. IDM.war (cuyo nombre se puede cambiar durante la instalación) incluye todos los portlets utilizados en la configuración por defecto de la interfaz de usuario del Gestor de identidades. También incluye algunos portlets adicionales que no se utilizan por defecto. (Los portlets IDM.war están descritos en Parte IV, “Referencia de portlet”, en la página 237).

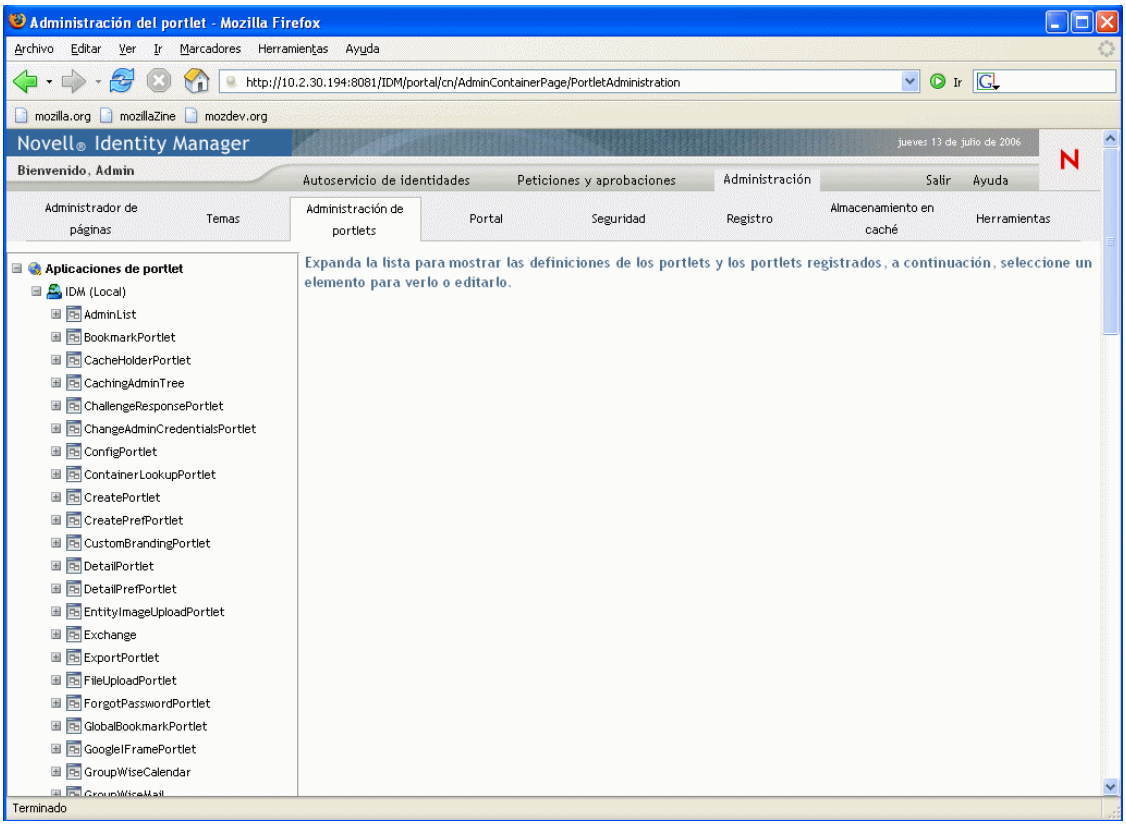
No obstante, no es preciso limitarse a utilizar los portlet de IDM.war. Si implanta cualquier otra *aplicación de portlet estándar* (WAR compatible con Java Portlet 1.0) en el servidor de aplicación, podrá trabajar con esas aplicaciones de portlet y sus portlets en la interfaz de usuario del Gestor de identidades. Por ejemplo, verá dichas aplicaciones de portlet enumeradas junto con los archivos IDM.war en la página ADMIN de portlet.

La página ADMIN de portlet le permite *administrar IDM.war y otras aplicaciones de portlet* de las formas siguientes:

9.2.1 Acceso a las aplicaciones de portlet del servidor

Cuando se va a la página ADMIN de portlet, ésta muestra automáticamente una *lista* de las aplicaciones de portlet (IDM.war y otras) que se implantan en el servidor de aplicación. Esta lista

aparece a la izquierda como un árbol que se puede *expandir y en el que se puede navegar* para administrar una aplicación de portlet seleccionada y su contenido:



9.2.2 Visualización de información acerca de aplicaciones de portlet

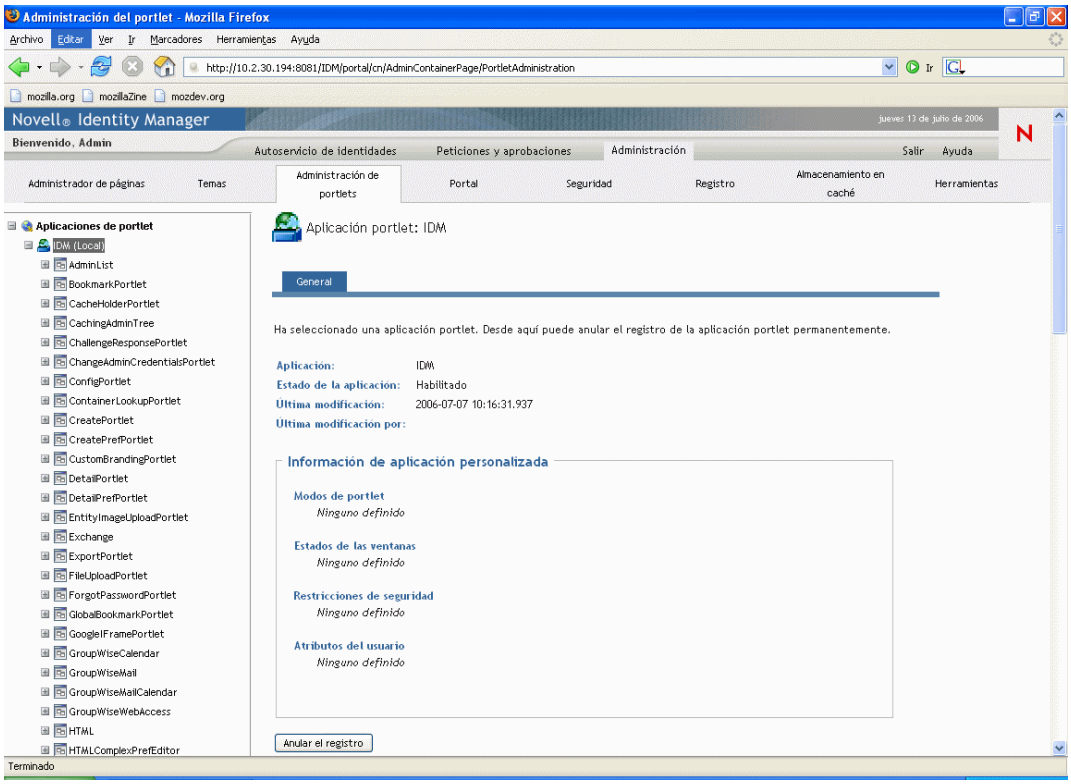
Puede ver la siguiente información de sólo lectura acerca de una aplicación de portlets de la lista:

- Nombre
- Estado (habilitada o inhabilitada)
- Fecha de la última modificación
- Usuario que modificó por última vez la aplicación
- Información de la aplicación personalizada (si la hay): modos de portlet, estados de ventanas, restricciones de seguridad y atributos de usuario

Para ver información acerca de una aplicación de portlet:

- En la lista Aplicaciones de portlet, *seleccione* la aplicación de portlet sobre la que desea informarse.

Se visualizará un panel *General* a la derecha, mostrando información acerca de la aplicación de portlet seleccionada:



9.2.3 Anulación del registro de aplicaciones de portlet

Cuando desee eliminar una aplicación de portlet del servidor de aplicación, deberá *anular el registro* de dicha aplicación antes de anular la implantación. De lo contrario, la aplicación de portlet se volverá a implantar automáticamente cuando el servidor se reinicie.

Cuando anule el registro de una aplicación de portlet, todas las preferencias y valores relacionados se eliminarán de la base de datos que almacena los datos de la aplicación.

Nota: No se puede anular el registro del contenedor de portlets *local*, que es una aplicación de portlet local para el portal. El contenedor de portlets local gestiona portlets contenidos dentro del portal (aplicación de usuario del Gestor de identidades).

Para anular el registro de una aplicación de portlet:

1. En la lista Aplicaciones de portlet, *seleccione* la aplicación de portlet cuyo registro desea anular.

   Se visualizará un panel *General* a la derecha (tal como se muestra en el procedimiento anterior).

2. Haga clic en *Anular el registro*.

   Aparecerá una ventana de confirmación.

3 Haga clic en *Aceptar* para confirmar la acción.

   Cuado el proceso se complete, la aplicación de portlet cuyo registro se ha anulado se eliminará de la lista Aplicaciones de portlet.

4 Para eliminar la aplicación de portlet del servidor de aplicación, utilice las herramientas del servidor para *anular la implantación del archivo de reserva* que contiene la aplicación de portlet.

Nota: Para volver a registrar una aplicación de portlet cuyo registro se ha anulado, deberá *volver a implantarla*.

9.3 Administración de definiciones de portlet

La página ADMIN de portlet le permite efectuar las tareas siguientes relacionadas con las *definiciones de portlet* de una aplicación de portlet:

- Sección 9.3.1, “Acceso a las definiciones de portlet de la aplicación de portlet implantada”, en la página 183
- Sección 9.3.2, “Registro de definiciones de portlet”, en la página 184
- Sección 9.3.3, “Visualización de información acerca de definiciones de portlet”, en la página 185

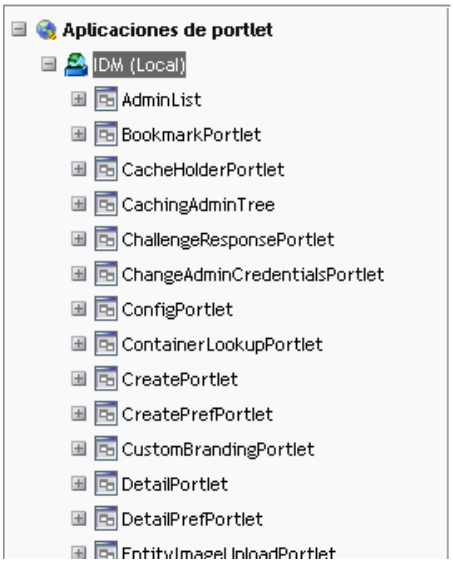
9.3.1 Acceso a las definiciones de portlet de la aplicación de portlet implantada

La lista Aplicaciones de portlet muestra las definiciones de portlet de una aplicación de portlet seleccionada.

Para acceder a las definiciones de portlet de la aplicación de portlet implantada:

- En la lista Aplicaciones de portlet, *expanda* la aplicación de portlet a cuyas definiciones de portlet desea acceder.

El árbol muestra todas las definiciones de portlet bajo dicha aplicación de portlet:



9.3.2 Registro de definiciones de portlet

Para poder utilizar un portlet, es preciso registrar la definición de dicho portlet en el portal (aplicación de usuario del Gestor de identidades). Una definición de portlet registrada se denomina *registro de portlet*. Se pueden crear varios registros de un único portlet, lo que permite poner varias instancias de dicho portlet en la misma página.

El registro de portlet hereda todas las *preferencias y valores* de la clase de portlet, aunque dichos valores se pueden modificar de las siguientes formas:

- *Al registrar* la definición del portlet (consulte Sección 9.4, “Administración de portlets registrados”, en la página 187)
- *Al añadir una instancia* del portlet a una página (Capítulo 7, “Administración de páginas”, en la página 135)

Todos los portlets que se entregan con la aplicación de usuario del Gestor de identidades se *registran automáticamente*.

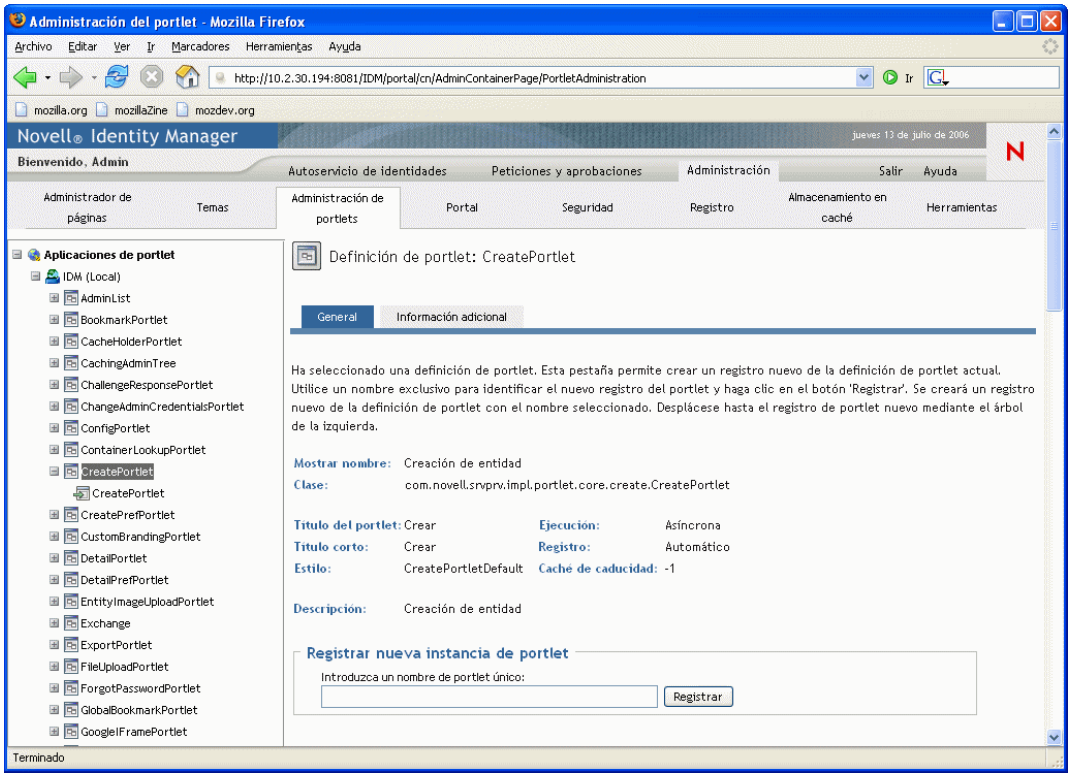
Modo de edición Si la definición del portlet proporciona un modo de edición, el usuario final puede modificar las preferencias específicas del registro de portlet en el tiempo de ejecución, según la lógica del método doEdit() del portlet.

La aplicación de usuario del Gestor de identidades también proporciona una implementación por defecto del modo de edición. Si el método doEdit() no se implementa explícitamente, se visualizará una hoja de preferencias por defecto.

Para registrar una definición de portlet:

1. En la lista Aplicaciones de portlet, *seleccione* la definición de portlet para la que desea crear un registro de portlet.

Se visualizará un panel *General* a la derecha:



Recuerde que todos los *registros existentes* del portlet seleccionado están listados en el árbol Aplicaciones de portlet (a la izquierda), bajo el nombre de la definición de portlet correspondiente.

2 En el cuadro de texto *Registrar nueva instancia de portlet*, escriba un nombre único para el registro de portlet y haga clic en *Registrar*.

El nuevo registro de portlet se creará y aparecerá listado en el árbol Aplicaciones de portlet.

3 Si desea modificar las preferencias y valores del nuevo registro de portlet, consulte Sección 9.4, “Administración de portlets registrados”, en la página 187.

9.3.3 Visualización de información acerca de definiciones de portlet

Puede ver la siguiente información de sólo lectura acerca de una definición de portlet de la lista:

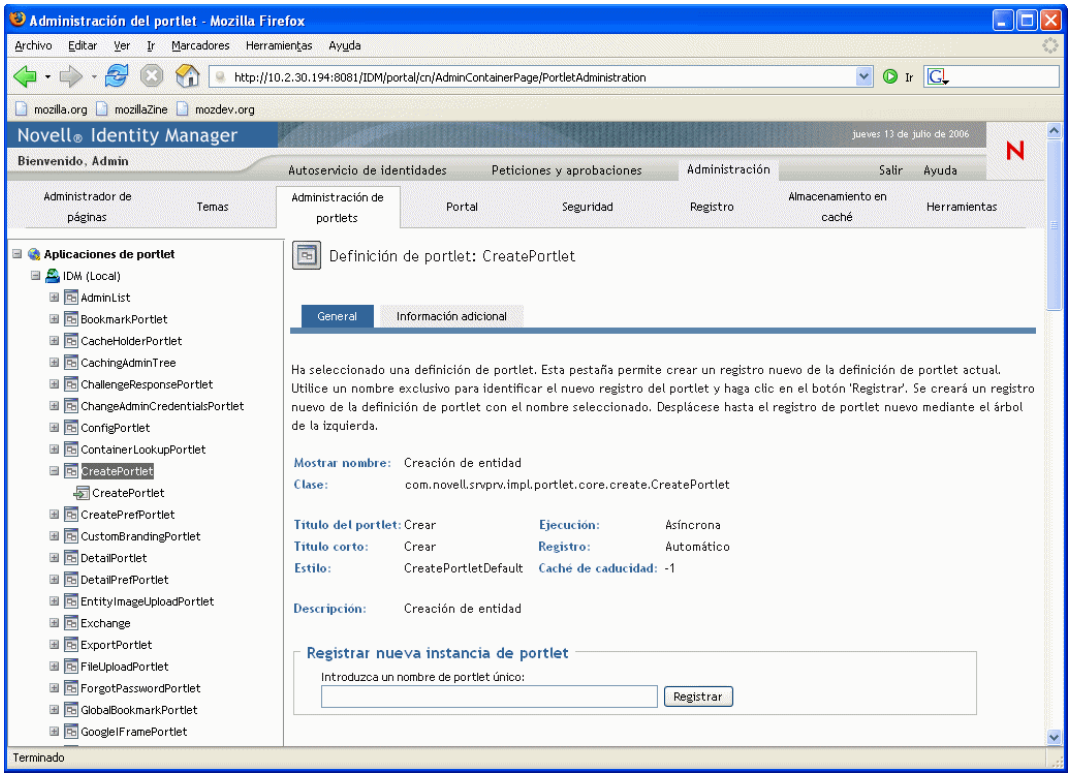
- Nombre de visualización
- Nombre de clase
- Título del portlet
- Tipo de ejecución (síncrona o asíncrona)
- Título corto
- Tipo de registro
- Estilo

- Hora de caducidad del caché
- Descripción
- Parámetros de inicialización
- Palabras clave
- Tipos MIME admitidos
- Modos admitidos por el portlet
- Configuraciones regionales admitidas
- Dispositivos admitidos
- Funciones de seguridad

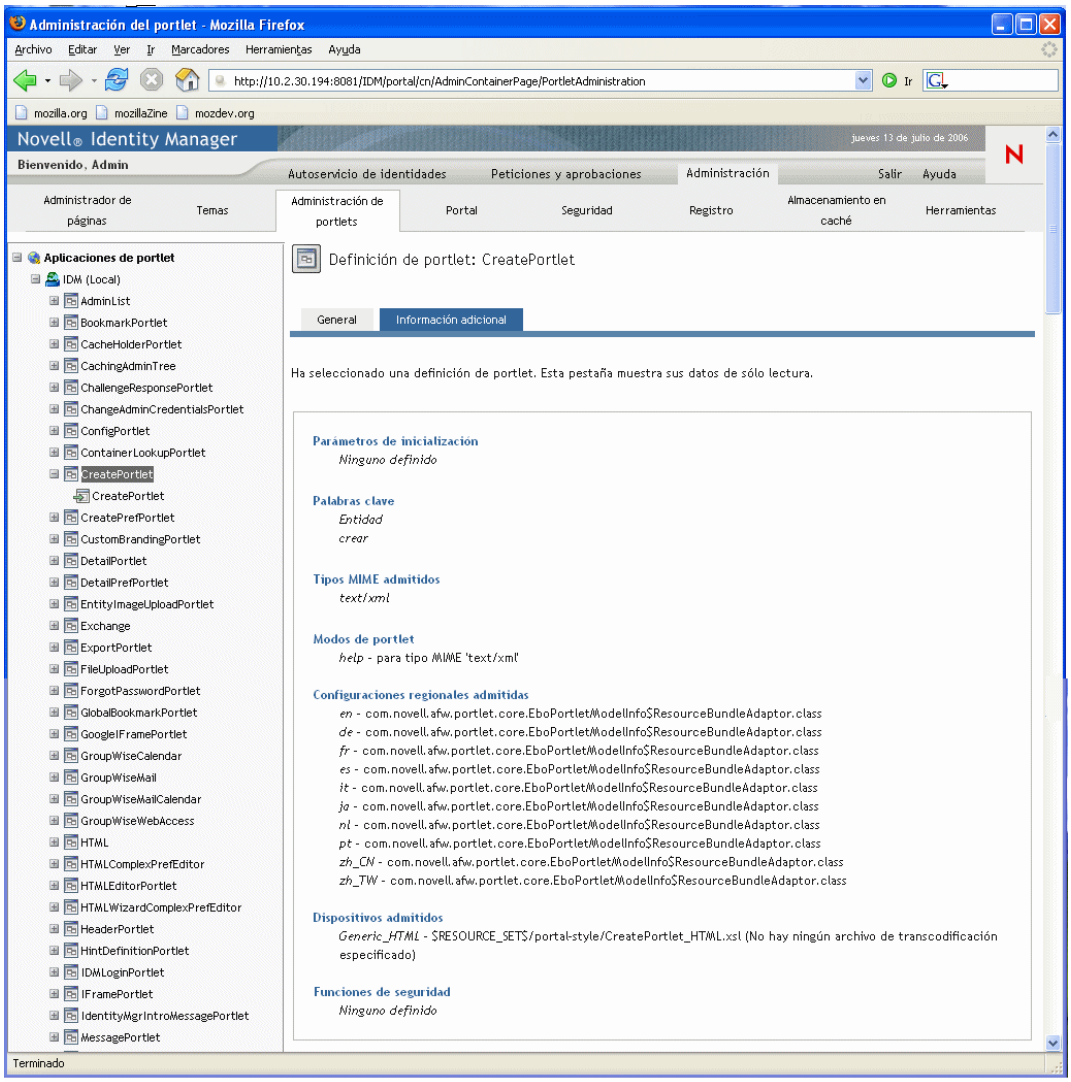
Para ver información acerca de definiciones de portlet:

1 En la lista Aplicaciones de portlet, *seleccione* la definición de portlet sobre la que desea informarse.

Se visualizará un panel *General* a la derecha, mostrando información acerca de la definición de portlet seleccionada:



2 Vaya al panel *Información adicional* para ver más información acerca de la definición del portlet seleccionado:



9.4 Administración de portlets registrados

La página ADMIN de portlet le permite efectuar las tareas siguientes relacionadas con los *registros de portlets* de una aplicación de portlet:

- Sección 9.4.1, “Acceso a los registros de portlets de la aplicación de portlet implantada”, en la página 188
- Sección 9.4.2, “Visualización de información acerca de registros de portlets”, en la página 189

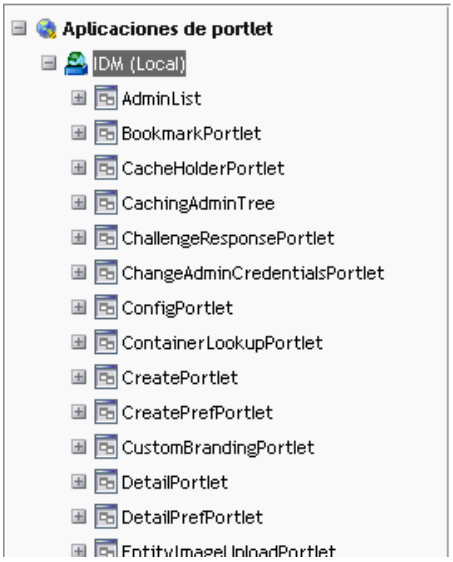
9.4.1 Acceso a los registros de portlets de la aplicación de portlet implantada

La lista Aplicaciones de portlet muestra los registros de portlet de cada definición de portlet de una aplicación de portlet seleccionada.

Para acceder a los registros de portlets de la aplicación de portlet implantada:

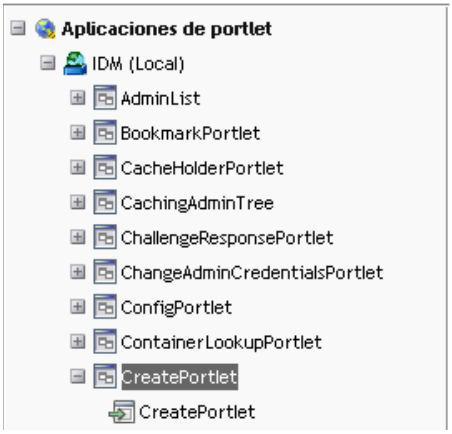
1 En la lista Aplicaciones de portlet, *expanda* la aplicación de portlet a cuyas definiciones y registros de portlets desea acceder.

El árbol muestra todas las definiciones de portlets bajo dicha aplicación de portlet:



2 *Expanda la definición de portlet* a cuyos registros de portlet desee acceder.

El árbol muestra todos los registros de portlets bajo dicha definición de portlet:



9.4.2 Visualización de información acerca de registros de portlets

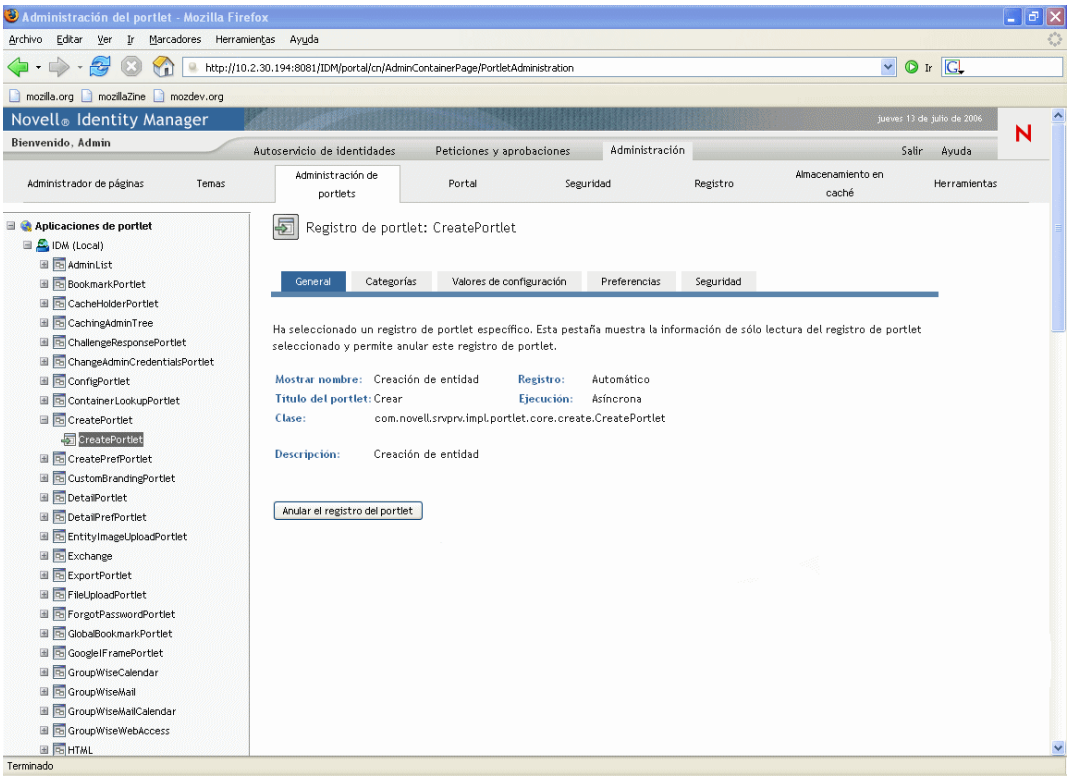
Puede ver la siguiente información de sólo lectura acerca de un registro de portlet de la lista:

- Nombre de visualización
- Tipo de registro
- Título del portlet
- Tipo de ejecución (síncrona o asíncrona)
- Nombre de clase
- Descripción

Para ver información acerca de registros de portlets:

- En la lista Aplicaciones de portlet, *seleccione* el registro de portlet sobre el que desea informarse.

Se visualizará un panel *General* a la derecha, mostrando información acerca del registro de portlet seleccionado:



9.4.3 Asignación de categorías a registros de portlet

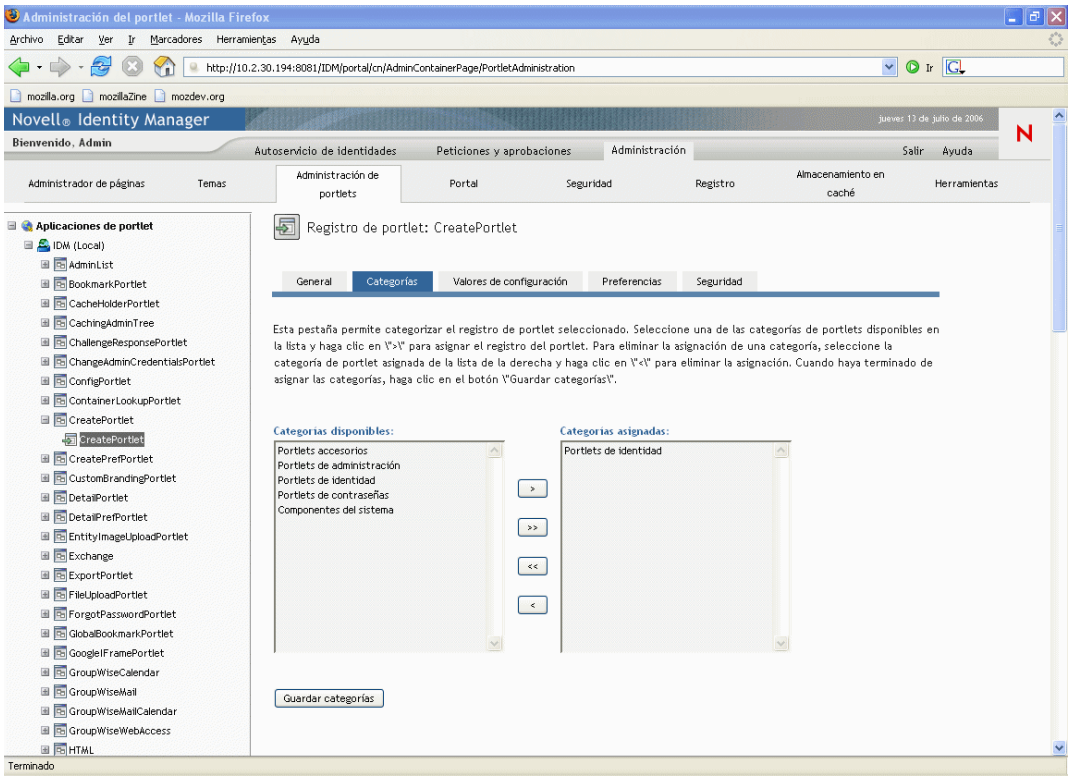
Para facilitar la búsqueda de portlets específicos en una aplicación de portlet, puede organizar los registros de portlets por categoría.

Para asignar categorías a registros de portlet:

1. En la lista Aplicaciones de portlet, *seleccione* el registro de portlet al que desea asignar una categoría.

   Se visualizará un panel *General* a la derecha.
2. Vaya al panel *Categorías*.

Este panel muestra listas de categorías disponibles y asignadas para el registro de portlet seleccionado:



3 Actualice la lista *Categorías asignadas*, según sus necesidades:

Si desea	Realice la operación siguiente
Asignar una o varias categorías al registro de portlet	Seleccione todas las categorías que desee asignar y haga clic en >
Asignar todas las categorías al registro de portlet	Haga clic en >>
Eliminar una o varias asignaciones de categoría	Seleccione todas las categorías que desee eliminar y haga clic en <
Eliminar todas las asignaciones de categoría	Haga clic en <<

4 Haga clic en *Guardar categorías*.

9.4.4 Modificación de los valores de los registros de portlet

Los valores de portlet definen cómo el portal (la aplicación de usuario del Gestor de identidades) interactúa con portlets individuales. Cada portlet se configura con los valores siguientes:

- Título
- Tiempo límite máximo

- Requiere autenticación
- Visualizar barra de título
- Oculto para el usuario
- Opciones definidas en la aplicación de portlet

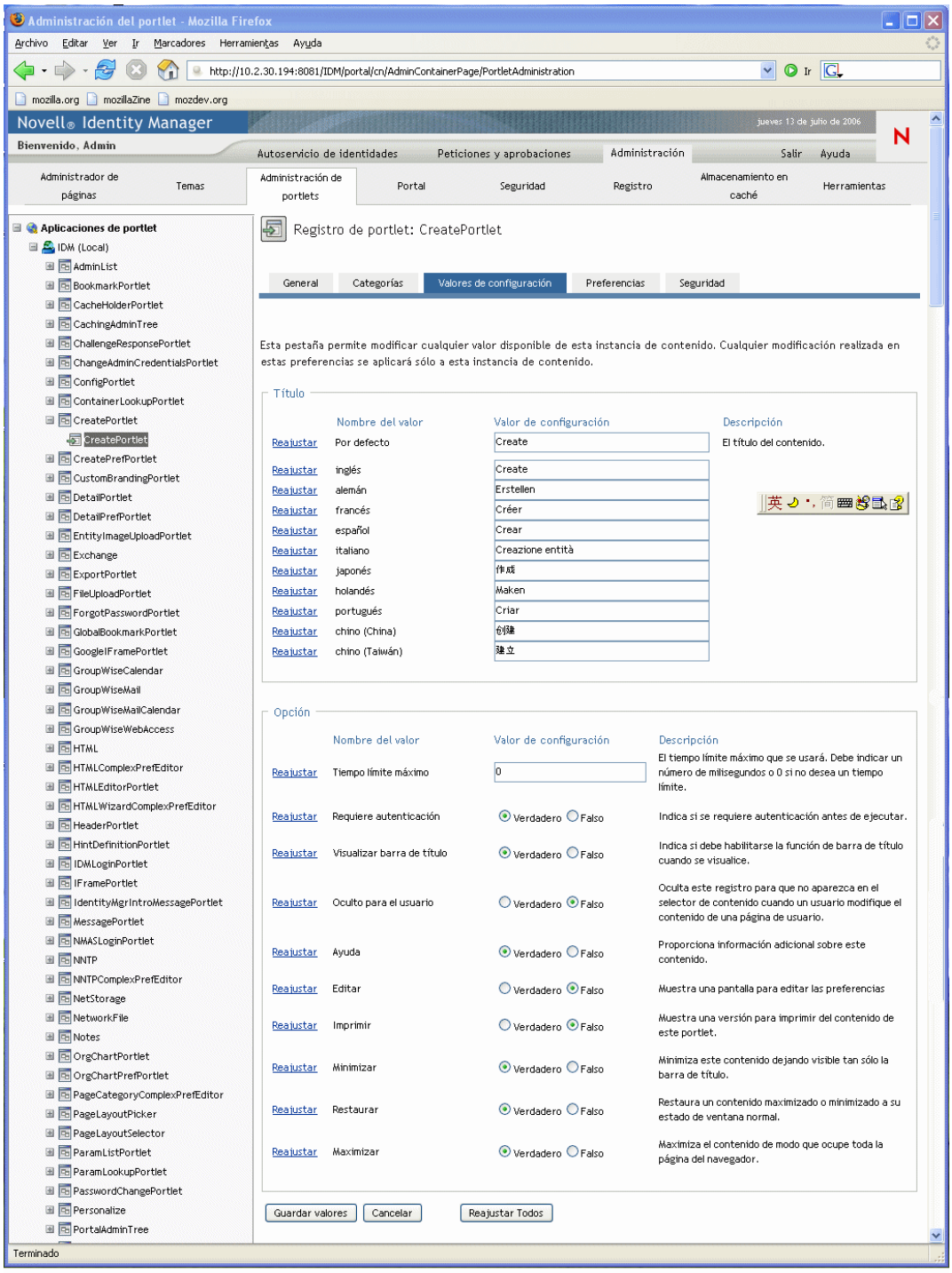
Los valores estándar de Java Portlet 1.0 están definidos en el descriptor de la implantación de portlet (portlet.xml) del WAR de la aplicación de portlet. Estos valores se pueden cambiar, registro a registro, mediante la página ADMIN de portlet. En este caso, los valores nuevos entrarán en vigor sólo para el registro de portlet seleccionado.

Para modificar los valores de un registro de portlet:

1. En la lista Aplicaciones de portlet, *seleccione* el registro de portlet cuyos valores desee modificar.

   Se visualizará un panel *General* a la derecha.
2. Vaya al panel *Valores de configuración*.

Este panel muestra los valores actuales del registro de portlet seleccionado:



3 *Modifique* los valores según sus necesidades.

Mientras trabaja en este panel, también puede ejecutar las acciones siguientes:

Si desea	Realice la operación siguiente
Descartar los cambios que no ha guardado	Haga clic en **Cancelar**
Que todos los valores de este registro de portlet recuperen sus valores por defecto (tal como están definidos en la definición de portlet correspondiente)	Haga clic en **Restaurar todos**
Que un valor individual recupere su valor por defecto	Haga clic en el enlace **Reajustar** situado al lado del valor

4 Haga clic en *Guardar valores*.

9.4.5 Modificación de las preferencias de los registros de portlet

El desarrollador del portlet define las preferencias en el momento del diseño, en el descriptor de implantación de portlet. Las preferencias pueden variar de portlet a portlet, según la implementación del desarrollador del portlet.

Los valores de las preferencias se pueden cambiar, registro a registro, mediante la página ADMIN de portlet. En este caso, los valores nuevos entrarán en vigor sólo para el registro de portlet seleccionado.

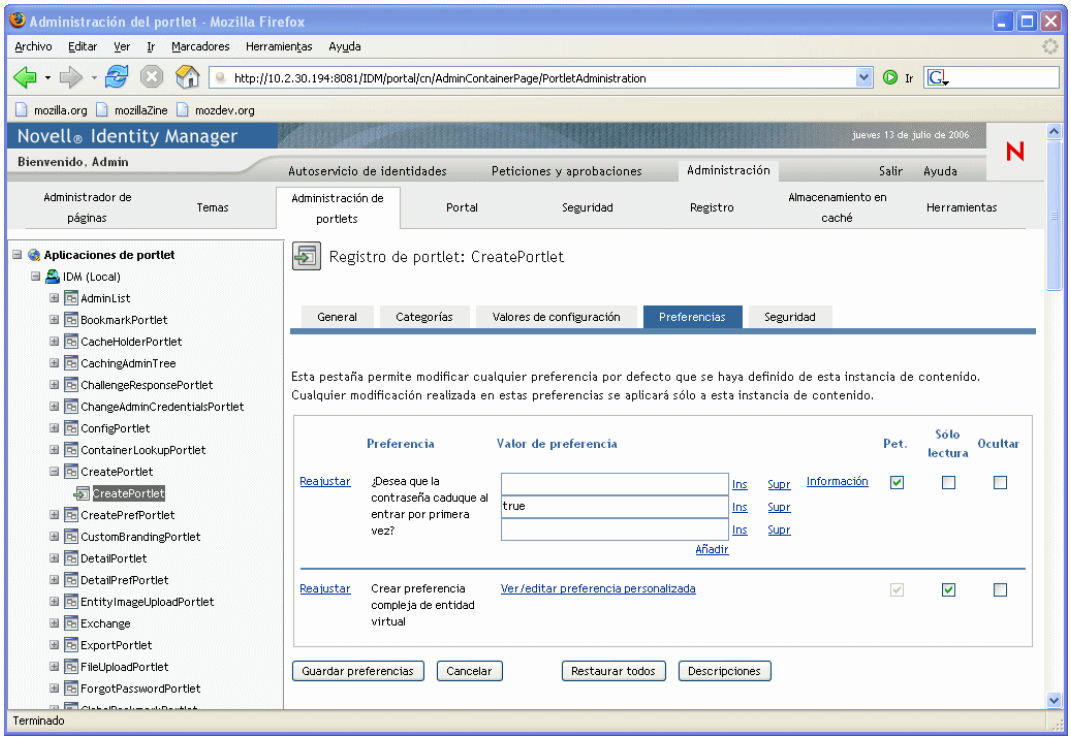
Para modificar las preferencias de registro de portlet:

1 En la lista Aplicaciones de portlet, *seleccione* el registro de portlet cuyas preferencias desee modificar.

Se visualizará un panel *General* a la derecha.

2 Vaya al panel *Preferencias*.

Este panel muestra las preferencias actuales del registro de portlet seleccionado:



3 *Modifique* las preferencias según sus necesidades.

Mientras trabaja en este panel, también puede ejecutar las acciones siguientes:

Si desea	Realice la operación siguiente
Visualizar más información acerca de las preferencias	Haga clic en **Descripciones**
Descartar los cambios que no ha guardado	Haga clic en **Cancelar**
Que todas las preferencias de este registro de portlet recuperen sus valores por defecto (tal como están dichos valores definidos en la definición de portlet correspondiente)	Haga clic en **Restaurar todos**
Que una preferencia individual recupere su valor por defecto	Haga clic en el enlace **Reajustar** situado al lado de la preferencia

4 Para modificar la *versión localizada* de una preferencia por cada configuración regional especificada en la definición de portlet, ejecute los pasos siguientes:

4a Haga clic en el enlace *Detalle* situado al lado de la preferencia (si está disponible).

El panel muestra los valores de preferencia de cada configuración regional.

4b *Modifique* los valores según sus necesidades.

4c Haga clic en *Aceptar* para aplicar los cambios y regresar a la lista de preferencias principal.

5 Haga clic en *Guardar preferencias*.

9.4.6 Asignación de permisos de seguridad para registros de portlet

Se pueden asignar los permisos de seguridad siguientes a usuarios, grupos y contenedores para los registros de portlet:

Permiso	Descripción
Lista	Los usuarios pueden **ver** el registro de portlet en una lista de selección
Ejecutar	Los usuarios pueden **ejecutar** el registro de portlet en una página del portal

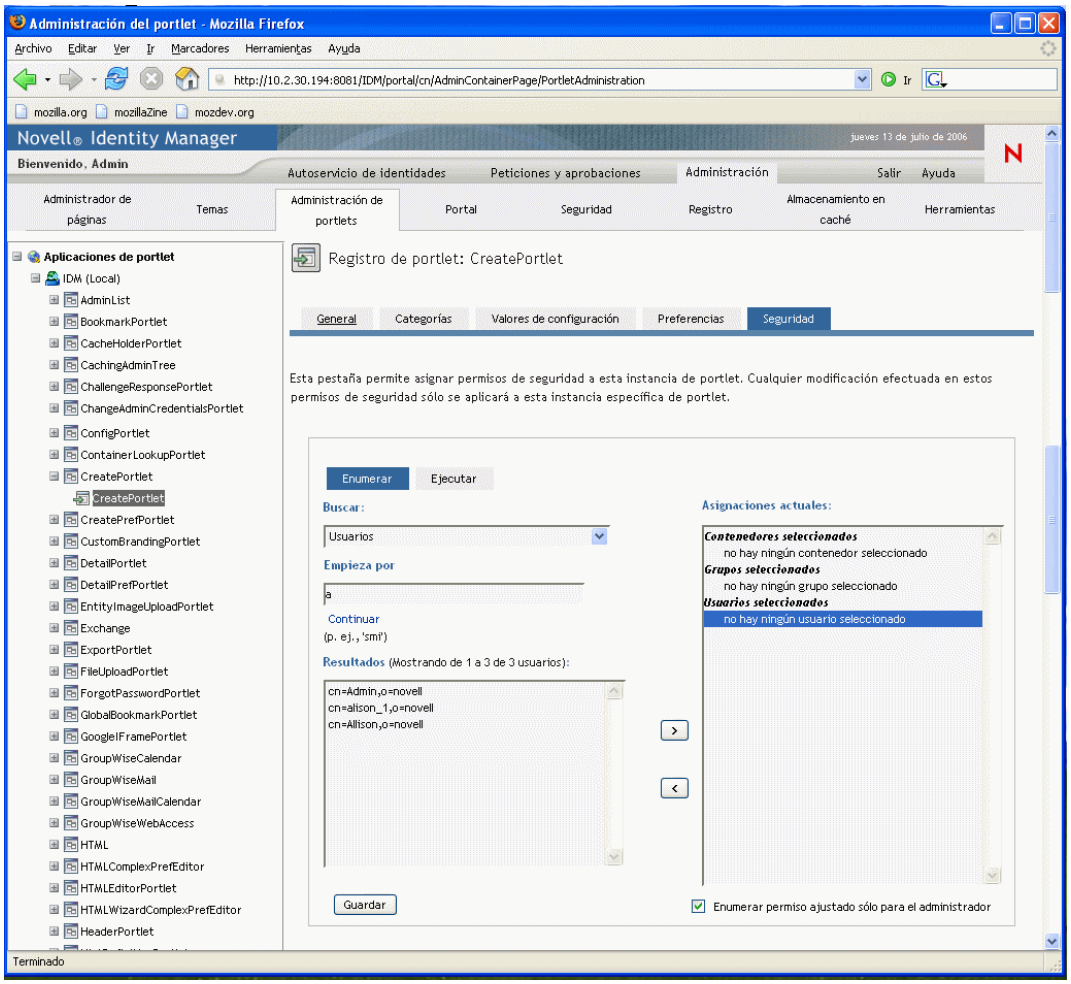
Si se modifican los permisos de seguridad, los valores nuevos entrarán en vigor sólo en el registro de portlet seleccionado.

Para asignar permisos de seguridad para registros de portlet:

1. En la lista Aplicaciones de portlet, *seleccione* el registro de portlet cuyos permisos de seguridad desee modificar.

   Se visualizará un panel *General* a la derecha.
2. Vaya al panel *Seguridad*.

Este panel muestra los permisos de seguridad actuales del registro de portlet seleccionado:



3 Vaya a la pestaña *Lista* o *Ejecutar*, según el tipo de permiso que desee asignar.

4 Especifique los *valores de búsqueda* siguientes:

Valor	Operaciones que puede realizar
Buscar	Seleccione una de las opciones siguientes en el menú desplegable: ◆ Usuarios ◆ Grupos ◆ Contenedores

Valor	Operaciones que puede realizar

Empieza por	Si desea:
	◆ **Encontrar todos** los objetos disponibles del tipo que ha especificado (usuario, grupo o contenedor), deje este valor en blanco.
	◆ **Encontrar un subconjunto** de los objetos, introduzca los caracteres de inicio de los valores CN. (No se distingue entre mayúsculas y minúsculas. No se admiten comodines).
	Por ejemplo, si busca grupos que empiezan por `S`, los resultados de la búsqueda disminuirán y obtendrá una respuesta similar a la siguiente:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Si busca grupos que empiezan por `Se` obtendrá:
	`cn=Service,ou=groups,o=MyOrg`

5 Haga clic en *Continuar*.

Los resultados de la búsqueda aparecerán en la lista *Resultados*.

6 *Seleccione* los usuarios, grupos o contenedores que desee asignar al registro de portlet y, a continuación, haga clic en el botón *Añadir* (>).

Sugerencia: Mantenga pulsada la tecla *Control* para realizar varias selecciones.

7 Habilite o inhabilite el *bloqueo* del registro de portlet, tal como se indica a continuación:

Si desea	Realice la operación siguiente
Bloquear el registro de portlet para que sólo los administradores de la aplicación de usuario puedan solicitar una lista o ejecutarlo	Active **Permiso de ejecución definido sólo para el administrador** o **Permiso de lista definido sólo para el administrador**

Si desea	Realice la operación siguiente
Permitir que todos los usuarios, grupos y contenedores asignados soliciten una lista de registros de portlet o ejecuten el registro de portlet	Desactive **Permiso de ejecución definido sólo para el administrador** o **Permiso de lista definido sólo para el administrador** **Nota:** Si desactiva este valor, pero no hay ningún usuario, grupo o contenedor asignado explícitamente al registro de portlet, **todos tendrán permiso de lista o de ejecución** sobre este registro de portlet.

8 Haga clic en *Guardar*.

9.4.7 Anulación del registro de un portlet

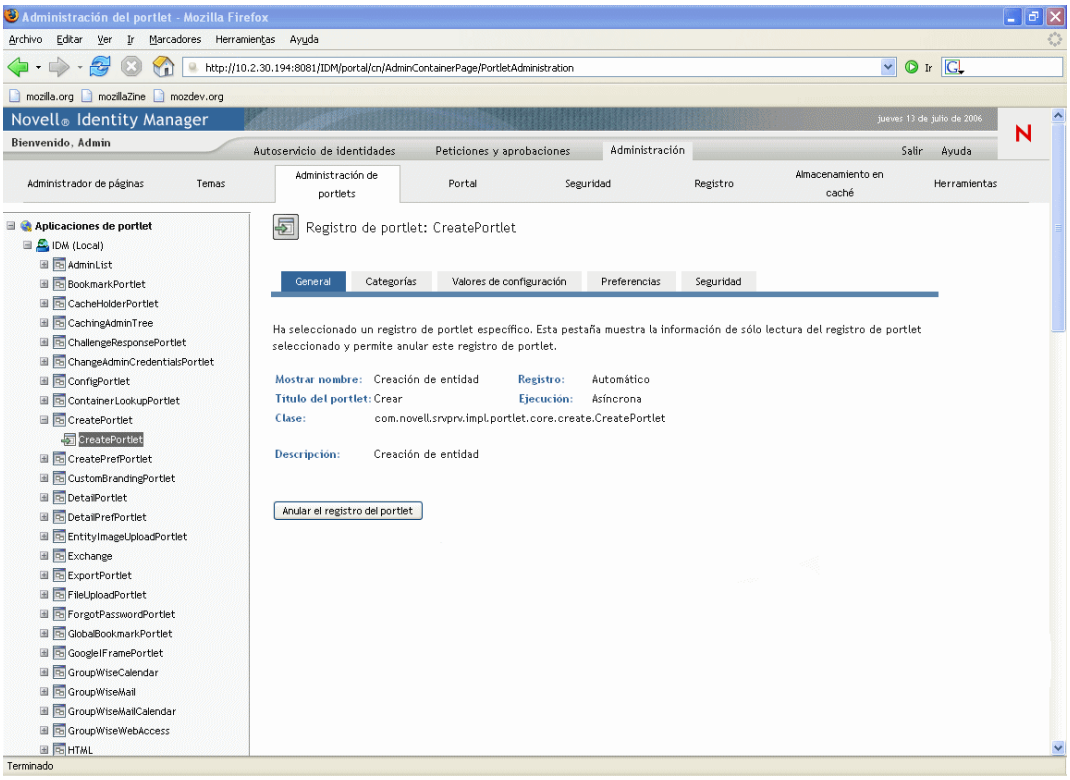
Puede utilizar la página ADMIN de portlet para anular el registro de un portlet, si es necesario.

Nota: Si anula el registro de un portlet definido como *registrado automáticamente*, dicho portlet se volverá a registrar automáticamente cuando reinicie el servidor de aplicación.

Para anular el registro de un portlet:

1 En la lista Aplicaciones de portlet, *seleccione* el registro de portlet que desea anular.

Se visualizará un panel *General* a la derecha, mostrando información acerca del registro de portlet seleccionado:



2 Haga clic en *Anular el registro del portlet*.

3 Cuando el sistema le solicite que confirme la operación de anulación de registro, haga clic en *Aceptar*.

Configuración del portal

10

En este capítulo se describe cómo utilizar la página *Portal* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general sobre cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

10.1 Acerca de la configuración del portal

Puede utilizar la página Portal para controlar las *características del portal* de la aplicación de usuario del Gestor de identidades y especificar cómo se conecta la aplicación de usuario al *repositorio seguro de identidades* (proveedor de LDAP).

10.2 Valores generales

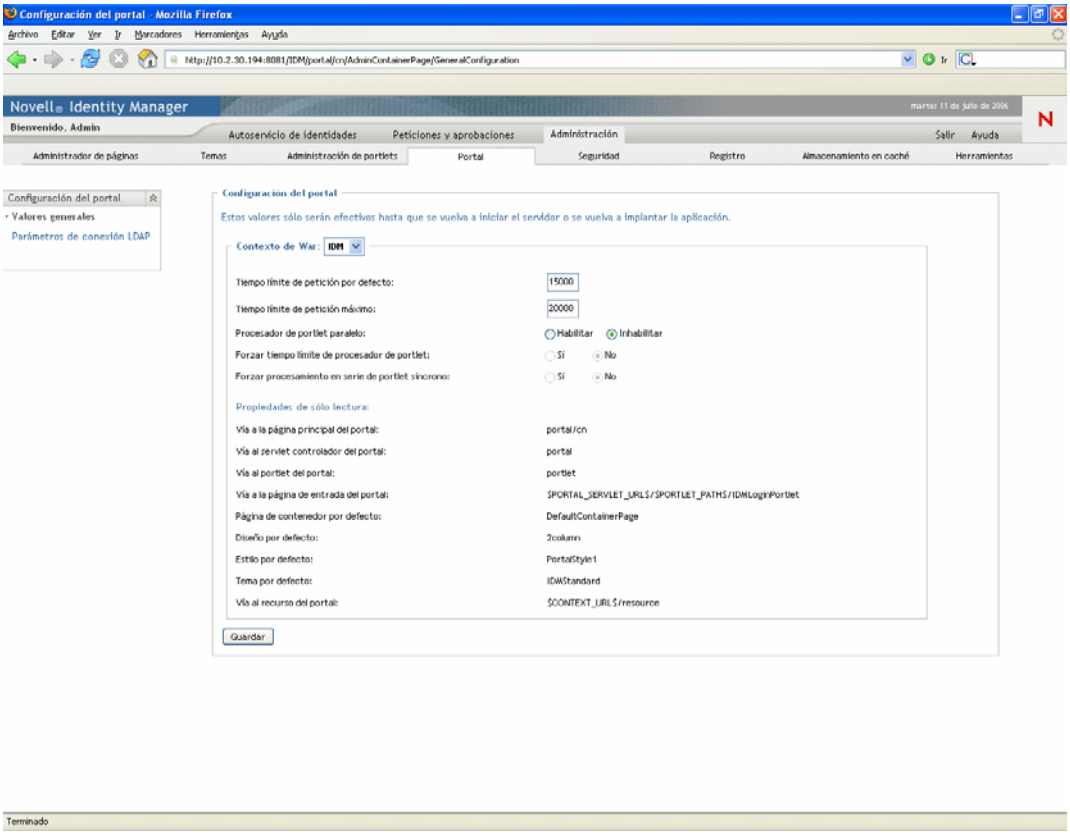
La página Portal dispone de un panel Valores generales que puede utilizar para:

- *Cambiar algunas características del portal* de la aplicación de usuario del Gestor de identidades temporalmente (hasta que se vuelva a reiniciar el servidor de aplicación o se reimplante la aplicación de usuario)
- *Ver otras características del portal* de la aplicación de usuario del Gestor de identidades

Para administrar valores generales:

1. En la página Portal, seleccione *Valores generales* en el menú de navegación de la izquierda.

Se visualizará el panel Valores generales:



2 Si tiene más de un *Contexto de War*, seleccione aquel a cuyos valores desee acceder.

   El panel se actualizará para mostrar los valores actuales del contexto elegido.

3 *Examine* y *modifique* los valores según sus necesidades. Para obtener información detallada, consulte:

   - Sección 10.2.1, “Valores que se pueden cambiar”, en la página 202
   - Sección 10.2.2, “Valores de sólo lectura”, en la página 204

4 Si introduce cambios que desea aplicar, haga clic en *Guardar*.

10.2.1 Valores que se pueden cambiar

Puede modificar varios valores del portal en el panel Valores generales. Los valores estarán en vigor hasta que se vuelva a reiniciar el servidor de aplicación o se reimplante la aplicación de usuario. Cuando se produce un reinicio o una reimplantación, estos valores recuperan sus valores por defecto para el WAR de la aplicación de usuario.

Valor	Operaciones que puede realizar
Tiempo límite de petición por defecto	Especificar el tiempo por defecto de espera (en milisegundos) de una petición, antes de alcanzar su límite. Si ninguno de los portlets asíncronos define un tiempo límite, o ninguno de los portlets define un tiempo límite superior a este valor, se utilizará este valor por defecto. Si uno o varios de los portlets que se van a procesar define un tiempo límite superior a este valor por defecto, se utilizará el valor más alto, en vez de utilizar el valor por defecto. Este valor se puede utilizar para proteger la aplicación y evitar que reciba demasiados mensajes indicando que los portlets han agotado el tiempo límite (caso que puede producirse si los valores que tienen definidos son demasiado bajos). **Nota:** En caso de que todos los portlets se puedan procesar antes de que se agote el tiempo límite, la petición regresará inmediatamente al cliente.
Tiempo límite de petición máximo	Especificar el tiempo máximo (en milisegundos) de retención de una petición para evitar que finalice. Esto significa que una vez transcurrido este tiempo, todas las peticiones regresarán al cliente, sin tener en cuenta si algún portlet define un valor de tiempo límite más alto. Este valor se puede utilizar para asegurarse de que el portal responde puntualmente, aunque uno o varios portlets tengan un valor de tiempo de espera más alto.
Procesador de portlet paralelo	Habilitar o inhabilitar el procesamiento de portlets asíncronos en el portal. Se trata de una función avanzada que, por defecto, está inhabilitada. Si habilita esta función, el portal asignará las peticiones de procesamiento asíncronas a hilos individuales (lo que permite a los portlets procesar contenido en paralelo). Cuando esta función esté inhabilitada, todos los portlets procesarán el contenido de forma síncrona en el hilo de petición principal.
Forzar tiempo límite de procesador de portlet	Determinar si los portlets asíncronos se delegan al hilo de petición principal para procesar contenido, en caso de que la agrupación de hilos no contenga suficientes hilos individuales. Si selecciona **No**, los portlets asíncronos podrán ejecutarse en el hilo de petición principal si no hay ningún hilo individual disponible. Si selecciona **Sí**, los portlets asíncronos tendrán que esperar a que haya hilos individuales disponibles para poder procesar contenido. Si los portlets agotan el tiempo límite antes de ejecutar la petición de procesamiento, se generará un mensaje de error específico del portlet en la ventana de éste.

Valor	Operaciones que puede realizar
Forzar procesamiento en serie de portlet síncrono	Determinar cómo se ejecutan los portlets síncronos. Si selecciona **Sí**, todos los portlets asíncronos se ejecutarán en el hilo de petición principal. Si selecciona **No**, el portal asignará un hilo separado para procesar las peticiones de procesamiento síncronas (lo que evitará atascos en el hilo de petición principal).

10.2.2 Valores de sólo lectura

Los valores que mostramos a continuación, se muestran únicamente por motivos puramente informativos y no se pueden cambiar en el panel Valores generales:

Vía a la página principal del portal	Disposición por defecto
Vía al servlet controlador del portal	Estilo por defecto
Vía al portlet del portal	Tema por defecto
Vía a la página de entrada del portal	Vía al recurso del portal
Página de contenedor por defecto	

Los valores se configuran en el archivo WAR de la aplicación de usuario. (Tenga en cuenta que el Tema por defecto refleja la opción de tema actual de la página Temas).

10.3 Parámetros de conexión LDAP

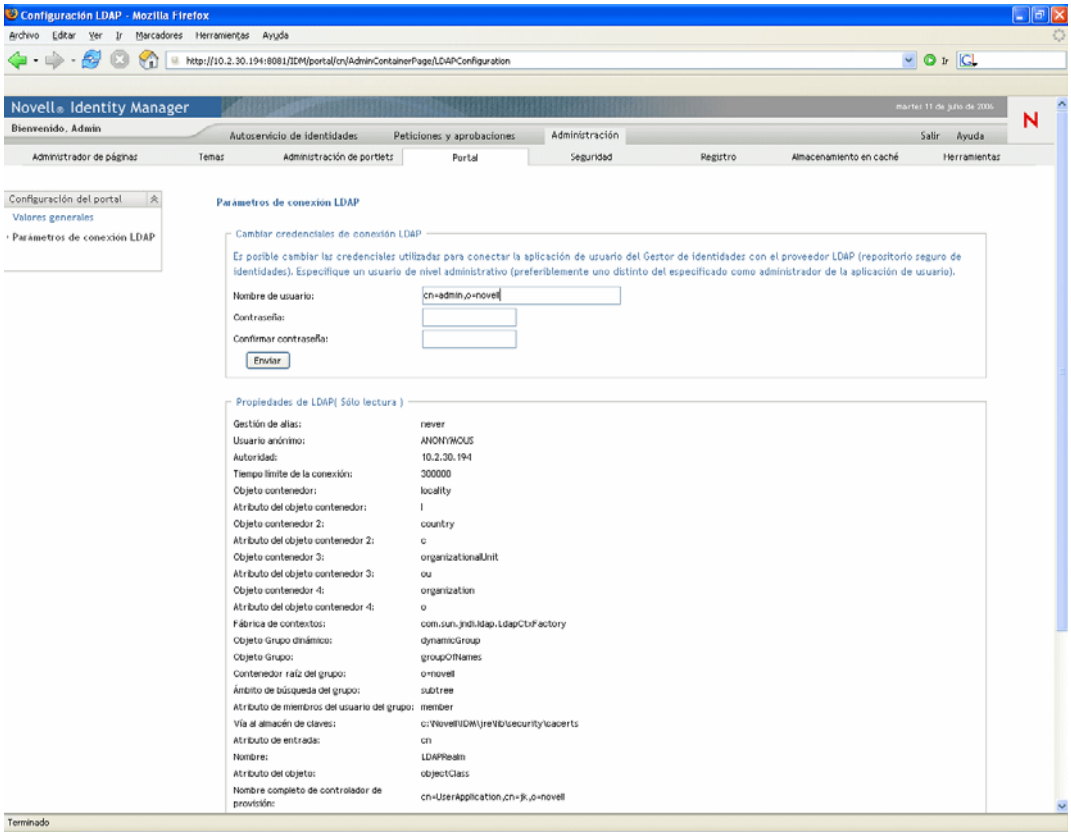
La página Portal dispone de un panel Parámetros de conexión LDAP que puede utilizar para:

- *Cambiar las credenciales* utilizadas por la aplicación de usuario del Gestor de identidades al conectarse al repositorio seguro de identidades (proveedor de LDAP)
- *Ver otras propiedades LDAP* de la aplicación de usuario del Gestor de identidades

Para administrar los parámetros de conexión LDAP:

1. En la página Portal, seleccione *Parámetros de conexión LDAP* en el menú de navegación de la izquierda.

El panel Parámetros de conexión LDAP se visualiza:



2 *Examine* y *modifique* los valores según sus necesidades. Para obtener información detallada, consulte:

- Sección 10.2.1, “Valores que se pueden cambiar”, en la página 202
- Sección 10.3.2, “Valores de sólo lectura”, en la página 206

3 Si introduce cambios que desea aplicar, haga clic en *Enviar*.

10.3.1 Valores que se pueden cambiar

En el panel Parámetros de conexión LDAP, puede modificar los valores de las credenciales que la aplicación de usuario del Gestor de identidades utilizará cuando se conecte al repositorio seguro de identidades (proveedor de LDAP). Los cambios que introduzca en este panel se guardarán en la base de datos de la aplicación del usuario para utilizarlos en el tiempo de ejecución y se comprobarán en el repositorio seguro de identidades. (Tenga en cuenta que este panel no actualiza los valores de las credenciales originales registrados en el WAR de la aplicación de usuario durante la instalación).

Valor	Operaciones que puede realizar
Nombre de usuario	Escriba el nombre de un usuario que tenga derechos completos de **administrador** en el repositorio seguro de identidades. Para poder funcionar, la aplicación de usuario del Gestor de identidades necesita acceder como administrador a dicho repositorio. Es normal especificar el administrador **root** (raíz) como nombre de usuario de la conexión LDAP. El administrador root (raíz) tiene pleno control sobre el árbol, por lo que no es necesario asignar ningún derecho de Trustee especial. Por ejemplo: `cn=admin,o=myorg` Si especifica algún otro usuario, deberá asignar derechos de Trustee heredables a las propiedades [Derechos sobre todos los atributos] y [Derechos de entrada] en el controlador de la aplicación de usuario. **Nota:** Para evitar confusiones, se recomienda que **no** especifique el administrador de la aplicación de usuario como nombre de usuario de la conexión LDAP. Es mejor utilizar cuentas diferentes para estos dos objetivos.
Contraseña y Confirmar contraseña	Escriba la contraseña definida actualmente para el nombre de usuario en el repositorio seguro de identidades

10.3.2 Valores de sólo lectura

Los valores que mostramos a continuación, se muestran únicamente por motivos puramente informativos y no se pueden cambiar en el panel Parámetros de conexión LDAP:

ALIAS_HANDLING	GROUP_USER_MEMBER_ATTRIB
ANONYMOUS_USER	KEYSTORE_PATH
AUTHORITY	LOGIN_ATTRIBUTE
CONNECTION_TIMEOUT	NAME
CONTAINER_OBJECT	OBJECT_ATTRIB
CONTAINER_OBJECT_ATTRIB	PROVISION_ROOT
CONTAINER_OBJECT2	REFERRAL
CONTAINER_OBJECT2_ATTRIB	ROOT_NAME
CONTAINER_OBJECT3	USE_DYNAMIC_GROUPS
CONTAINER_OBJECT3_ATTRIB	USE_REGISTERED_DYNAMIC_GROUPS

CONTAINER_OBJECT4	USE_SSL
CONTAINER_OBJECT4_ATTRIB	USER_GROUP_MEMBER_ATTRIB
CONTEXT_FACTORY	USER_OBJECT
DYNAMIC_GROUP_OBJECT	USER_ROOT_CONTAINER
GROUP_OBJECT	USER_SEARCH_SCOPE
GROUP_ROOT_CONTAINER	UUID_ATTRIB
GROUP_SEARCH_SCOPE	UUID_AUX_CLASS

Los valores de configuración se determinan al instalar la aplicación de usuario.

Configuración de la seguridad 11

En este capítulo se describe cómo utilizar la página *Seguridad* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general sobre cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

11.1 Acerca de la configuración de seguridad

Puede utilizar la página Seguridad para especificar quién es un *administrador de la aplicación de usuario* para la aplicación de usuario del Gestor de identidades.

Un administrador de la aplicación de usuario tiene permiso para ejecutar todas las funciones de gestión de la aplicación de usuario del Gestor de identidades. Esto incluye acceder a la pestaña Administración de la interfaz de usuario del Gestor de identidades para ejecutar cualquier acción de administración que admita.

Durante la instalación, se especifica un usuario como administrador de la aplicación de usuario. Después de la instalación, dicho usuario puede utilizar la página Seguridad para especificar otros administradores de la aplicación de usuario, según las necesidades.

Un usuario que va a ser administrador de la aplicación de usuario normalmente debe *encontrarse en el contenedor raíz de usuarios* especificado en la configuración LDAP de la aplicación de usuario; esto permite que el usuario se registre simplemente con el nombre de usuario (en vez de tener que indicar cada vez el nombre completo). También es normal que este usuario tenga *derechos para mantener y crear objetos* del árbol; no obstante, no es obligatorio.

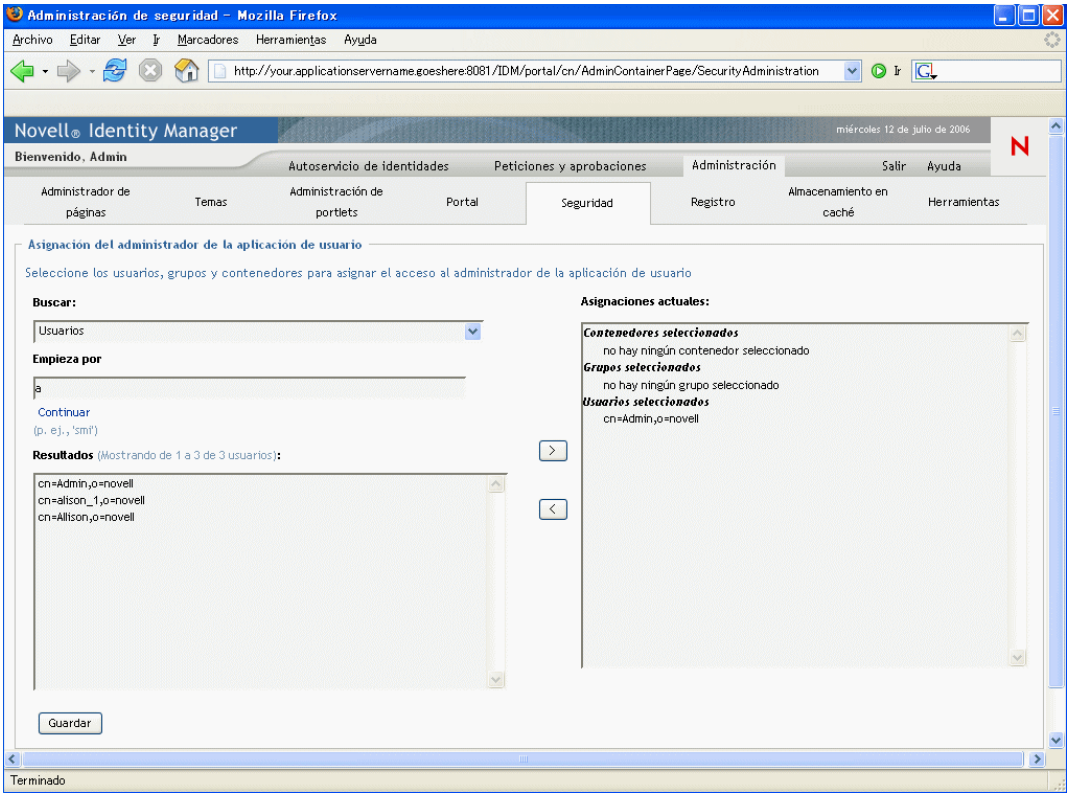
Nota: Si es preciso, un administrador de la aplicación de usuario puede asignar permisos a uno o varios usuarios para que vean o accedan a páginas específicas de la pestaña Administración. Dichos permisos se asignan utilizando la página *Administrador de páginas* de la pestaña Administración. (Para obtener información detallada, consulte Capítulo 7, “Administración de páginas”, en la página 135).

11.2 Asignación del administrador de la aplicación de usuario

Cuando se asignan administradores de la aplicación de usuario, también se pueden especificar usuarios, grupos o contenedores.

Para asignar administradores de la aplicación de usuario:

1 Vaya a la página *Seguridad*:



2 Especifique los *valores de búsqueda* siguientes:

Valor	Operaciones que puede realizar
Buscar	Seleccione una de las opciones siguientes en el menú desplegable: ◆ Usuarios ◆ Grupos ◆ Contenedores

Valor	Operaciones que puede realizar

Empieza por	Si desea:
	◆ **Encontrar todos** los objetos disponibles del tipo especificado (usuario, grupo o contenedor), deje este valor en blanco.
	◆ **Encontrar un subconjunto** de los objetos, introduzca los caracteres de inicio de los valores CN. (No se distingue entre mayúsculas y minúsculas. No se admiten comodines).
	Por ejemplo, si busca grupos que empiezan por `S`, los resultados de la búsqueda disminuirán y obtendrá una respuesta similar a la siguiente:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Si busca grupos que empiezan por `Se` obtendrá:
	`cn=Service,ou=groups,o=MyOrg`

3 Haga clic en *Continuar*.

Los resultados de la búsqueda aparecerán en la lista *Resultados*.

4 *Seleccione* los usuarios, grupos o contenedores que desee asignar como administradores de la aplicación de usuario y, a continuación, haga clic en el botón *Añadir* (>).

Sugerencia: Mantenga pulsada la tecla *Control* para realizar varias selecciones.

5 Haga clic en *Guardar*.

Para anular la asignación de administradores de la aplicación de usuario:

1 En la lista *Asignaciones actuales*, seleccione los usuarios, grupos o contenedores cuya asignación como administradores de la aplicación de usuario desee anular y, a continuación, haga clic en el botón *Eliminar* (<).

Sugerencia: Mantenga pulsada la tecla *Control* para realizar varias selecciones.

2 Haga clic en *Guardar*.

Configuración del registro

12

En este capítulo se describe cómo utilizar la página *Registro* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general acerca de cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

12.1 Acerca de la configuración del registro

Puede utilizar la página Registro para controlar los *niveles de los mensajes de registro* que desea que la aplicación de usuario del Gestor de identidades genere, y especificar si dichos mensajes se enviarán a *Novell Audit*.

La aplicación de usuario del Gestor de identidades implementa el registro mediante *log4j*, un paquete de registro de código abierto distribuido por The Apache Software Foundation. Por defecto, los mensajes de eventos se registran en:

- *La consola del sistema* del servidor de aplicación en el que se implanta la aplicación de usuario del Gestor de identidades.
- *Un archivo de registro* del servidor de aplicación; por ejemplo:

  ```
  jboss/server/IDM/log/server.log
  ```

Se trata de un archivo de registro desplazable; cuando el archivo alcanza un tamaño determinado, el registro se desplaza a otro archivo (etc.).

Si ha configurado su entorno para que incluya Novell Audit, también tiene la opción de registrar mensajes de eventos.

Para obtener información acerca de cómo configurar el entorno de registro y Novell Audit, consulte Capítulo 5, “Configuración de las entradas”, en la página 119.

12.2 Acerca de los registros

La página Registro enumera una serie de registros que producen, cada uno, mensajes de eventos de diferentes partes de la aplicación de usuario del Gestor de identidades. Cada registro tiene su propio nivel de salida independiente.

Los nombres de los registros están basados en convenciones de log4j. Verá dichos nombres en los mensajes de eventos que se generan, indicando el contexto de la salida de mensaje.

Registro	Descripción
com.novell	Padre de otros registros de la aplicación de usuario del Gestor de identidades
com.novell.afw.portal.aggregation	Mensajes relacionados con el proceso de la página del portal
com.novell.afw.portal.persist	Mensajes relacionados con la consolidación de datos del portal (incluidos los registros de portlet y las páginas del portal)
com.novell.afw.portal.portlet	Mensajes de los portlets del núcleo del portal y de los portlets accesorios
com.novell.afw.portal.util	Mensajes de los portlets de importación, exportación y de navegación
com.novell.afw.portlet.consumer	Mensajes relacionados con el procesamiento de portlets
com.novell.afw.portlet.core	Mensajes relacionados con la API del portlet básico
com.novell.afw.portlet.persist	Mensajes relacionados con la consolidación de datos del portlet (incluidos los valores de configuración y las preferencias del portlet)
com.novell.afw.portlet.producer	Mensajes relacionados con el registro y configuración de los portlets del portal
com.novell.afw.portlet.util	Mensajes relacionados con el código de utilidad utilizado por los portlets
com.novell.afw.theme	Mensajes del subsistema de temas
com.novell.afw.util	Mensajes relacionados con las clases de utilidad del portal
com.novell.soa.af.impl	Mensajes del subsistema de flujo de aprobación (flujo de trabajo de provisión)
com.novell.srvprv.apwa	Mensajes de la aplicaciones Web de Peticiones y aprobaciones (acciones y etiquetas)
com.novell.srvprv.impl.portlet.core	Mensajes de los portlets de identidad del núcleo y de los portlets de contraseña
com.novell.srvprv.impl.portlet.util	Mensajes de los portlets de utilidad relacionados con la identidad
com.novell.srvprv.impl.servlet	Mensajes de los servicios ajax y del servlet ajax del marco de control de la IU
com.novell.srvprv.impl.uictrl	Mensajes de la API del registro de control de la IU y del procesamiento del formulario de aprobación
com.novell.srvprv.impl.vdata	Mensajes del nivel de abstracción del directorio
com.novell.srvprv.spi	Mensajes de la API del registro de control de la IU
com.sssw.fw.cachemgr	Mensajes relacionados con el subsistema de caché del marco
com.sssw.fw.core	Mensajes relacionados con el subsistema núcleo del marco

Registro	Descripción
com.sssw.fw.directory	Mensajes relacionados con el subsistema de directorios del marco
com.sssw.fw.event	Mensajes relacionados con el subsistema de eventos del marco
com.sssw.fw.factory	Mensajes relacionados con el subsistema de fábrica del marco
com.sssw.fw.persist	Mensajes relacionados con el subsistema de consolidación del marco
com.sssw.fw.resource	Mensajes relacionados con el subsistema de recursos del marco
com.sssw.fw.security	Mensajes relacionados con el subsistema de seguridad del marco
com.sssw.fw.server	Mensajes relacionados con el subsistema de servidores del marco
com.sssw.fw.servlet	Mensajes relacionados con el subsistema de servlets del marco
com.sssw.fw.session	Mensajes relacionados con el subsistema de sesiones del marco
com.sssw.fw.usermgr	Mensajes relacionados con el subsistema de usuarios del marco
com.sssw.fw.util	Mensajes relacionados con el subsistema de utilidades del marco
com.sssw.portal.manager	Mensajes relacionados con el gestor de portales
com.sssw.portal.persist	Mensajes relacionados con la consolidación de portales

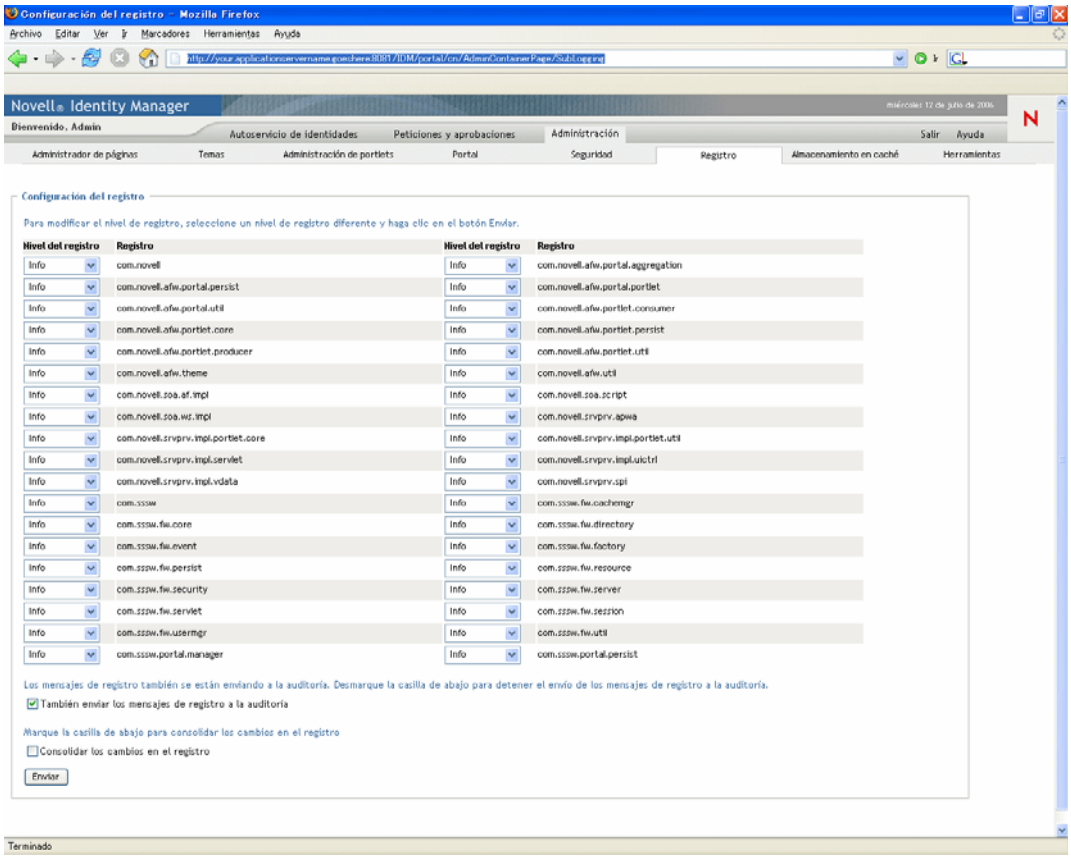
Tenga en cuenta que los registros de la aplicación de usuario son jerárquicos. Por ejemplo, com.novell es padre de los registros que tiene debajo. Todos los registros adicionales heredarán sus propiedades.

12.3 Cambio de los niveles de registro

Se puede controlar la cantidad de información que se escribe en un registro determinado, cambiando el nivel que se ha definido para él. Por defecto, todos los registros están definidos en *Info*, que es un nivel intermedio.

Para cambiar los niveles de registro:

1 Vaya a la página *Registro*:



2 En la parte superior de la página, *busque el registro* cuyo nivel desee cambiar.

3 Utilice el menú desplegable para *seleccionar* uno de los niveles siguientes:

Nivel	Descripción
Grave	**La información mínima:** escribe los errores graves en el registro
Error	Escribe los errores (más todo lo anterior) en el registro
Advertir	Escribe advertencias (más todo lo anterior) en el registro
Info	Escribe mensajes de tipo informativo (más todo lo anterior) en el registro
Depurar	Escribe información de depuración (más todo lo anterior) en el registro

Nivel	Descripción
Seguimiento	**La información más detallada:** Escribe información de seguimiento (más todo lo anterior) en el registro

4 *Repita* Paso 2 y Paso 3 para los registros restantes, si es preciso.

5 Haga clic en *Enviar*.

12.4 Envío de mensajes de registro a Novell Audit

Puede utilizar la página Registro para controlar si la aplicación de usuario del Gestor de identidades envía la producción de mensajes de eventos a Novell Audit. Por defecto, el registro de Novell Audit está desactivado, a menos que lo haya activado al instalar la aplicación de usuario.

Para activar o desactivar el registro de Novell Audit:

1 Vaya a la página *Registro*.

2 *Seleccione o anule la sección* del valor siguiente, según sus necesidades:

```
Envíe también mensajes de registro a Audit
```

3 Haga clic en *Enviar*.

12.5 Persistencia de los valores de registro

Por defecto, los cambios que introduzca en la página Registro permanecerán en vigor hasta que el usuario reinicie la aplicación de servidor o se reimplante la aplicación de usuario. Después de esto, los valores de registro recobrarán sus valores por defecto.

No obstante, la página Registro brinda la posibilidad de que los cambios en los valores persistan. Si activa esta función, los valores de los registros se almacenarán en un *archivo de configuración del registro* del servidor de aplicación en el que está implantada la aplicación de usuario del Gestor de identidades. Por ejemplo:

```
jboss/server/IDM/conf/extendlogging.xml
```

Para activar o desactivar la persistencia de los valores:

1 Vaya a la página *Registro*.

2 *Seleccione o anule la sección* del valor siguiente, según sus necesidades:

```
Consolidar los cambios en el registro
```

3 Haga clic en *Enviar*.

Configuración del almacenamiento en caché

13

En este capítulo se describe cómo utilizar la página *Almacenamiento en caché* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general sobre cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

13.1 Acerca de la configuración del almacenamiento en caché

Puede utilizar la página Almacenamiento en caché para gestionar diversos *cachés* mantenidos por la aplicación de usuario del Gestor de identidades. La aplicación de usuario utiliza estos cachés para almacenar los datos reutilizables y temporales en el servidor de aplicación, a fin de optimizar el rendimiento.

Tiene la posibilidad de controlar estos cachés cuando así lo necesite, *limpiando su contenido* y *cambiando sus valores de configuración*.

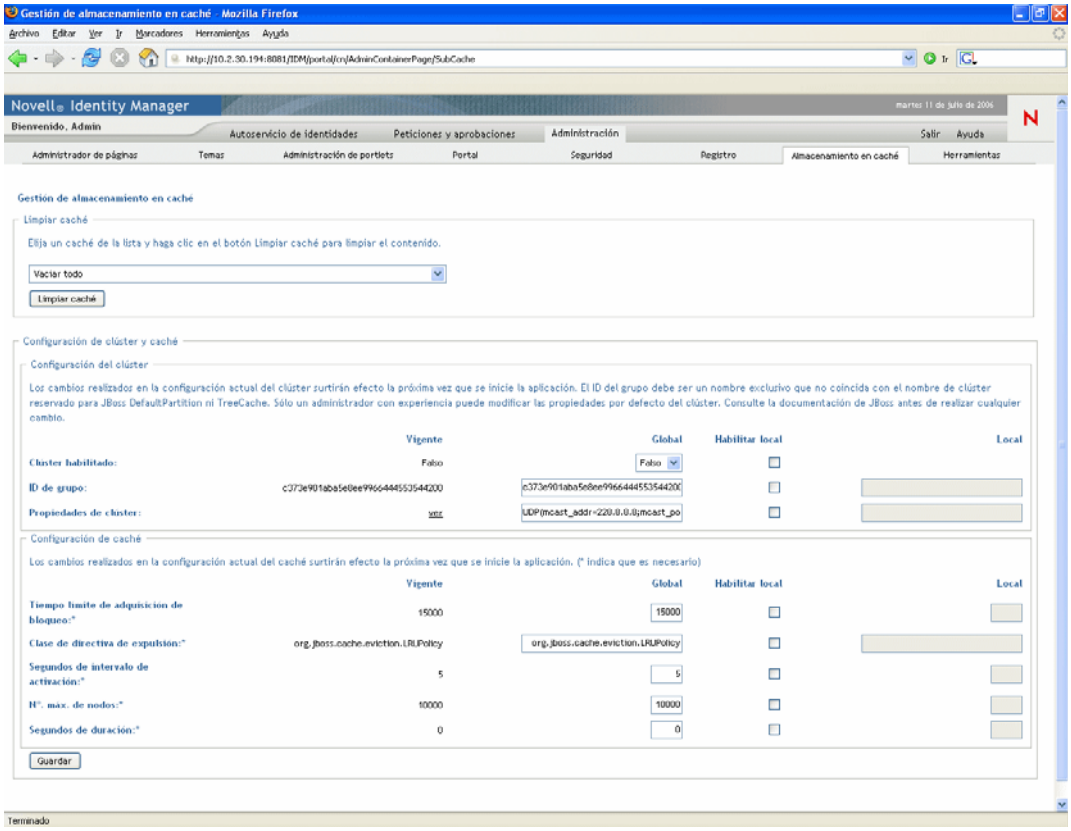
13.2 Limpieza de cachés

Los cachés se denominan en función de los *subsistemas* que los utilizan en la aplicación de usuario del Gestor de identidades. Por lo general, no es necesario que el usuario los limpie, ya que la aplicación de usuario los limpia automáticamente basándose en la frecuencia de uso de los datos o

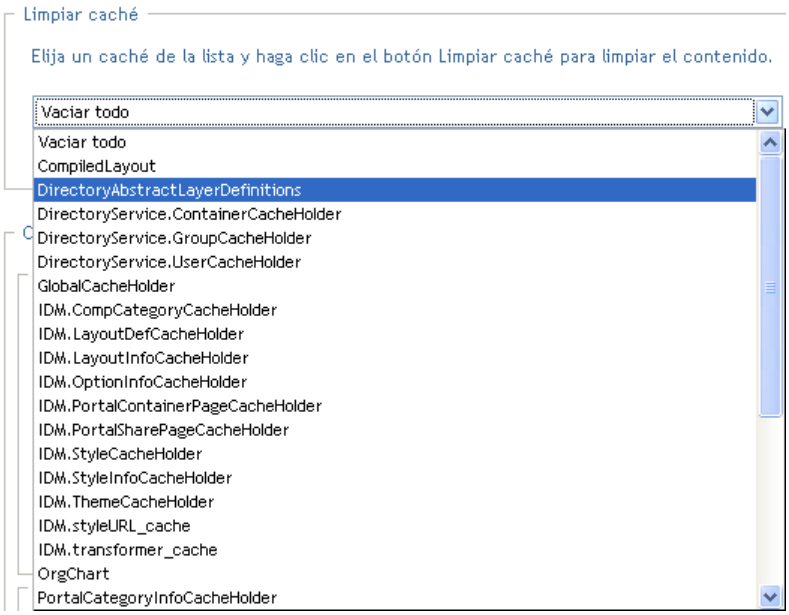
en cuándo cambian los datos de origen. No obstante, si tiene una necesidad específica, puede *limpiar manualmente* los cachés seleccionados o todos los cachés.

Para limpiar cachés:

1 Vaya a la página *Almacenamiento en caché*:



2 En la sección *Limpiar caché* de la página, utilice el menú desplegable para *seleccionar* un caché particular para eliminarlo (o seleccionar *Vaciar todo*):



Tenga en cuenta que la lista de cachés disponibles es *dinámica*; cambia en función de los datos que están almacenados en caché en ese momento.

3 Haga clic en el botón *Limpiar caché*.

13.2.1 Limpieza del caché del nivel de abstracción del directorio

El *nivel de abstracción del directorio* de la aplicación de usuario también tiene un caché. El caché *DirectoryAbstractLayerDefinitions* almacena las definiciones del nivel de abstracción en el servidor de aplicación, a fin de optimizar el rendimiento de todas las operaciones del modelo de datos.

En una situación típica, la aplicación de usuario mantiene sincronizado automáticamente el caché DirectoryAbstractLayerDefinitions con las definiciones del nivel de abstracción almacenadas en el repositorio seguro de identidades. No obstante, si es preciso, puede limpiar manualmente el caché DirectoryAbstractLayerDefinitions (tal como se describe arriba) para obligar a cargar las últimas definiciones del repositorio de identidades.

Para obtener más información acerca del nivel de abstracción del directorio de la aplicación de usuario, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

13.2.2 Limpieza de los cachés de un clúster

La limpieza de cachés está admitida en los entornos de servidores de aplicación en clúster y que no están en clúster. Si su servidor de aplicación forma parte de un clúster y limpia manualmente un caché, dicho caché se *limpiará automáticamente en todos los servidores* del clúster.

13.3 Configuración de los valores del caché

Puede utilizar la página Almacenamiento en caché para visualizar y cambiar los valores de configuración del caché de un entorno de servidores de aplicación *que están en clúster o no lo están*. Los cambios se guardan inmediatamente, pero no entrarán en vigor hasta que el usuario*reinicie la aplicación*.

Sugerencia: Para reiniciar la aplicación de usuario, puede ejecutar una de las acciones siguientes: reiniciar el servidor de aplicación; volver a implantar la aplicación (si se ha introducido algún cambio en el WAR); u obligar a la aplicación a reiniciarse (tal como se describe en la documentación del servidor de aplicación).

Para configurar los valores de caché, necesita saber:

- Sección 13.3.1, “Cómo se implementa el almacenamiento en caché”, en la página 222
- Sección 13.3.2, “Cómo se almacenan los valores de caché”, en la página 222
- Sección 13.3.3, “Cómo se visualizan los valores de caché”, en la página 224
- Sección 13.3.4, “Valores básicos del caché”, en la página 224
- Sección 13.3.5, “Valores de caché para los clústeres”, en la página 226

13.3.1 Cómo se implementa el almacenamiento en caché

En la aplicación de usuario del Gestor de identidades, el almacenamiento en caché se implementa a través de *JBoss Cache*. JBoss Cache es una arquitectura de almacenamiento en caché de código abierto incluida en el servidor de aplicación de JBoss, que también se ejecuta en otros servidores de aplicación.

Para saber más acerca de JBoss Cache, vaya a www.jboss.org/products/jbosscache (http://www.jboss.org/products/jbosscache).

13.3.2 Cómo se almacenan los valores de caché

Existen *dos niveles de valores* disponibles que permiten controlar la configuración del caché. Puede utilizarlos conjuntamente para adaptar el comportamiento del almacenamiento en caché de la aplicación de usuario del Gestor de identidades.

Nivel	Descripción

Valores globales	Los valores globales se **almacenan en una ubicación central** (el repositorio seguro de identidades) para que un gran número de servidores de aplicación puedan utilizar los mismos valores de configuración. Por ejemplo, alguien que tenga un clúster de servidores de aplicación utilizará normalmente valores globales para los valores de configuración del clúster.
	
	Para **encontrar los valores globales** del repositorio seguro de identidades, busque el objeto siguiente en el controlador de la aplicación de usuario del Gestor de identidades:
	
	`configuration.AppDefs.AppConfig`
	
	Por ejemplo:
	
	`configuration.AppDefs.AppConfig.MyUserApplicationDriver.MyDriverSet.MyOrg`
	
	El **atributo XmlData** del objeto de configuración contiene los datos de los valores globales.

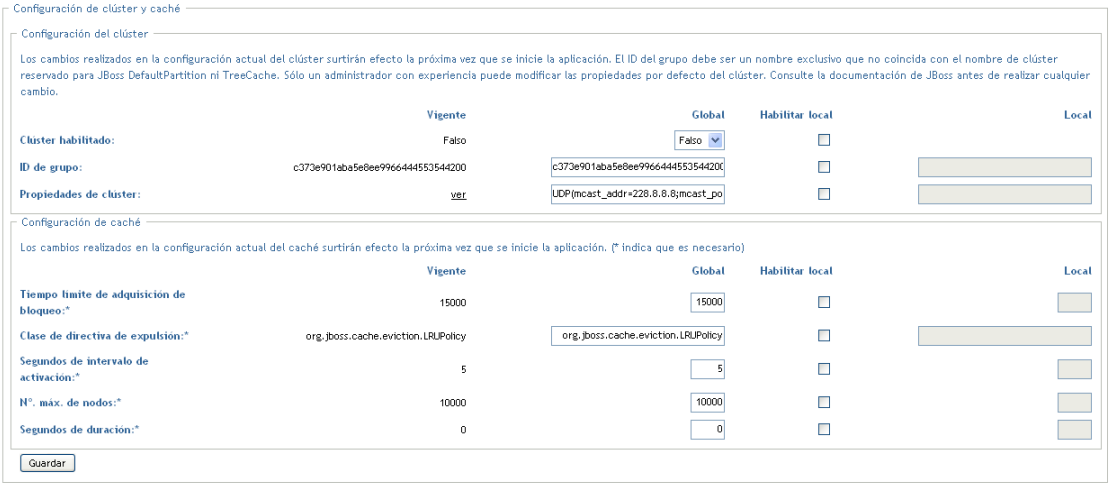
Valores locales	Los valores locales se **almacenan por separado en cada servidor de aplicación**, de tal manera que un servidor individual pueda **anular** el valor de uno o varios valores globales. Por ejemplo, supongamos que desea especificar un valor local para eliminar un servidor de aplicación del clúster especificado en los valores globales, o bien desea cambiar la asignación de un servidor a otro clúster.
	
	Para **encontrar los valores locales** del servidor de aplicación, busque el archivo siguiente en el directorio conf de la configuración de servidor de JBoss:
	
	`sys-configuration-xmldata.xml`
	
	Por ejemplo:
	
	`jboss/server/IDM/conf/sys-configuration-xmldata.xml`
	
	Si el servidor tiene valores locales, dichos datos estarán contenidos en este archivo. (Si no se ha especificado ningún valor local, el archivo no existirá).

Los valores globales deben considerarse los *valores por defecto* de todos los servidores de aplicación que utilicen una instancia concreta del controlador de la aplicación de usuario. Si se

cambia un valor global, dicho cambio *repercutirá sobre todos estos servidores* (cuando el usuario reinicie la aplicación), salvo en los casos en que un servidor local especifique una anulación local.

13.3.3 Cómo se visualizan los valores de caché

La página Almacenamiento en caché visualiza los *valores de caché actuales* (desde el último reinicio de la aplicación por parte del usuario). Asimismo, visualiza los valores *globales y locales* correspondientes de dichos valores, y permite *cambiarlos* (para utilizarlos en el siguiente reinicio de la aplicación).



Tenga en cuenta que los valores globales siempre tienen valores. Los valores locales son opcionales.

13.3.4 Valores básicos del caché

Estos valores de caché se aplican a servidores en clúster y que no están en clúster.

Para configurar valores básicos de caché:

1. Vaya a la página *Almacenamiento en caché*.
2. En el apartado *Configuración de caché* de la página, especifique *valores globales o locales* para los valores siguientes, según sus necesidades:

Valor	Operaciones que puede realizar
Bloquear tiempo límite de adquisición	Especifique el **intervalo de tiempo (en milisegundos)** que esperará el caché para adquirir un bloqueo sobre un objeto. Puede que necesite aumentar este valor si la aplicación de usuario recibe un gran número de excepciones de tiempo límite de bloqueo en el registro de la aplicación. El valor por defecto es 15000 ms.

Valor	Operaciones que puede realizar
Clase de directiva de expulsión	Especifique la **clase** para la directiva de expulsión de caché que desee utilizar. El valor por defecto es la política de expulsión LRU que proporciona JBoss Cache: `org.jboss.cache.eviction.LRUPolicy` Si es preciso, puede cambiar esta política por otra política de expulsión que JBoss Cache admita. Para saber más acerca de las políticas de expulsión admitidas, vaya a www.jboss.org/products/jbosscache (http://www.jboss.org/products/jbosscache).
Segundos de intervalo de activación	Especifique el **intervalo de tiempo (en segundos)** que esperará la política de expulsión antes de activarse para ejecutar las operaciones siguientes: ◆ Procesar los eventos del nodo expulsado ◆ Limpiar los nodos desfasados y que superan el límite de tamaño
Nº. máx. de nodos	Especifique el **número máximo de nodos** permitidos en el caché. Si no desea ningún límite, especifique: `0`
Segundos de duración	Especifique el **tiempo de inactividad (en segundos)** antes de que el nodo desaparezca. Si no desea ningún límite, especifique: `0`

Estos valores son *obligatorios*, lo que significa que debe haber un valor global para cada uno y, opcionalmente, también un valor local.

Si desea *anular* el valor global de un valor con un valor local, seleccione la casilla de verificación *Habilitar local* para dicho valor. A continuación, especifique el valor local. (Asegúrese de que todos los valores locales sean *válidos*. De lo contrario, no podrá guardar los cambios).

Nota: En el caso de aquellos valores para los que Habilitar local no esté seleccionado, todos los valores locales existentes se suprimirán al guardar.

3 Haga clic en *Guardar*.

4 Cuando esté preparado para que los valores guardados entren en vigor, *reinicie la aplicación de usuario* en los servidores de aplicación pertinentes.

13.3.5 Valores de caché para los clústeres

En esta sección se explica cómo configurar el almacenamiento en caché cuando se ejecuta la aplicación de usuario del Gestor de identidades en un clúster de servidores de aplicación. Necesita tener conocimientos sobre:

Cómo se implementa la agrupación en clúster

En la aplicación de usuario del Gestor de identidades, la compatibilidad de clúster para el almacenamiento en caché se implementa a través de *JGroups*. JGroups es una arquitectura de agrupación en clúster de código abierto incluida en el servidor de aplicación de JBoss, que también se ejecuta en otros servidores de aplicación.

El *clúster de la aplicación de usuario* está formado por los nodos de una red que ejecutan JGroups y utilizan un *ID de grupo* común. Por defecto, el ID de grupo que suministra el clúster de la aplicación de usuario es un UUID que tiene el aspecto siguiente:

```
c373e901aba5e8ee9966444553544200
```

El UUID ayuda a asegurar la exclusividad, de modo que el ID de grupo del clúster de la aplicación de usuario no entre en conflicto con los ID de grupo de otros clústeres del entorno. Por ejemplo, el servidor de aplicación de JBoss utiliza dos clústeres JGroup y *reserva los ID de grupo DefaultPartition y TreeCache* para ellos.

Para saber más acerca de JGroups, vaya a www.jboss.org/products/jgroups (http://www.jboss.org/products/jgroups).

Cómo funciona el almacenamiento en caché con un clúster

Cuando se inicia la aplicación de usuario, los valores de configuración del caché de la aplicación determinan si se participará en un clúster y si los cambios del caché se duplicarán en los otros nodos del clúster. Si se habilita la agrupación en clúster, la aplicación de usuario ejecutará la duplicación enviando *mensajes de invalidación de entrada de caché* a cada nodo, cuando se produzcan los cambios.

Preparación para utilizar un clúster

Para utilizar el almacenamiento en caché en un clúster, es preciso ejecutar dos grandes pasos:

1. *Configurar el clúster JGroups propio*

   Esto implica instalar el servidor de aplicación de JBoss para que utilice *toda* la configuración y, a continuación, distribuir la aplicación de usuario del Gestor de identidades (IDM.war) a todos los servidores del clúster, normalmente poniéndola en el directorio *farm*.
2. *Habilitar el uso de dicho clúster* en los valores de configuración de la aplicación de usuario

Consulte “Configuración de los valores de caché para los clústeres” en la página 227 (más abajo).

Configuración de los valores de caché para los clústeres

Una vez tenga un clúster listo para utilizarlo, podrá especificar valores para el soporte del almacenamiento en caché en dicho clúster.

Para configurar los valores de caché para los clústeres:

1. Vaya a la página *Almacenamiento en caché*.
2. En el apartado *Configuración del clúster* de la página, especifique *valores globales o locales* para los valores siguientes, según sus necesidades:

Valor	Operaciones que puede realizar
Clúster habilitado	Seleccione **True** para duplicar los cambios del caché en los nodos restantes del clúster especificados mediante el ID de grupo. Si no desea participar en un clúster, seleccione **False**.
ID de grupo	Especifique el ID de grupo del clúster JGroups en el que desee participar. **No es preciso cambiar el** ID de grupo por defecto proporcionado para el clúster de la aplicación de usuario, **a menos que desee utilizar otro clúster**. Recuerde que los ID de grupo siguientes están reservados para que los utilice el servidor de aplicación de JBoss: DefaultPartition y TreeCache. **Sugerencia:** Para ver el ID de grupo en los mensajes de registro, asegúrese de que el nivel del registro de almacenamiento en caché (com.sssw.fw.cachemgr) esté establecido en Info o en un valor superior.
Propiedades del clúster	Especifique la **pila de protocolos** de JGroups para el clúster especificado por el ID de grupo. Tenga en cuenta que este valor es **para administradores experimentados** que pueden necesitar ajustar las propiedades de clúster. De lo contrario, no cambie la pila de protocolos por defecto. Para ver las propiedades actuales del clúster, haga clic en **ver**. Para obtener información acerca de la pila de protocolos de JGroups, vaya a www.joss.org/wiki/Wiki.jsp?page=JGroups (http://www.jboss.org/wiki/Wiki.jsp?page=JGroups).

Si desea *anular* el valor global de un valor con un valor local, seleccione la casilla de verificación *Habilitar local* para dicho valor. A continuación, especifique el valor local.

Nota: En el caso de aquellos valores para los que Habilitar local no esté seleccionado, todos los valores locales existentes se suprimirán cuando guarde.

Asegúrese de que *todos los nodos* del clúster *especifiquen las mismas* propiedades de ID de grupo y Clúster. (Para ver estos valores en el caso de un nodo en concreto, acceda a la interfaz de usuario del Gestor de identidades de dicho nodo, (yendo a la URL de la interfaz de usuario de dicho servidor) y visualice allí la página de almacenamiento en caché).

3. Haga clic en *Guardar*.
4. Cuando esté preparado para que los valores guardados entren en vigor, *reinicie la aplicación de usuario* en los servidores de aplicación pertinentes.

Herramientas para exportar e importar datos del portal

14

En este capítulo se describe cómo utilizar la página *Herramientas* de la *pestaña Administración* de la interfaz de usuario del Gestor de identidades. Los temas son:

Para obtener más información general sobre cómo acceder a la pestaña Administración y cómo utilizarla, consulte Capítulo 6, “Utilización de la pestaña Administración”, en la página 129.

14.1 Acerca de la exportación e importación de datos del portal

Puede utilizar la página Herramientas para *exportar o importar* contenido del portal (páginas y portlets) utilizado en la aplicación de usuario del Gestor de identidades. A este contenido también se le conoce como *estado de configuración del portal* e incluye:

- Páginas de contenedor y compartidas (incluidos los portlets asignados de cada página y las preferencias y valores de cada portlet)
- Registros de portlets

Las herramientas de exportación e importación permiten mover el estado de configuración de un portal (aplicación de usuario) a otro portal, según las necesidades. A continuación, indicamos cómo funcionan estas herramientas:

Herramienta	Cómo funciona
Exportación de datos del portal	Genera descripciones XML de un conjunto de páginas de contenedor y compartidas seleccionadas, así como de portlets. Los archivos XML se almacenan en un **archivo ZIP de exportación de datos del portal** que se puede utilizar como entrada a la herramienta de importación de datos del portal.
Importación de datos del portal	Acepta el archivo de exportación de datos del portal como entrada. Utiliza el archivo ZIP de exportación de datos del portal para generar páginas de contenedor y compartidas, así como portlets en un portal (aplicación de usuario).

14.1.1 Usos

Las herramientas de exportación e importación de datos del portal se pueden utilizar para:

- *Mover* el estado de configuración del portal de un entorno de prueba (origen) a un entorno de producción (destino)
- *Actualizar* incrementalmente el estado de configuración de un portal

- *Clonar* un portal
- Opcionalmente, *sobrescribir* el estado de configuración del portal de destino

14.1.2 Requisitos

Para utilizar las herramientas de importación y exportación de datos del portal, asegúrese de que la aplicación de usuario del Gestor de identidades (portal) esté *implantada y ejecutándose* en los servidores de aplicación de origen y de destino.

No es preciso que los servidores de origen y de destino accedan al mismo *repositorio seguro de identidades*; pueden acceder a otros, si es pertinente. *No es obligatorio* que los *usuarios, grupos y contenedores* de dichos repositorios seguros de identidades sean los mismos.

14.1.3 Restricciones

No se puede utilizar las herramientas de importación y exportación de datos del portal para:

- Exportar o importar un estado de configuración del portal cuando un servidor esté dando servicio en ese momento a las peticiones de usuarios
- Exportar o importar clases y recursos de portal
- Exportar o importar clases y recursos de portlet
- Exportar o importar los datos de identidad y provisión utilizados en un portal
- Exportar o importar valores de administración que no sean para páginas y portlets
- Migrar el estado de configuración de una versión de portal anterior a una versión posterior (los portales deben ser de la misma versión)

14.1.4 Pasos

Para exportar e importar datos del portal:

1. Si va a efectuar una actualización incremental, *realice una copia de seguridad* del portal de destino.
2. Desde el portal de origen, *exporte* los datos del portal utilizando la herramienta de exportación de datos del portal.

   Consulte Sección 14.2, “Exportación de datos del portal”, en la página 231.
3. Desde el portal de destino, *importe* los datos del portal utilizando la herramienta de importación de datos del portal.

   Consulte Sección 14.3, “Importación de datos del portal”, en la página 232.
4. *Pruebe* el portal de destino para asegurarse de que ha importado los datos que esperaba.

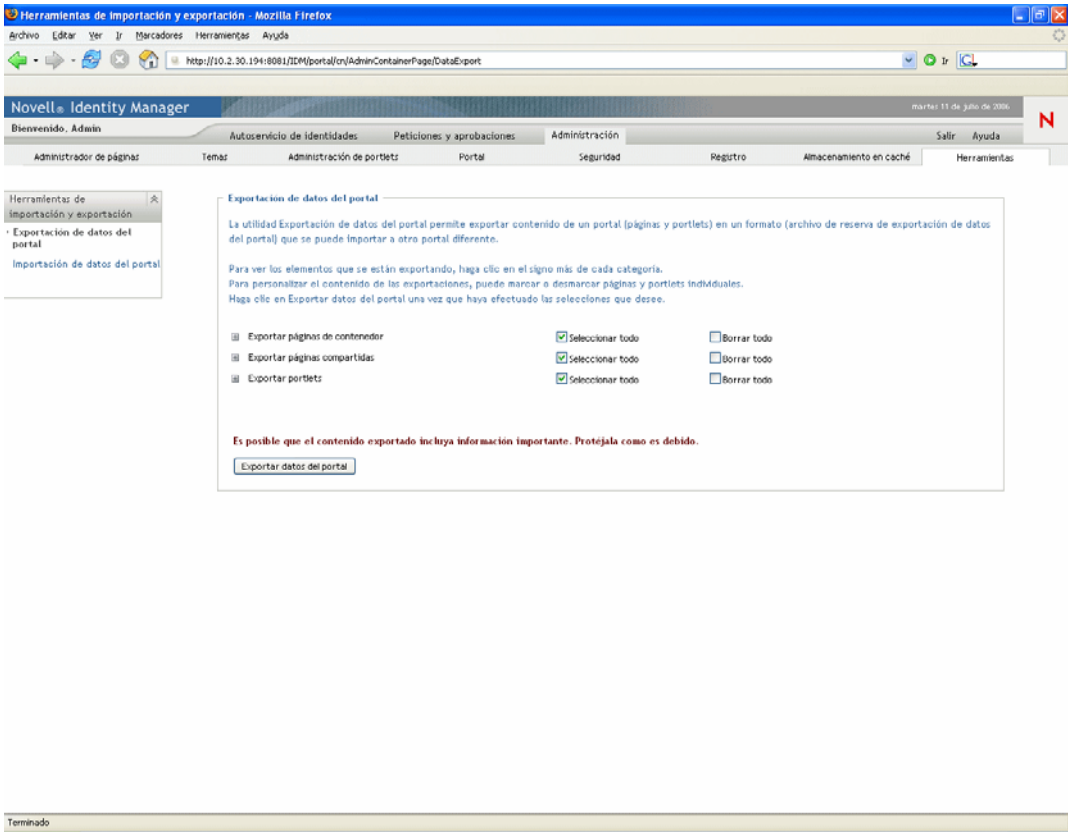
14.2 Exportación de datos del portal

En esta sección se describe cómo exportar un estado de configuración de portal a un archivo ZIP de exportación de datos del portal.

Para exportar datos del portal:

1 En la página Herramientas, seleccione *Exportación de datos del portal* en el menú de navegación de la izquierda.

Se visualizará el panel de exportación de datos del portal:



2 Siga las instrucciones que aparecen en pantalla para *seleccionar las páginas y portlets del portal* que desee exportar.

Nota: Es posible que se exporten algunos portlets que no haya seleccionado para exportarlos. Si exporta una página que contiene un portlet, pero no selecciona dicho portlet para exportarlo, el portlet se exportará (a fin de que no se produzca un error de tiempo de ejecución para la página exportada).

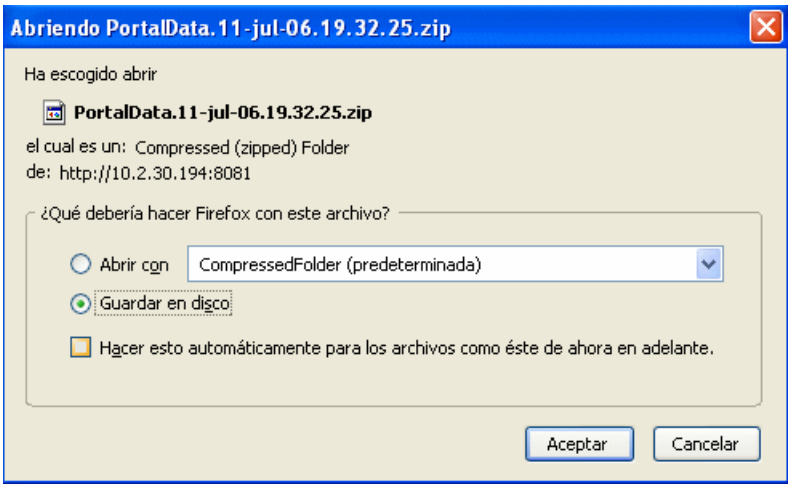
---

3 Cuando haya acabado de seleccionar, haga clic en el botón *Exportar datos del portal*.

Se generará el nuevo *archivo ZIP de exportación de datos del portal*, con un nombre por defecto que incluye la fecha y hora actuales. Por ejemplo:

```
PortalData.21-Oct-05.09.12.16.zip
```

A continuación, el sistema le solicitará que guarde localmente el archivo ZIP (o que lo abra en una utilidad de archivo de reserva apropiada). Por ejemplo:



4 *Guarde* el archivo ZIP de exportación de datos del portal en una ubicación adecuada.

14.3 Importación de datos del portal

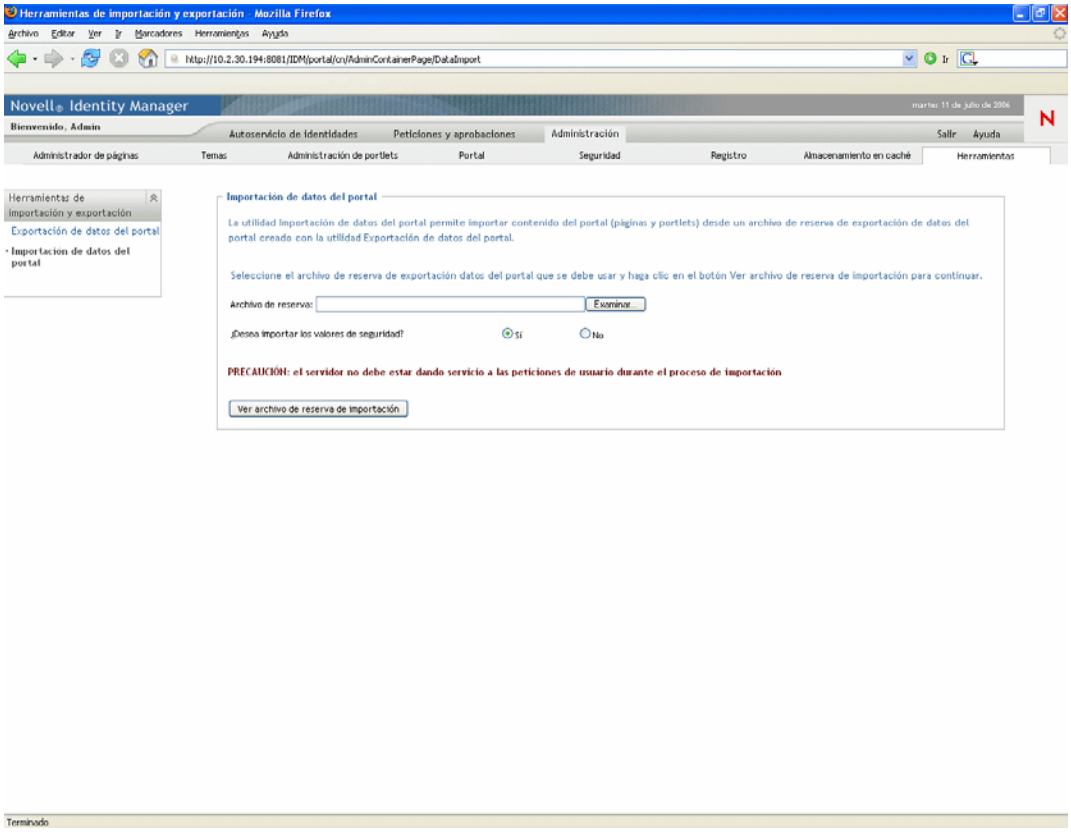
En esta sección se describe cómo importar un archivo ZIP de exportación de datos del portal a un portal.

Nota: Recuerde que, durante la importación, el servidor de aplicación de destino debe estar funcionando, aunque *sin atender, en ese momento, peticiones de usuarios*.

Para importar datos del portal:

1 En la página Herramientas, seleccione *Importación de datos del portal* en el menú de navegación de la izquierda.

Se visualizará el panel de importación de datos del portal:

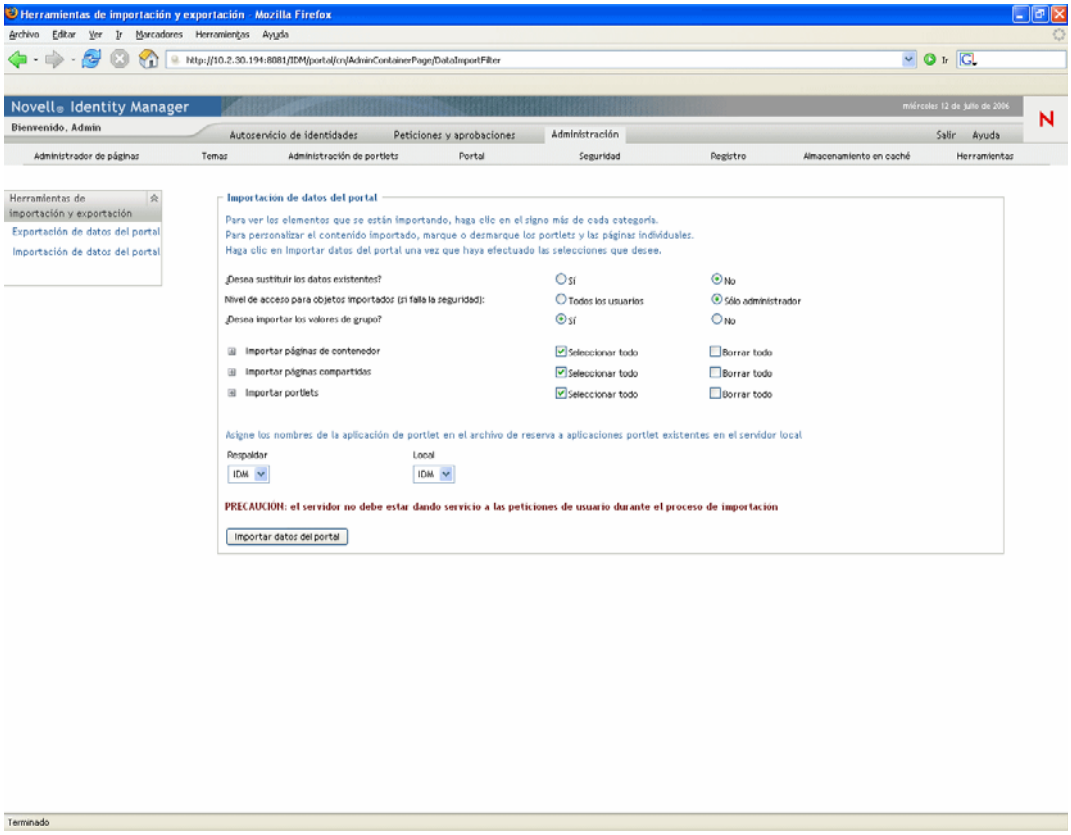


2 Especifique los *valores de importación generales* siguientes:

Valor	Operaciones que puede realizar
Archivo de reserva	Haga clic en el botón **Examinar** para seleccionar el **archivo ZIP de exportación de datos del portal** que se importará. Por ejemplo: `PortalData.21-Oct-05.09.12.16.zip`
¿Desea importar los valores de seguridad?	Seleccione una de las opciones siguientes: ◆ **Sí**: si desea importar los permisos que el archivo ZIP de exportación de datos del portal especifica para que los usuarios, grupos y contenedores accedan a las páginas y portlets. Asegúrese de que los usuarios, grupos y contenedores implicados existan en el repositorio seguro de identidades, ya que los permisos de las entidades que falten no se podrán importar. ◆ **No**: si desea ignorar los permisos que el archivo ZIP de exportación de datos del portal especifica.

3 Haga clic en el botón *Ver archivo de reserva de importación*.

El panel visualizará información más específica relativa al archivo ZIP de exportación de datos del portal y a cómo desea importarlo:



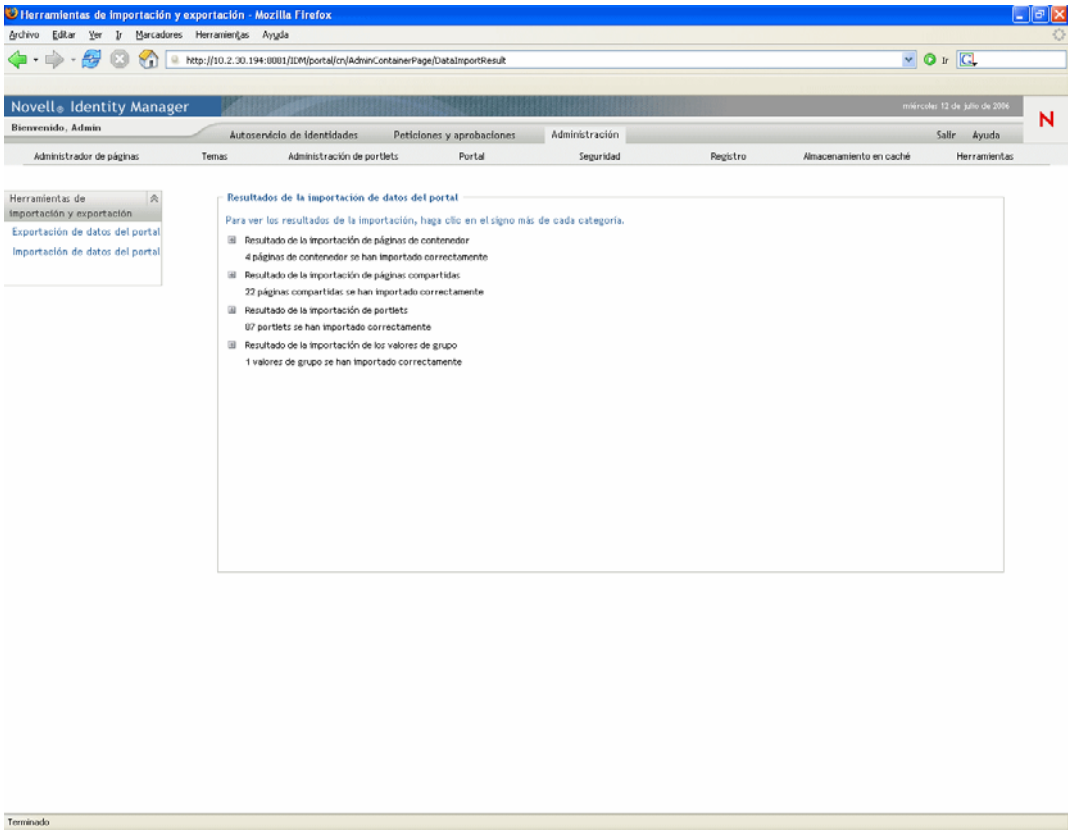
4 Especifique los *valores de importación detallados* siguientes:

Valor	Operaciones que puede realizar
¿Desea sustituir los datos existentes?	Seleccione una de las opciones siguientes: ◆ **Sí**: si desea que el contenido del archivo ZIP de exportación de datos sobrescriba los portlets y páginas correspondientes que ya existen en el portal de destino. Por ejemplo, si el archivo ZIP de exportación de datos del portal contiene una página compartida denominada MyPage y el portal de destino contiene también una página compartida denominada MyPage, esta última página del portal de destino quedará sobrescrita. ◆ **No**: si desea saltar la importación de todos los portlets y páginas existentes.

Valor	Operaciones que puede realizar
Nivel de acceso para objetos importados	Seleccione una de las opciones siguientes: ◆ **Todos los usuarios**: acceso sin restricciones a las páginas y los portlets importados. ◆ **Sólo el administrador**: acceso restringido a las páginas y portlets importados. **Si selecciona importar los valores de seguridad**, este nivel de acceso se aplicará únicamente a las páginas y portlets importados donde el valor de seguridad no se ha podido importar (normalmente debido a que los usuarios, grupos o contenedores especificados no existen en el repositorio seguro de identidades del portal de destino). **Si decide no importar los valores de seguridad**, este nivel de acceso se aplicará a todas las páginas y portlets que se importen.
¿Desea importar los valores de grupo?	(Si ha elegido importar los valores de seguridad) Seleccione una de las opciones siguientes: ◆ **Sí**: si desea importar los permisos las asignaciones de la página de contenedor por defecto y de la página compartida por defecto que el archivo ZIP de exportación de datos del portal especifica para los grupos. Asegúrese de que los grupos implicados existan en el repositorio seguro de identidades, ya que las asignaciones para los grupos que falten no se podrán importar. ◆ **No**: si desea ignorar las asignaciones de páginas por defecto que el archivo ZIP de exportación de datos del portal especifica para los grupos.
Importar páginas de contenedor Importar páginas compartidas Importar portlets	Siga las instrucciones que aparecen en pantalla para **seleccionar las páginas y portlets** que desee importar desde el archivo ZIP de exportación de datos del portal al portal de destino. **Nota:** Es posible que se importen algunos portlets que no haya seleccionado para importarlos. Si importa una página que contiene un portlet, pero no selecciona dicho portlet para importarlo, el portlet se importará (a fin de que no se produzca un error de tiempo de ejecución para la página importada).
Asigne los nombres de la aplicación de portlet... Archivo de reserva/Local	Utilice los menús desplegables **Archivo de reserva** y **Local** para asignar los nombres de aplicación portlet del archivo de reserva (archivo ZIP de exportación de datos del portal) a aplicaciones portlet existentes del servidor de aplicación (destino) local.

5 Cuando este listo para empezar la importación, haga clic en el botón *Importar datos del portal*.

Cuando finalice la importación, se visualizará el panel *Resultados de la importación de datos del portal*:



Las importaciones que no hayan sido correctas se visualizarán en rojo. Para *resolver los problemas* de importación (o exportación), mire la consola del sistema del servidor de aplicación o el archivo de registro (como jboss/server/IDM/log/server.log) y busque mensajes del *registro* de aplicación de usuario siguiente:

```
com.novell.afw.portal.util
```

Referencia de portlet

IV

En estos capítulos se describe cómo configurar los portlets del sistema y de identidad que se utilizan en la interfaz de usuario del Gestor de identidades.

Acerca de los portlets

15

En este capítulo, se proporciona información acerca de los portlets utilizados en la aplicación de usuario del Gestor de identidades. Los temas son:

Si desea obtener más información acerca de cómo gestionar portlets, consulte Capítulo 9, “Administración de portlets”, en la página 179.

15.1 Portlets accesorios

Los portlets accesorios proporcionan un conjunto diverso de funciones que se pueden añadir a la aplicación de usuario del Gestor de identidades. Los portlets accesorios proporcionan funciones de correo electrónico, de sistema de archivos, etc. Para más información:

Categoría de portlet	Para más información
Correo electrónico Sistema de archivos Varios	Consulte Identity Manager Accessory Portlet Administration Guide (Portlets accesorios del Gestor de identidades: Guía de administración)

15.2 Portlets de administración

Los portlets de la categoría Administración se utilizan para controlar el diseño y contenido de la interfaz de usuario.

Nota: Se recomienda que no utilice ni modifique dichos portlets, ya que proporcionan servicios de marco a la aplicación de usuario.

Los portlets de administración son:

Nombre del portlet	Descripción
Portlet del encabezado	Muestra la pestaña de máximo nivel y la información del encabezado de la interfaz de usuario. No hay preferencias para este portlet.

Nombre del portlet	Descripción
Navegación de páginas compartidas	Muestra un menú que contiene las páginas compartidas de la aplicación de usuario del Gestor de identidades. Las preferencias definen qué se visualizará y cómo. Consulte Sección 15.2.1, “Portlet Navegación de páginas compartidas”, en la página 240.

15.2.1 Portlet Navegación de páginas compartidas

El portlet Navegación de páginas compartidas genera enlaces con las páginas compartidas de la aplicación de usuario del Gestor de identidades. Los valores de preferencia definen los enlaces de la página compartida que se visualizarán. Las preferencias son:

Preferencia	Datos que se deben especificar
sharedpages-sorting	Orden de visualización de las páginas compartidas dentro de una categoría: ascendente o descendente.
sharedpages-sortmode	Cómo se ordenarán las páginas compartidas: alfabéticamente o por orden de prioridad.
sharedpages-category	Especifique una o varias categorías de páginas compartidas. El nombre de la categoría se muestra como un encabezado, con todas las páginas compartidas de dicha categoría visualizadas como enlace. Si una categoría no contiene ninguna página compartida, no se visualizará. Si la página compartida no se encuentra en una categoría, se visualizará como si no tuviera categoría.
guest-category	Especifique una categoría cuyos portlets desee visualizar en la página de acceso al portal. Debe tratarse de una categoría que exista previamente y las páginas contenidas en dicha categoría no deben tener ninguna limitación de lectura de ACL.

15.3 Portlets de identidad

La pestaña Autoservicio de identidades de la aplicación de usuario del Gestor de identidades utiliza los portlets de identidad. Incluyen:

Nombre del portlet	Descripción
Crear	Proporciona una interfaz basada en asistente que habilita a los usuarios para que creen objetos en el repositorio seguro de identidades. Consulte Capítulo 16, “Referencia del portlet de creación”, en la página 243.
Información	Permite que los usuarios visualicen y manipulen la información del atributo de una entidad. Consulte Capítulo 17, “Referencia del portlet de información”, en la página 249.

Nombre del portlet	Descripción
Organigrama corporativo	Permite que los usuarios vean y examinen las relaciones jerárquicas entre los objetos del repositorio seguro de identidades. Consulte Capítulo 18, “Referencia del portlet Organigrama corporativo”, en la página 265.
Lista de búsqueda	Permite que los usuarios busquen objetos en el repositorio seguro de identidades. Consulte Capítulo 20, “Referencia del portlet Lista de búsqueda”, en la página 295.

15.4 Portlets de contraseñas

Los portlets de contraseñas proporcionan la funcionalidad de autoservicio de contraseñas para la aplicación de usuario del Gestor de identidades. Incluyen:

Nombre del portlet	Para más información
Respuesta de verificación de IDM Cambiar contraseña IDM Contraseña olvidada de IDM Definición de sugerencias en IDM Entrada a IDM	Consulte Capítulo 19, “Referencia de los portlets de gestión de contraseñas”, en la página 281

15.5 Portlets del sistema

Los portlets del sistema proporcionan servicios a la aplicación de usuario del Gestor de identidades.

Nota: Se recomienda que no utilice ni modifique dichos portlets en esta categoría.

Los portlets del sistema son:

Nombre del portlet	Descripción
Controlador de páginas de portal	Muestra la página compartida que el usuario tiene actualmente seleccionada mediante el portlet de navegación de páginas compartidas. No hay preferencias para este portlet.

Referencia del portlet de creación

16

En este capítulo se describe cómo utilizar el *portlet de creación* de la aplicación de usuario del Gestor de identidades. Los temas son:

16.1 Acerca del portlet de creación

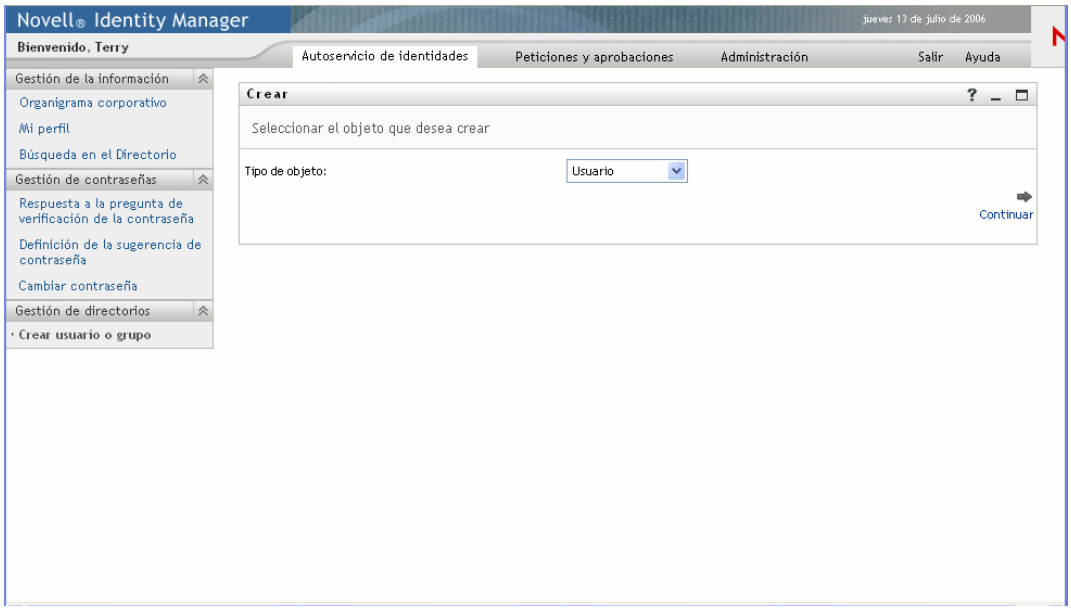
El portlet de creación proporciona un asistente fácil de utilizar que permite a los usuarios crear objetos del repositorio seguro de identidades de diferentes tipos. Las preferencias del portlet controlan:

- Los tipos de objetos que el usuario puede crear.
- Los atributos que el usuario puede suministrar.

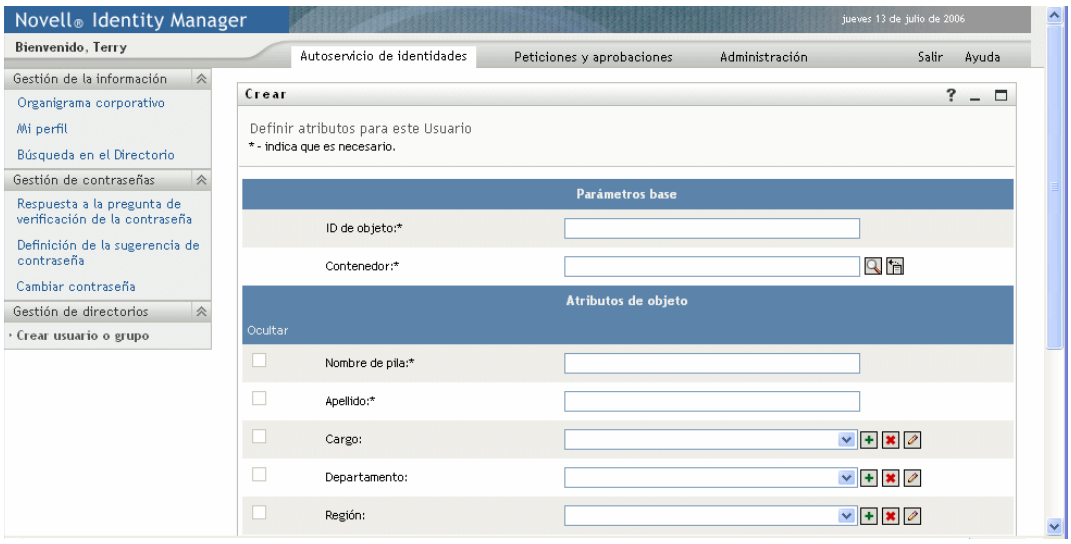
Si desea obtener más información, consulte Sección 16.3, “Configuración de las preferencias de creación”, en la página 246.

La configuración por defecto del portlet de creación (al que se accede mediante la acción *Crear usuario o grupo* de la aplicación de usuario del Gestor de identidades) permite que los usuarios creen un usuario, un grupo o un grupo de tareas. Por defecto, este portlet está restringido al administrador de la aplicación de usuario. En el ejemplo siguiente se muestra cómo el asistente por defecto del portlet de creación solicita al usuario que:

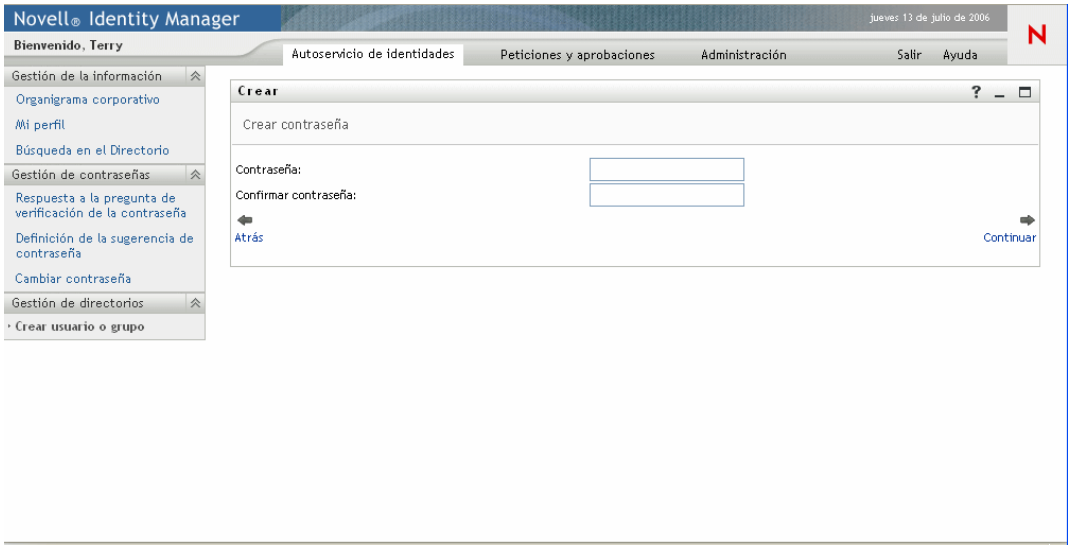
- *Seleccione el tipo de objeto* que se creará:



- *Cumplimente los atributos del objeto*:



- *Solicite una contraseña*, cuando el tipo de objeto la necesite:



  Si se asigna una directiva de contraseña, este portlet visualizará los mensajes de directivas personalizadas.

- *Proporcione un mensaje de tipo informativo,* cuando el objeto se cree correctamente, que enlace con el portlet de información de dicho objeto (asumiendo que el portlet de información tiene la misma configuración) para proseguir la edición.

16.2 Configuración del portlet de creación

Para configurar el portlet de creación:

Paso	Tarea	Descripción
1	Decida si la función Crear usuario o grupo por defecto responde a sus necesidades	En caso afirmativo, no necesitará ejecutar ninguna operación adicional. En caso negativo, deberá ejecutar los pasos restantes.
2	Defina los tipos de objetos que desea permitir que los usuarios creen	Añada los objetos y atributos al nivel de abstracción del directorio. Si desea obtener más información, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75
3	Determine cómo desea que los usuarios accedan a este nuevo portlet	¿Desea que los usuarios lancen este portlet desde una página ya existente o desde una nueva? ¿Qué usuarios pueden acceder al portlet y a la página? Para obtener más información acerca de las páginas, consulte Capítulo 7, “Administración de páginas”, en la página 135.
4	Especifique los usuarios que tienen acceso a la página y a la instancia de portlet	Edite la seguridad de la página y añada los usuarios a la lista. Si desea obtener más información acerca de cómo restringir el acceso de los usuarios a las páginas, consulte Capítulo 7, “Administración de páginas”, en la página 135. Edite la instancia de portlet para cambiar la seguridad. Si desea obtener más información acerca de cómo restringir el acceso de los usuarios a los portlets, consulte Capítulo 9, “Administración de portlets”, en la página 179.
5	Defina las preferencias del portlet	Las preferencias permiten definir: ◆ Qué objetos pueden crear los usuarios. ◆ Qué atributos deben suministrarse durante la creación. Si desea obtener más información, consulte Sección 16.3, “Configuración de las preferencias de creación”, en la página 246.
6	Prueba	Verifique que los objetos se creen y que los atributos se cumplimenten adecuadamente.
7	Establezca los derechos vigentes adecuados en eDirectory para los usuarios finales	Para crear un objeto, el usuario deberá ser **Trustee** de la unidad administrativa y de la organización en la que se crea el objeto.

16.2.1 Configuración del nivel de abstracción del directorio

Los objetos que los usuarios del portlet de creación pueden crear o los atributos que pueden cumplimentar, deben estar definidos en el nivel de abstracción del directorio, tal como se indica a continuación:

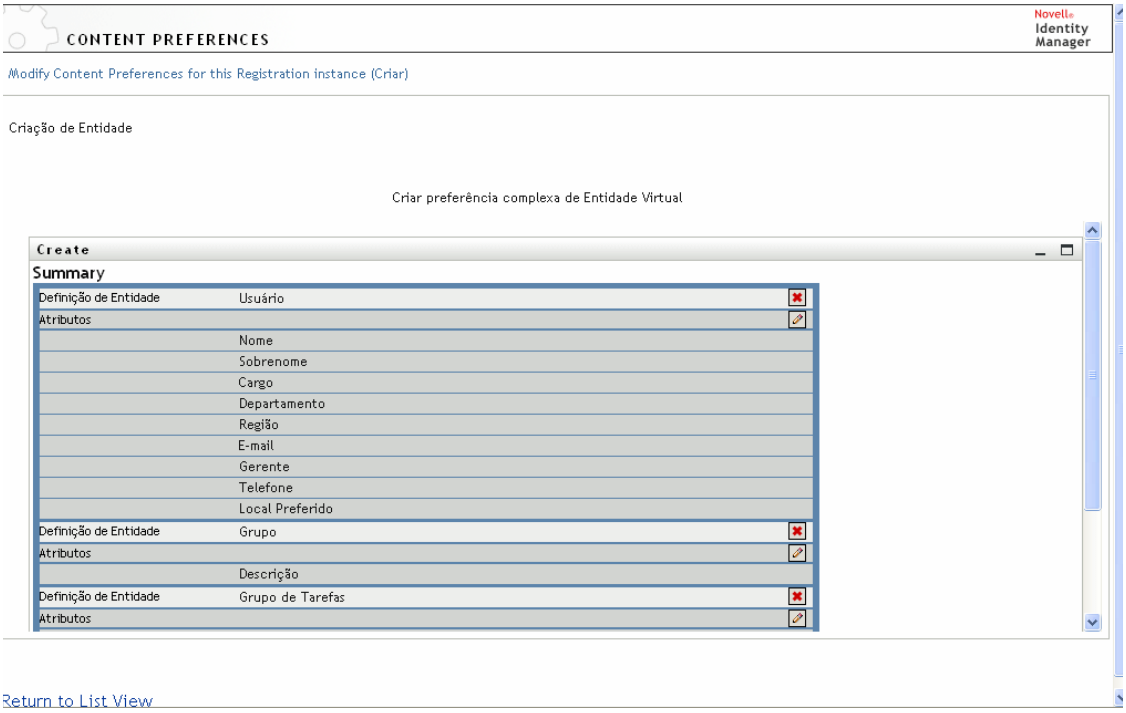
Tipo de definición	Propiedad	Valor
entidad	crear	Seleccionado
	ver	Seleccionado Si no se selecciona, la entidad no se visualizará en la lista de entidades que se pueden crear.
	Contenedor para crear	Especifique un contenedor del repositorio seguro de identidades. Si no se especifica un contenedor válido, se utilizará el contenedor raíz especificado durante la instalación de la aplicación de usuario.
	Contraseña	Seleccionado, si el tipo de entidad necesita una contraseña al crearse. Todos los que tengan acceso a Crear y tengan derechos de Trustee sobre la OU pueden crear usuarios y asignar la **contraseña inicial**. Cuando un usuario nuevo se registra por primera vez, el sistema lo redirige al portlet de cambio de contraseña de IDM, donde modificará la contraseña inicial. Para obtener más información acerca del cambio de contraseña de IDM, consulte Capítulo 15, “Acerca de los portlets”, en la página 239.
atributo	habilitado	Seleccionado
	visualizable	Si no se selecciona habilitado o visualizable (false), el portlet no podrá utilizar el atributo.

Para obtener más información acerca de cómo configurar el nivel de abstracción, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

16.3 Configuración de las preferencias de creación

Mediante la configuración de las preferencias, se pueden configurar los tipos de objetos que un usuario tiene permiso para crear y los atributos que tiene permiso para proporcionar o que debe proporcionar.

Las preferencias del portlet de creación se encuentran en una única página de preferencias personalizada. Cuando se abre, se visualizan las preferencias de creación individuales:



A continuación, se describen las preferencias (o puede hacer clic en el botón Descripciones para visualizar la ayuda en línea de este portlet).

Preferencia	Descripción
Definición de entidad	Nombre del tipo de objeto que se creará. Representa el principio de un bloque de definición de entidad en el que se define cómo el portlet gestionará la operación de creación. **Para restringir objetos:** Los objetos que aparecen en las preferencias complejas se visualizan al usuario en una lista desplegable. Para restringir los objetos que los usuarios pueden crear, elimínelos de esta hoja de preferencias mediante el botón de supresión. **Para añadir otras entidades:** Haga clic en **Añadir definición de entidad** y complete el asistente.

Preferencia	Descripción
Atributos	Controla los atributos que el sistema solicita al usuario que cumplimente. Debe incluir todos los atributos obligatorios del objeto; de lo contrario, la creación real del objeto fallará. Asimismo, las preferencias no se guardarán correctamente si falta un atributo obligatorio. **Para añadir o eliminar un atributo:** ◆ Haga clic en el botón Modificar atributos.  ◆ Para añadir un atributo, selecciónelo (en la lista de atributos disponibles). Puede seleccionar varios atributos con la tecla Ctrl o Mayús. ◆ Haga clic en la flecha para moverlo a la lista Seleccionado. Ejecute la operación inversa para eliminar un atributo. ◆ Para reordenar la lista de atributos, haga clic en las flechas hacia arriba o hacia abajo situadas a la derecha de la lista Seleccionado. Haga clic en **Enviar**. **Atributos y tipos de datos:** El tipo de datos del atributo influye en la forma en que se visualiza. Por ejemplo, si se define un atributo como subtipo de la lista Local o Global, se visualizará en un cuadro de lista. Si desea obtener más información, consulte Sección 4.3, “Funcionamiento de las entidades y los atributos”, en la página 87.

Cumplimentación del panel de preferencias Para verificar que ha enviado entradas válidas, haga clic en *Enviar*. Si una entrada no es válida, verá un mensaje de error en la parte superior de la página de preferencias. Haga clic en *Regresar a la vista de lista* cuando pueda hacer clic en *Enviar* y no se produzca ningún error. Debe hacer clic en *Guardar preferencias* una vez haya regresado a la vista de lista.

Referencia del portlet de información

17

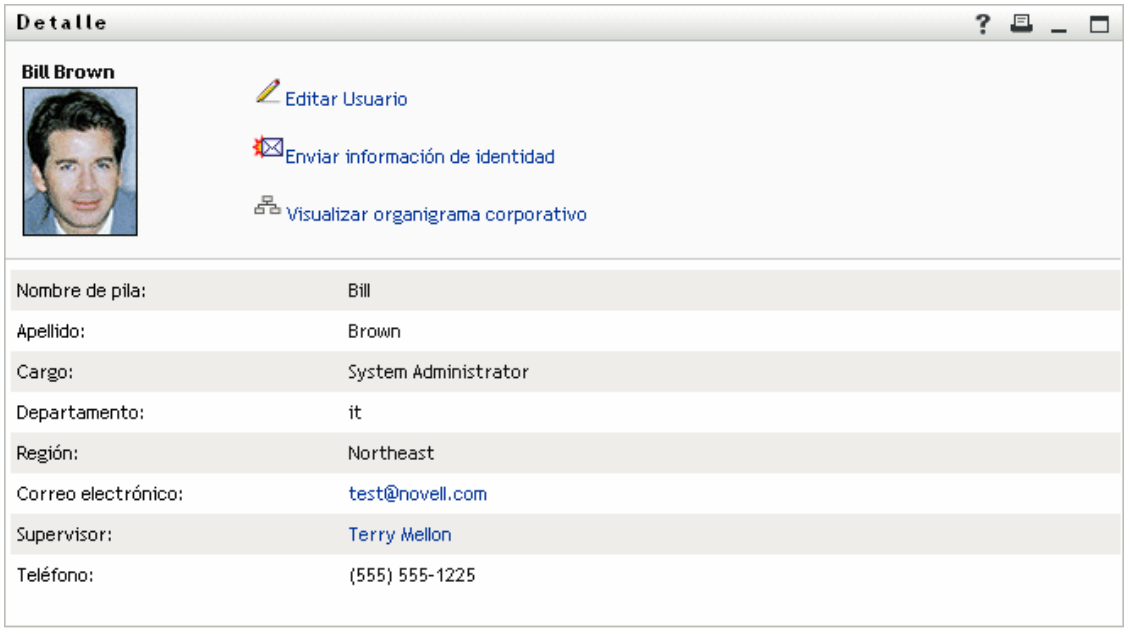
En este capítulo se informa acerca del *portlet de información*, que permite que los usuarios visualicen y manipulen los datos de atributos de una entidad. Se trata de la base de la acción Mi perfil de la pestaña Autoservicio de identidades de la aplicación de usuario del Gestor de identidades. Los temas son:

17.1 Acerca del portlet de información

El portlet de información proporciona a los usuarios una vista detallada de los atributos de una entidad y sus valores. El portlet tiene dos modos: visualización y edición. Cuando los usuarios acceden al portlet de información, pueden aprovechar sus capacidades incorporadas para trabajar con esta información, incluidos:

17.1.1 Visualización de los datos de una entidad

Cuando se accede al portlet de información, éste visualiza los *datos de los atributos de la entidad seleccionada* como un usuario o grupo. Por ejemplo, a continuación indicamos qué puede mostrar el portlet de información cuando el usuario Bill Brown ve su propia información:



Imágenes de usuario Por defecto, el portlet de información está configurado para incluir el atributo Fotografía del usuario. No obstante, si el repositorio seguro de identidades no incluye este atributo o no está cumplimentado, se visualizará una imagen por defecto en el tiempo de ejecución. Si almacena las imágenes del usuario en otra ubicación, puede configurar el portlet para que las visualice.

Si desea obtener más información, consulte “Carga dinámica de imágenes” en la página 253.

Determinación de los atributos que se visualizarán

El portlet de información sólo muestra los atributos que:

- Las definiciones de datos del *nivel de abstracción del directorio*permiten visualizar

  Si desea más información acerca de la configuración de VDD, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

- Están especificados en las *preferencias* de información

  Para obtener información sobre cómo especificar qué atributos se visualizarán en el portlet de información, consulte Sección 17.5, “Configuración de las preferencias”, en la página 260.

- El usuario actual tiene *derechos* para ver

  Por ejemplo, los supervisores con derechos sobre el atributo salario verán dichos datos, mientras que los usuarios restantes no los verán.

  Si desea obtener más información, consulte Sección 17.2.2, “Asignación de derechos a entidades”, en la página 258.

- Están actualmente cumplimentados con un *valor*

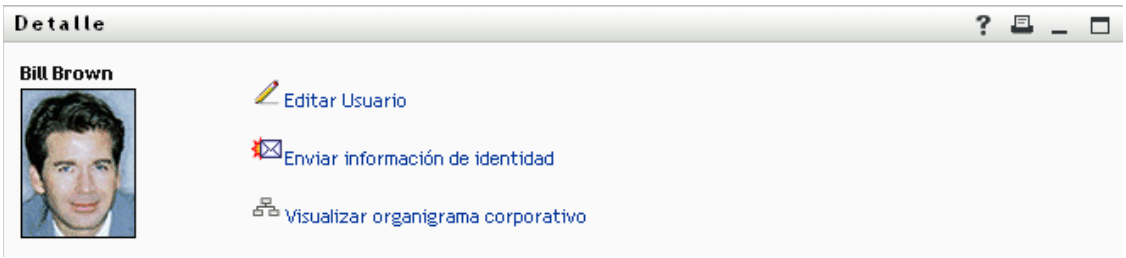
Determinación de cómo se visualizarán los atributos

Cuando se visualicen atributos, el portlet de información *dará formato de texto a los datos*, salvo en los casos siguientes:

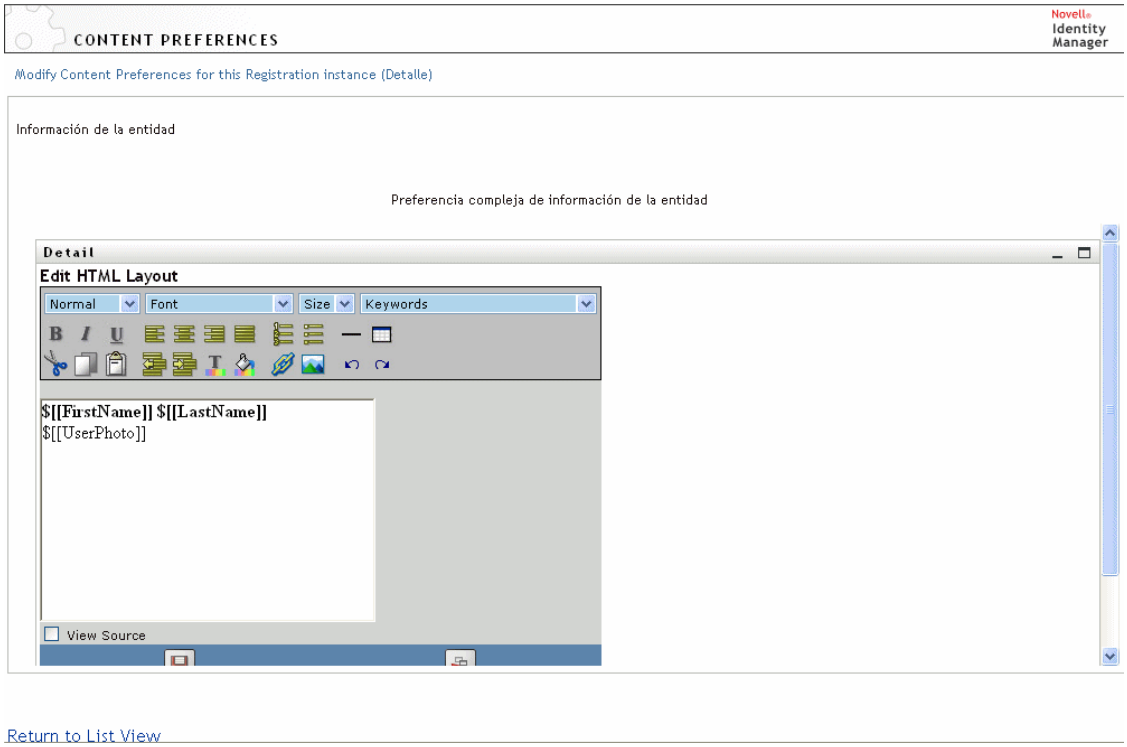
Especificación de formato en la definición del nivel de abstracción	Cómo se visualiza
Formato: correo electrónico	Como un enlace a un correo
Formato: ◆ groupwise-im ◆ aol-im ◆ yahoo-im	Como un icono que inicia una charla y añade dicho usuario
Tipo de datos: binario **Formato:** imagen	Como botón y como enlace para ver la imagen
Tipo de datos: booleano	Como botones circulares inhabilitados que indican true o false Los botones se visualizan sin indicar un valor por defecto, ya que el atributo no se crea realmente para el usuario hasta que se especifica un valor.
Multivalente:seleccionado	Como conjunto repetitivo de controles para editar, añadir y eliminar valores de atributo individuales (en forma de lista separada con comas)
Tipo de control:DNLookup	Como enlace En el ejemplo anterior, un enlace (`Terry Mellon`) se visualiza para acceder a los datos de información del supervisor de Bill Brown.
Tipo de control: ◆ Lista local ◆ Lista global	Como etiqueta de visualización en vez del valor (clave) actual Por ejemplo, el atributo EmployeeType visualiza `Tiempo completo`, en vez del valor real `ft`.

Determinación de qué visualizará el área de título

Puede diseñar el área de título del portlet de información utilizando funciones HTML estándar:



Las preferencias de información proporcionan un *Editor de diseño HTML* que puede utilizar para crear la apariencia y contenido que desee:



Utilización del editor de diseño HTML

El editor de diseño HTML proporciona las funciones típicas de un editor HTML para definir el formato de texto y las listas, especificar anclajes e imágenes, etc.

Palabras clave Cuando diseñe la disposición, puede utilizar la lista desplegable de palabras clave para insertar variables dentro del área de título del portlet de información que, en el tiempo de ejecución, se sustituirán por valores de atributo específicos. También puede escribirlas utilizando la sintaxis siguiente:

```
$[[palabra clave]]
```

Donde *palabra clave* es el valor de un atributo como LastName.

Puede concatenar atributos utilizando la sintaxis siguiente:

```
$[[palabra clave+palabra clave]]
```

Por ejemplo:

```
$[[FirstName+LastName]]
```

Puede concatenar tantos atributos como desee e incluir cadenas entre comillas como se indica a continuación:

```
$[[palabra clave+”texto de ejemplo”+palabra clave]]
```

De esta manera, los valores de las palabras clave y del texto entre comillas se procesarán.

Nota: Cuando una palabra clave está mal escrita en un diseño, en el tiempo de ejecución se procesará tal cual (incluido $[[]]).

Carga dinámica de imágenes Para visualizar imágenes, como fotografías del usuario, que están almacenadas en el repositorio seguro de identidades, puede añadir el nombre del atributo mediante el editor de diseño HTML. Por ejemplo, si añade el atributo User Photo, se visualizará la fotografía del usuario. Si almacena imágenes fuera del repositorio seguro de identidades, necesitará utilizar la etiqueta IMG: (desde el *modo Ver origen* del editor de HTML) tal como se indica a continuación:

1. Vaya a las preferencias del portlet y acceda al editor de HTML.
2. Haga clic en *Ver origen*.
3. Utilice la etiqueta IMG: para combinar una ubicación, una clave de atributo y una extensión de archivo, mediante una sintaxis como la que indicamos a continuación:

   ```
   $[[IMG:”URL” + nombre-clave-atributo + ”extensión_archivo”]]
   ```

En el ejemplo siguiente, se muestra la sintaxis que deberá utilizar si ha almacenado fotografías del empleado como imágenes JPG, según el apellido, en el subdirectorio de imágenes del servidor de la aplicación:

```
$[[IMG:"http://mihost:8080/images/"+LastName+".jpg"]]
```

En el tiempo de ejecución, el portlet concatenará la URL con el atributo LastName y la extensión de archivo .jpg.

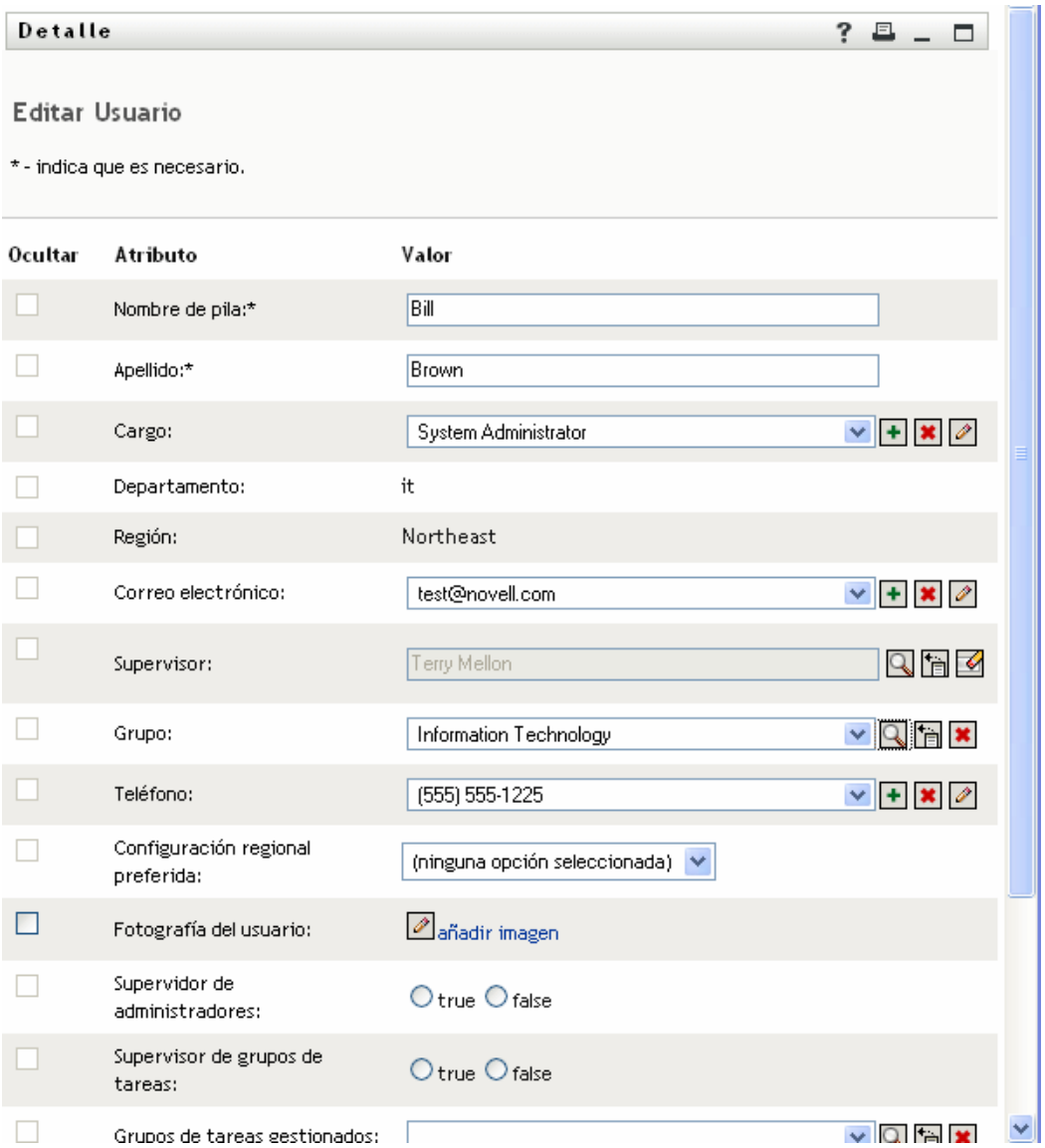
Tenga en cuenta que el editor de HTML admite una sintaxis flexible y es compatible con cualquier combinación de texto y atributos, por lo que la sintaxis es:

```
$[[IMG:”texto” + nombre-clave-atributo + ...]]
```

17.1.2 Edición de los datos de una entidad

El portlet Información proporciona automáticamente un enlace de *edición* (como *Editar su información* o *Editar usuario* o *Editar dispositivo*) para pasar del modo de visualización al modo de edición. Esto permite que los usuarios con derechos adecuados para la entidad actual cambien sus valores de atributo y guarden dichos cambios.

Por ejemplo, a continuación indicamos qué mostrará el portlet Información cuando el usuario Bill Brown (que tiene los derechos necesarios) edite su propia información:



Nota: En el caso de los atributos booleanos, cuando los dos botones circulares no estén seleccionados, el atributo no existirá para el usuario. Si selecciona el botón circular *true* o *false* creará el atributo para el usuario y definirá su valor.

Determinación de los atributos que se visualizarán

En el modo de edición, el portlet Información muestra únicamente los atributos que:

- Las definiciones de datos del *nivel de abstracción del directorio*permiten visualizar

  Si desea más información acerca de las definiciones de datos, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

- El usuario actual tiene *derechos* para ver

Por ejemplo, los supervisores con derechos sobre el atributo salario verán dichos datos, mientras que los usuarios restantes no los verán.

Si desea obtener más información, consulte Sección 17.2.2, “Asignación de derechos a entidades”, en la página 258.

Un atributo debe cumplir todos los criterios anteriores, para poder visualizarse en modo de edición.

Determinación de cómo se visualizarán los atributos

En el modo de edición, el portlet Información da formato a todos los atributos editables como un *cuadro de texto*, salvo en los casos siguientes:

Especificación del tipo de atributo (en archivos VDD)	Cómo se visualiza
Tipo de datos: binario Formato: imagen	Como un botón y enlace en el portlet de carga de la imagen de la entidad para visualizar, actualizar o añadir la imagen
Tipo de datos: booleano	Como botones circulares que indican true o false
ocultar: Seleccionado	Como casilla de verificación etiquetada Ocultar
multivalor=Seleccionado	Como un conjunto de controles para editar, añadir o eliminar valores del atributo
Tipo de control: DNLookup	Como un botón para iniciar el portlet de lista de parámetros para buscar y seleccionar un DN
Tipo de control: ◆ Lista local ◆ Lista global	Como una lista desplegable (que permite efectuar varias selecciones, si es preciso)

Los atributos que no se pueden editar (ya sea por definición o por derechos de usuario inadecuados) se visualizan como *inhabilitados* o *de sólo lectura*.

Validación de los cambios

Durante la edición, la validación de datos se efectúa automáticamente para las especificaciones de tipos de atributo siguientes:

- Formato: correo electrónico
- Tipo de datos: entero
- Tipo de control: rango

Cuando utilice un tipo de control de lista local o global, es posible que la lista visualizada incluya valores que no entren dentro de los límites especificados de un atributo. No obstante, dichos valores se marcarán como fuera de rango, y la validación evitará que se envíen.

Definición de una entidad Mi perfil por defecto

Cuando defina una entidad en el nivel de abstracción del directorio, puede especificar un valor para *Entidad Mi perfil por defecto*(en el elemento de configuración del editor del nivel de abstracción del directorio) para especificar que debe utilizarse otra definición de la entidad para la edición. Cuando

pase del modo de visualización al modo de edición, el portlet Información siempre comprueba si éste está especificado y utiliza la definición de entidad adecuada para presentar los atributos.

Por ejemplo, supongamos que la definición de entidad para Estudiante incluye *usuario* como el valor de *Entidad Mi perfil por defecto*. En dicho caso, la modalidad de visualización utilizará la definición de la entidad Estudiante, pero el modo de edición utilizará la definición de entidad del usuario.

17.1.3 Envío por correo electrónico de datos de una entidad

El portlet Información proporciona automáticamente un enlace llamado *Enviar información de identidad*. Los usuarios pueden hacer clic en él para enviar por correo electrónico la URL de la Información de la entidad actual a uno o varios usuarios. Como se envía la URL de la Información, en vez de enviar la información real, la seguridad se mantiene (ya que todos los que reciben la URL deben tener una autorización adecuada para utilizarla).

17.1.4 Enlace con un organigrama corporativo

El portlet Información proporciona automáticamente un enlace llamado *Visualizar organigrama corporativo*. Los usuarios pueden hacer clic en él para visualizar el portlet Organigrama corporativo de la entidad actual.

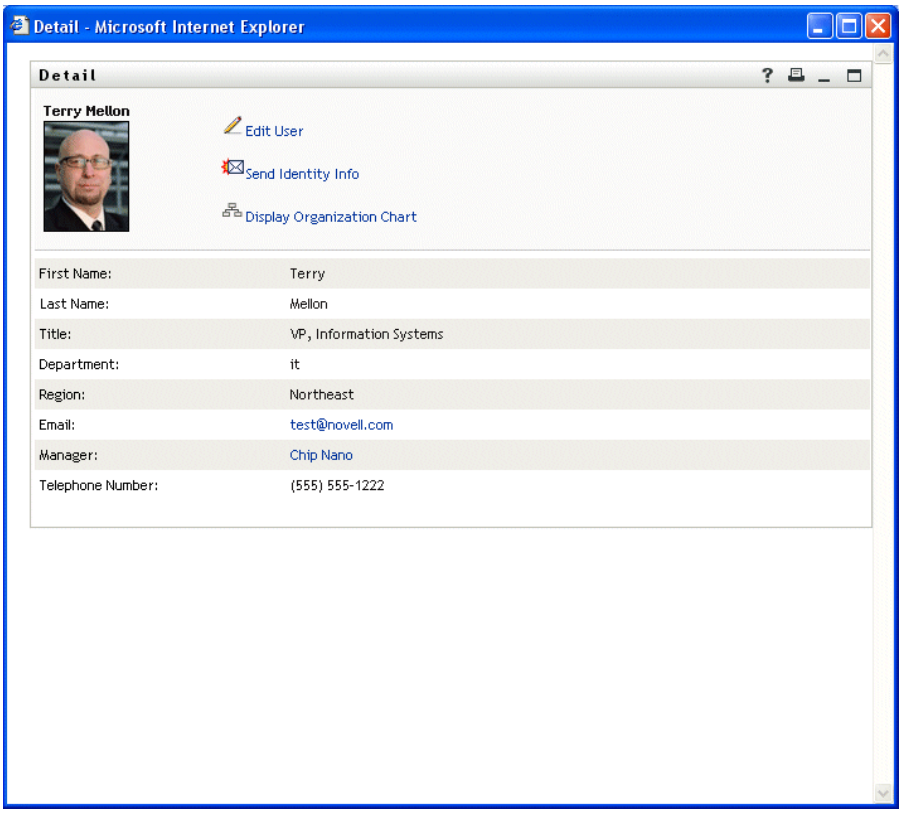
Por ejemplo, si está visualizando Información del usuario Bill Brown y hace clic en este enlace, se visualizará:

Para obtener más información acerca del portlet Organigrama corporativo, consulte Capítulo 18, “Referencia del portlet Organigrama corporativo”, en la página 265.

17.1.5 Enlace con la información de otras entidades

Cuando configure el portlet Información, es posible que desee que los usuarios puedan enlazarse con entidades relacionadas desde la entidad actual. Para ello, puede incluir los atributos que están definidos (en el nivel de abstracción del directorio) con el *tipo de control DNLookup* .

Cuando visualice el atributo Manager en la Información de un usuario, aparecerá como un *enlace*. Si hace clic en dicho enlace, se visualizará la Información del Supervisor.



Para obtener más información acerca del nivel de abstracción del directorio , consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

Para obtener información sobre cómo especificar qué atributos se visualizarán en el portlet Información, consulte Sección 17.5, “Configuración de las preferencias”, en la página 260.

17.1.6 Impresión de los datos de una entidad

Por defecto, los valores de visualización del portlet Información habilitan la opción *Imprimir* en la barra de título del portlet. Si mantiene dicha opción habilitada, los usuarios podrán hacer clic en ella para visualizar una versión de fácil impresión del contenido de la Información:

Para cambiar este u otros valores del portlet Información, utilice la pestaña Administración para actualizar el Registro de portlet de *DetailPortlet* (en la página de Administración del portlet).

Si desea obtener más información, consulte Capítulo 9, “Administración de portlets”, en la página 179.

17.2 Requisitos previos

Antes de empezar a utilizar el portlet Información, deberá tener conocimientos sobre:

- Sección 17.2.1, “Configuración del nivel de abstracción del directorio”, en la página 258
- Sección 17.2.2, “Asignación de derechos a entidades”, en la página 258

17.2.1 Configuración del nivel de abstracción del directorio

El portlet Información depende de las definiciones del *nivel de abstracción del directorio* de diferentes formas. En las secciones siguientes de este capítulo, se proporcionan instrucciones acerca de cómo configurar las definiciones de datos del nivel de abstracción para dar soporte a funciones específicas del portlet Información:

- Sección 17.1.1, “Visualización de los datos de una entidad”, en la página 250
- Sección 17.1.2, “Edición de los datos de una entidad”, en la página 253
- Sección 17.4, “Utilización del portlet Información en una página”, en la página 260

Si desea más información acerca de la configuración, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

17.2.2 Asignación de derechos a entidades

Para poder acceder a una entidad y a sus atributos en el portlet Información, los usuarios deben tener los *derechos adecuados asignados en eDirectory*:

Para realizar esta operación	El usuario necesita este derecho
Visualizar un atributo	Lectura
Editar un atributo	Escritura

Se pueden asignar derechos especificando que un usuario es un *Trustee* de un objeto (entidad) y, a continuación, especificar qué derechos se asignarán a qué atributos.

17.3 Inicio del portlet Información desde otros portlets

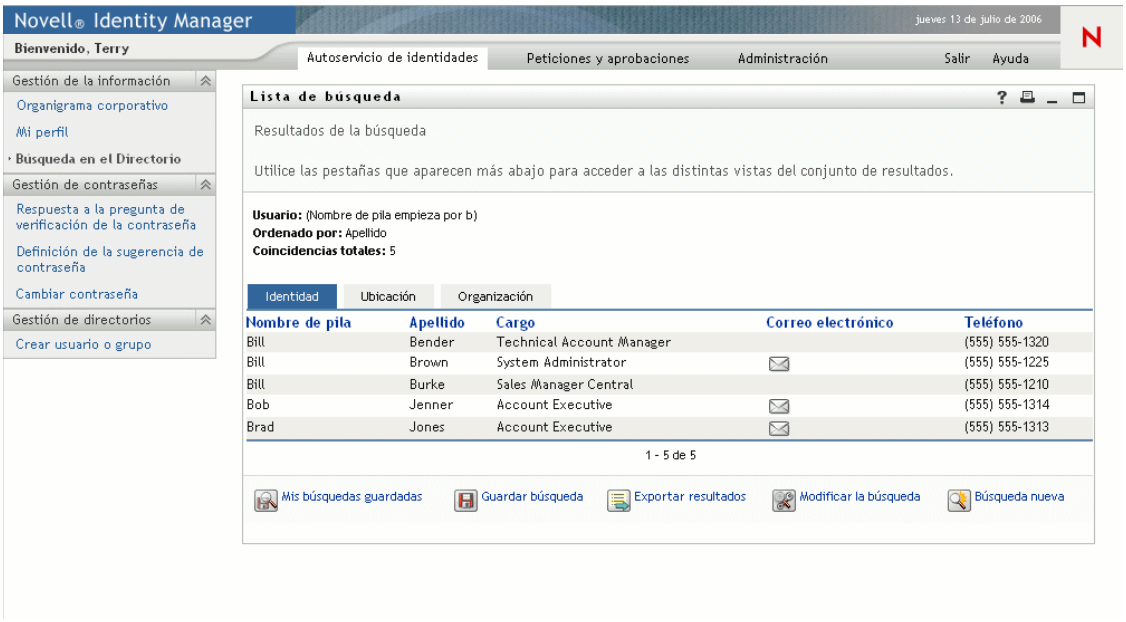
El portlet Información se suele iniciar después de seleccionar una entidad en uno de los otros portlets de identidad. El portlet Información se puede iniciar:

- Sección 17.3.1, “Desde el portlet Lista de búsqueda”, en la página 258
- Sección 17.3.2, “Desde el portlet Organigrama corporativo”, en la página 259

17.3.1 Desde el portlet Lista de búsqueda

En el portlet Lista de búsqueda, los usuarios pueden *hacer clic en la fila de una entidad* de los resultados de la búsqueda, para visualizar la Información de dicha entidad. Por ejemplo, si hace clic

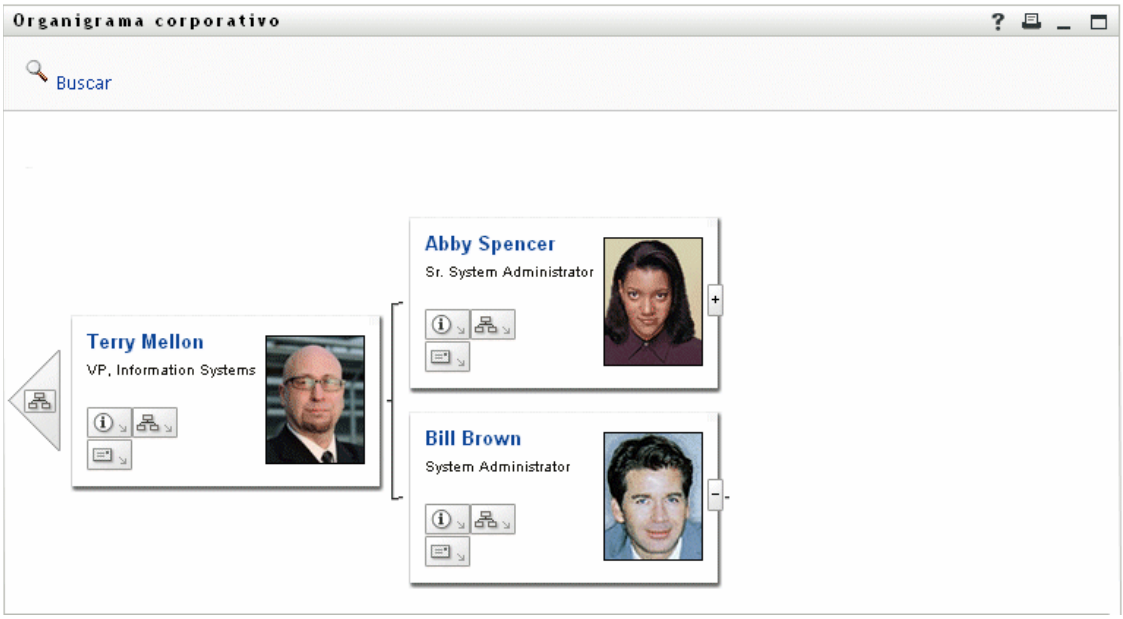
en la fila Bill Brown de la lista siguiente, se visualizará el portlet Información con sus datos de atributos:



Para obtener más información acerca del portlet Lista de búsqueda, consulte Capítulo 20, “Referencia del portlet Lista de búsqueda”, en la página 295.

17.3.2 Desde el portlet Organigrama corporativo

En el portlet Organigrama corporativo, los usuarios pueden hacer clic en el *icono Acciones de identidad* de una entidad y seleccionar *Mostrar información* para visualizar la información de la entidad. Por ejemplo, si hace clic en Mostrar información de Bill Brown en el organigrama corporativo siguiente, se visualizará el portlet Información con sus datos de atributos:

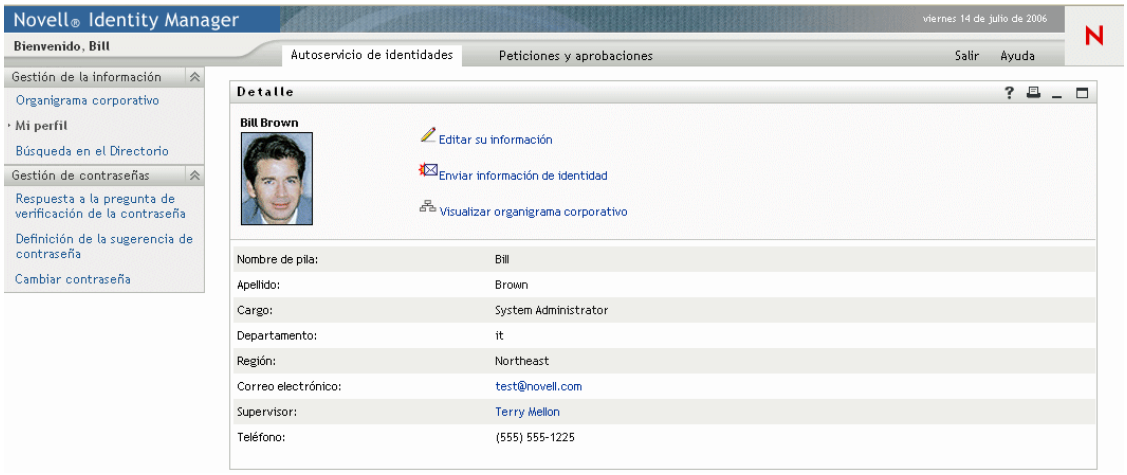


Para obtener más información acerca del portlet Organigrama corporativo, consulte Capítulo 18, “Referencia del portlet Organigrama corporativo”, en la página 265.

17.4 Utilización del portlet Información en una página

Si desea que los usuarios puedan visualizar o incluso editar ellos mismos los datos de sus atributos, añada el portlet Información a una *página compartida*. Cuando dicho portlet se utiliza en una página compartida, accede automáticamente a los datos del usuario actual (o a otra entidad por defecto).

Por ejemplo, el usuario Bill Brown puede registrarse e ir a la página personal siguiente para mantener su propia información a través del portlet Información:



Para determinar qué definición de entidad va a utilizar el portlet Información en esta situación (es decir, cuando se accede a él desde una página y no lo inicia otro portlet), especifique el valor *Por defecto ‘Mi perfil’ Entidad* del elemento Configuración del nivel de abstracción del directorio.

17.5 Configuración de las preferencias

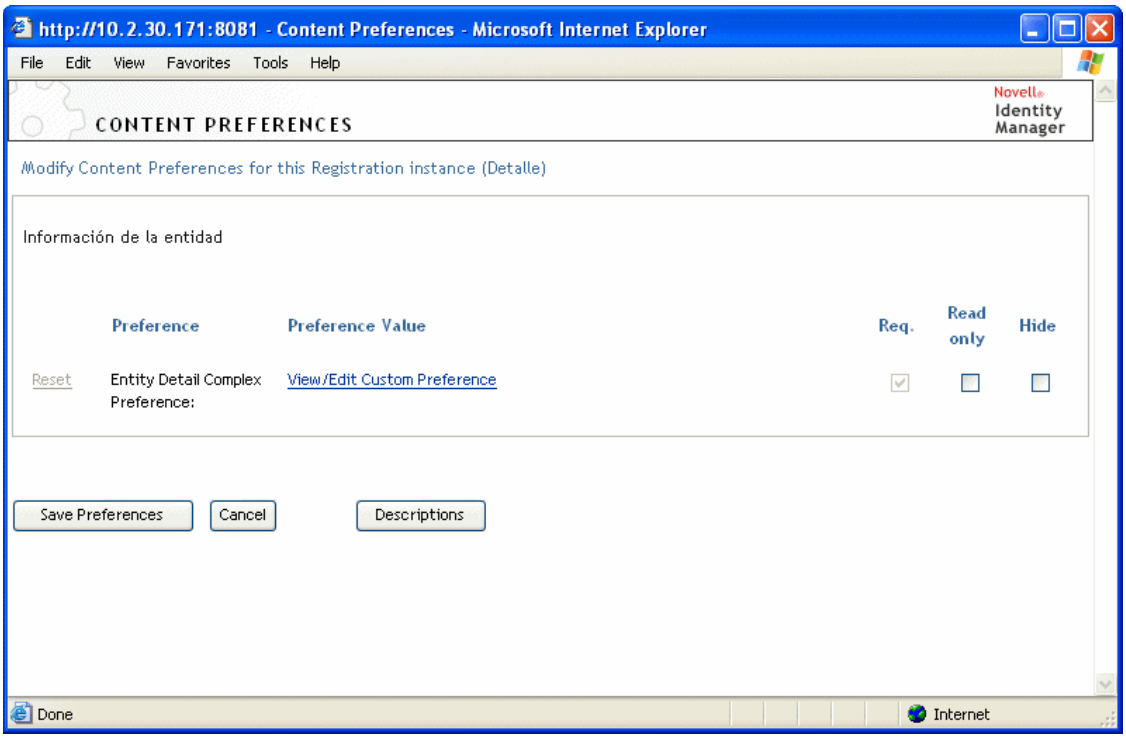
Las preferencias se definen para ajustar el contenido y la apariencia del portlet Información. La forma de utilización del portlet Información, determinará dónde definirá sus preferencias:

Para obtener información acerca de cómo acceder a las preferencias de portlet desde una página compartida o una página de contenedor, consulte Capítulo 7, “Administración de páginas”, en la página 135.

Para obtener información acerca de cómo acceder a las preferencias de portlet de un registro de portlet, consulte Capítulo 9, “Administración de portlets”, en la página 179.

17.5.1 Acerca de las preferencias

Las preferencias del portlet Información están todas contenidas en una única *Preferencia compleja Información*:



Cuando abre esta preferencia compleja, se presentan las preferencias individuales del portlet Información:

Dichas preferencias *se aplican únicamente en el modo de visualización* (y no en el modo de edición). Incluyen los elementos siguientes:

Preferencia	Información
Definición de entidad	Especifica la lista de atributos y el diseño HTML que se visualizará cuando se utilice el portlet Información para un tipo de entidad concreto (como Usuario, Dispositivo o Grupo). Puede hacer clic en **Añadir definición de entidad** para especificar el soporte del portlet Información a tipos de entidad adicionales.
Atributos que se visualizarán como una lista	Especifica qué atributos de la entidad seleccionada desea que el portlet visualice. Dichos atributos se listarán en el orden que seleccione. Se proporciona un botón para que pueda añadir o eliminar atributos según sus necesidades.

Preferencia	Información
Diseño HTML	Proporciona un botón para abrir el **editor de diseño HTML**, en el que puede diseñar el área de título que el portlet Información visualizará para la entidad seleccionada. Para obtener información detallada, consulte “Determinación de qué visualizará el área de título” en la página 251.

Referencia del portlet Organigrama corporativo

18

En este capítulo se informa acerca de cómo modificar funciones del organigrama corporativo ya existentes o cómo añadirle funciones nuevas en la aplicación de usuario del Gestor de identidades. Los temas son:

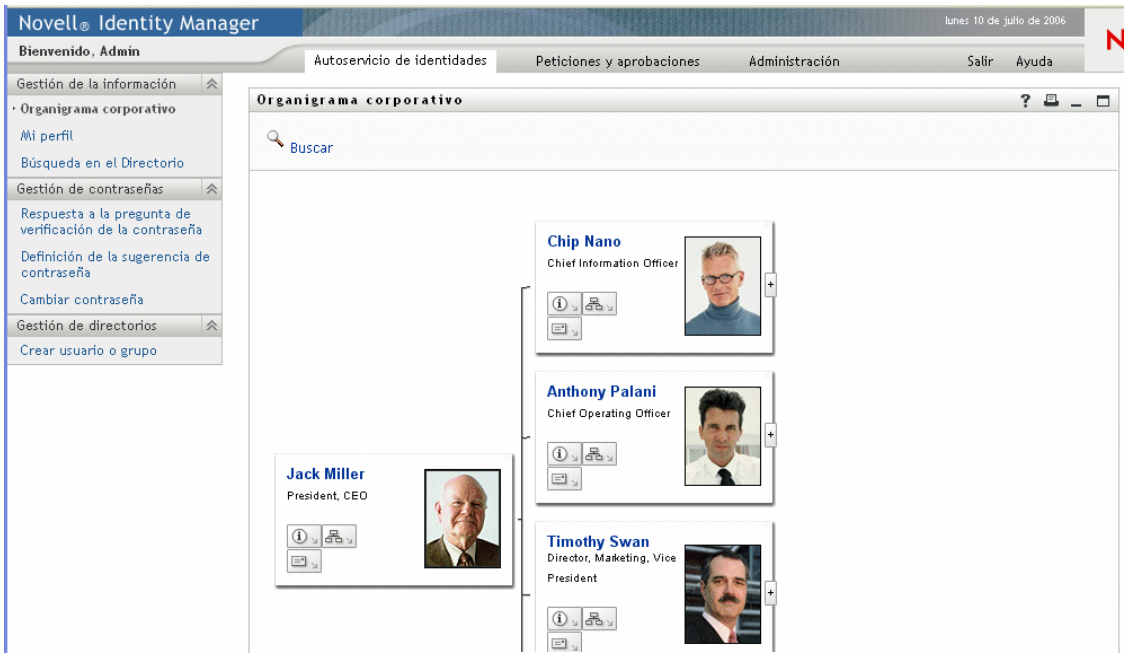
18.1 Acerca del organigrama corporativo

El portlet Organigrama corporativo permite que los usuarios finales vean y examinen la representación gráfica de las relaciones jerárquicas entre objetos del repositorio seguro de identidades. Por ejemplo, puede definir portlets Organigrama corporativo que muestren la jerarquía de:

- Una organización (como empleados y supervisores)
- La pertenencia a un grupo (como todos los empleados de un grupo)
- Los dispositivos asignados a un usuario (como los móviles y portátiles)

La configuración por defecto de la pestaña Autoservicio de identidades de la aplicación de usuario del Gestor de identidades incluye una acción Organigrama corporativo. Dicha acción es un portlet Organigrama corporativo configurado para mostrar las relaciones entre objetos de usuario del

repositorio seguro de identidades. En el ejemplo siguiente se muestra cómo el portlet Organigrama corporativo procesa esta relación (con datos de ejemplo).



Enlaces incorporados El portlet Organigrama corporativo incluye estos enlaces incorporados.

Enlace	Descripción
	Permite que el usuario navegue hasta el siguiente nivel superior. This is only available when viewing a relationship where the parent and child entities are the same.Sólo está disponible cuando se visualiza una relación en el que las entidades padre e hijo son las mismas.Inicia el portlet Información. Este enlace incorporado se puede configurar a través de las preferencias de diseño del organigrama corporativo descritas en “Preferencias de diseño del organigrama corporativo” en la página 274
	Visualiza una lista de organigramas corporativos. Permite que los usuarios seleccionen un organigrama corporativo para visualizarlo. Esta lista de organigramas corporativos es dinámica. Visualiza también otros organigramas corporativos que comparten el mismo tipo de entidad padre. Por ejemplo, si está visualizando un organigrama corporativo de supervisor y empleado (la entidad padre es usuario) y hace clic en este icono, la lista de organigramas corporativos que podrá ver sólo contendrá las relaciones en las que la entidad padre sea también usuario. Este enlace incorporado se puede configurar a través de las preferencias de diseño del organigrama corporativo descritas en “Preferencias de diseño del organigrama corporativo” en la página 274

Enlace	Descripción
	Inicia una herramienta de correo electrónico para: ◆ Enviar la información de entidad del usuario seleccionado actualmente ◆ Componer un mensaje de correo electrónico Este enlace incorporado se puede configurar a través de las preferencias de diseño del organigrama corporativo descritas en “Preferencias de diseño del organigrama corporativo” en la página 274
	El enlace Buscar permite que los usuarios realicen búsquedas de entidades. El resultado de la búsqueda hace que la entidad encontrada se convierta en el nodo superior del organigrama visualizado.
	Permite que los usuarios detallen al nivel siguiente.

Si desea más información acerca de cómo añadir y restringir los enlaces incorporados de sus organigramas corporativos, consulte “Preferencias de diseño del organigrama corporativo” en la página 274.

18.1.1 Acerca de las relaciones de los organigramas corporativos

El portlet Organigrama corporativo visualiza las relaciones que están definidas en el nivel de abstracción del directorio. Las relaciones siguientes están disponibles después de instalar la aplicación de usuario del Gestor de identidades.

- Pertenencia a grupo
- Supervisor-empleado
- Grupos de usuarios

Si desea saber más acerca de cómo crear o modificar relaciones de organigramas corporativos, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

Nota: Los grupos dinámicos no son totalmente compatibles con el portlet del organigrama corporativo. Un grupo dinámico no se puede definir como entidad padre de una relación, si bien se puede definir como entidad hijo de una relación.

18.1.2 Acerca de la visualización de los organigramas corporativos

Por defecto, el organigrama corporativo se visualiza en el marco del portlet, dentro de un área definida por las preferencias de altura y anchura de éste. Si el contenido necesita más espacio que el área definida, los límites del portlet se ampliarán, al igual que la altura y anchura de la página. Los usuarios pueden visualizar completamente un organigrama corporativo haciendo clic en el icono de maximización disponible en la barra de título del portlet. (Por defecto, el organigrama corporativo se visualiza en modo maximizado completo, cuando lo inicia el portlet Información).

Imágenes de usuario Por defecto, el diseño del organigrama corporativo del objeto Usuario incluye el atributo Fotografía del usuario. No obstante, si el repositorio seguro de identidades no incluye este

atributo o no está cumplimentado, el organigrama corporativo omitirá este atributo en el tiempo de ejecución. Si almacena las fotografías en otra ubicación, puede configurar el organigrama corporativo para visualizar dichas fotografías.

Si desea obtener más información, consulte Sección 18.2.3, “Carga dinámica de imágenes”, en la página 279.

18.2 Configuración del portlet Organigrama corporativo

Para configurar el portlet del organigrama corporativo, deberá:

Paso	Tarea	Descripción
1	Definir la relación que desee visualizar.	Puede utilizar una de las relaciones predefinidas que se instalan con la aplicación de usuario del Gestor de identidades o puede crear sus propias relaciones. Si desea obtener más información acerca de cómo definir una relación, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.
2	Verifique que las entidades y atributos que desee utilizar en la relación estén disponibles en el nivel de abstracción del directorio.	Si desea obtener más información acerca de cómo definir una relación, consulte Sección 18.2.1, “Configuración del nivel de abstracción del directorio”, en la página 269.
3	Determine dónde desea visualizar esta relación	¿Desea crear una página nueva para iniciar el organigrama corporativo? ¿O bien desea iniciarlo desde el portlet Información u otro organigrama corporativo? Si desea obtener más información acerca de cómo crear páginas y añadir portlets a dichas páginas, consulte Capítulo 7, “Administración de páginas”, en la página 135.
4	Defina las preferencias del portlet	Las preferencias permiten definir: ◆ Qué atributos se visualizarán ◆ Cómo se visualizarán (su diseño HTML) Si desea obtener más información, consulte Sección 18.2.2, “Configuración de las preferencias del organigrama corporativo”, en la página 269.
5	Prueba	Pruebe las definiciones de relaciones y el diseño

Paso	Tarea	Descripción
6	Defina los derechos de eDirectory y establezca los índices que sean necesarios para mejorar el rendimiento	**Derechos vigentes**: para visualizar los atributos definidos por el portlet, los usuarios han de tener derechos de **Lectura** sobre los atributos. **Mejora del rendimiento:** el rendimiento de la visualización del organigrama corporativo se puede mejorar añadiendo un índice de valor de eDirectory al atributo hijo de la relación, ya que dicho atributo se utiliza para realizar una búsqueda LDAP.

18.2.1 Configuración del nivel de abstracción del directorio

Las entidades y atributos que se visualizan en un organigrama corporativo han de estar definidas en el nivel de abstracción del directorio. La tabla siguiente muestra los atributos y propiedades que deben definirse para cada entidad y atributo visualizado en un organigrama corporativo.

Tipo de definición	Configuración	Valor
entidad	ver	Seleccionado (true)
atributo	lectura	Seleccionado (true)
	buscar	Seleccionado (true)

Requisitos del enlace Buscar El enlace Buscar permite que los usuarios naveguen por el organigrama corporativo mediante búsquedas de otros objetos del mismo tipo como la clave de entidad padre. Para ello, es preciso que la clave de entidad padre tenga, como mínimo, un atributo con las propiedades de acceso *obligatorio* y *buscar* definidas en true (seleccionadas en el editor del nivel de abstracción del directorio). De lo contrario, el diálogo Búsqueda de objetos del enlace Buscar no podrá cumplimentarse y visualizará un diálogo vacío.

Si desea obtener más información acerca de la configuración de entidades y atributos, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

18.2.2 Configuración de las preferencias del organigrama corporativo

Se definen dos tipos de preferencias:

- “Preferencias de relación de los organigramas corporativos” en la página 270
- “Preferencias de diseño del organigrama corporativo” en la página 274

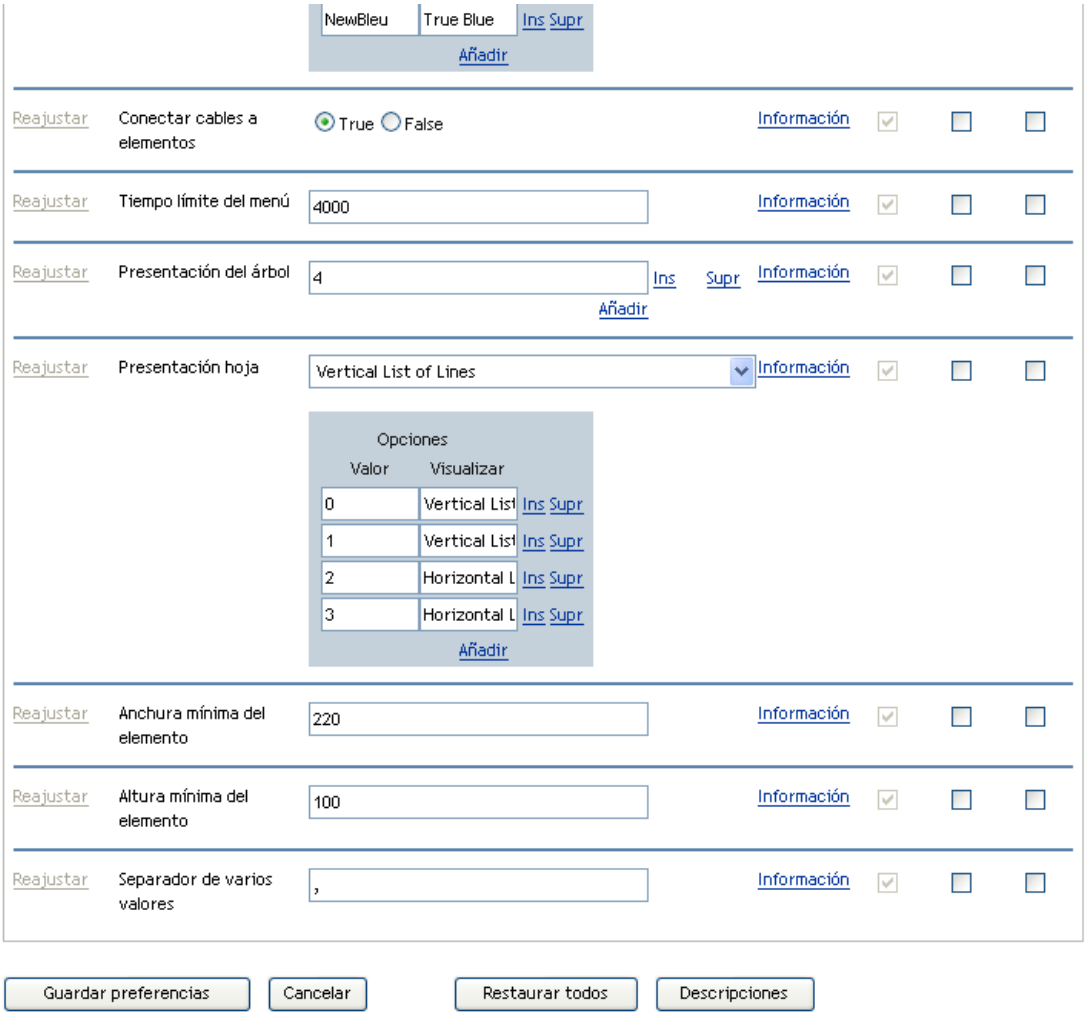
Preferencias de relación de los organigramas corporativos

Las preferencias de relación de los organigramas corporativos están contenidas en una única página de preferencias.

.

.

.



Preferencia	Operaciones que puede realizar
Diseños de presentación	Haga clic en Ver/Editar preferencia personalizada para acceder a las preferencias de diseño. Están descritas en “Preferencias de diseño del organigrama corporativo” en la página 274.
Clave de relación	Introducir la clave de relación. Este valor debe corresponder con una de las claves de relación especificadas en el nivel de abstracción del directorio.

Preferencia	Operaciones que puede realizar

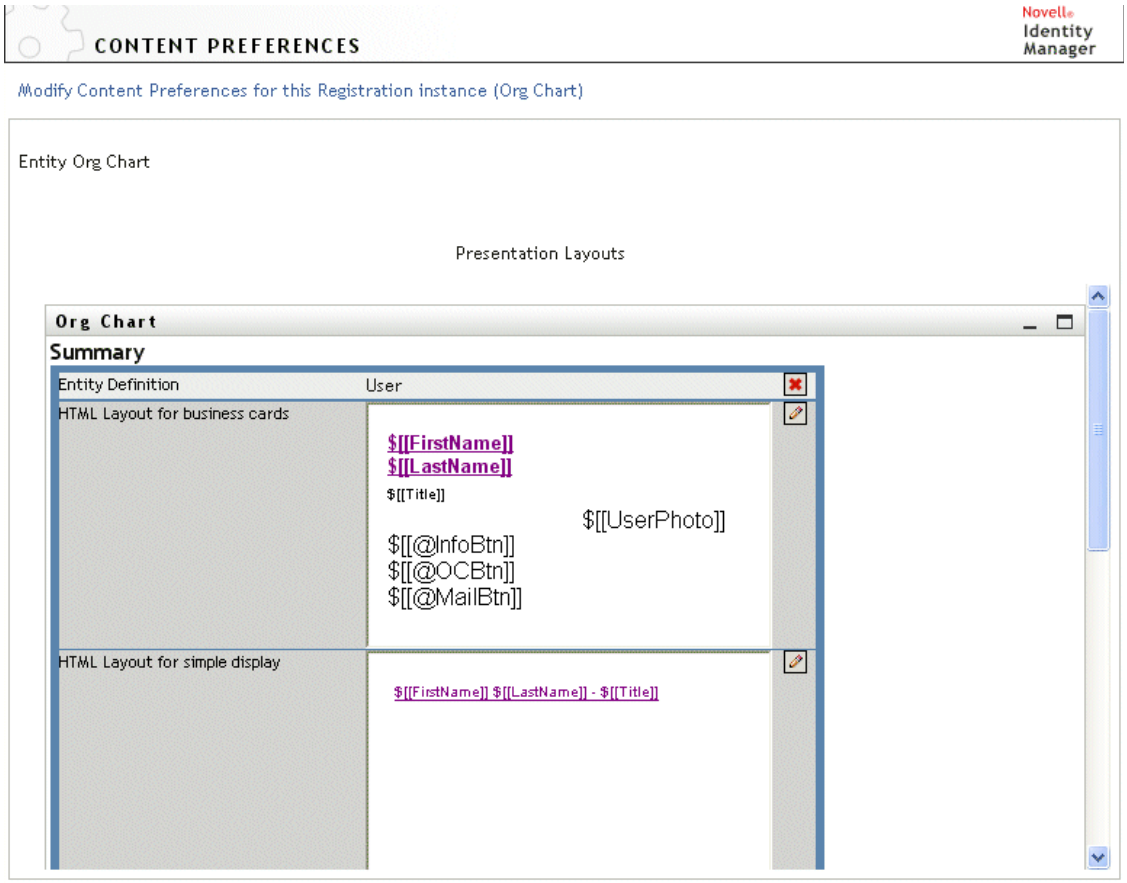
Clave de entidad Padre	Escriba el DN de la entidad que representa el nodo raíz del organigrama corporativo que desea visualizar o, para visualizar el organigrama corporativo del usuario actual, escriba ${User/id}. (El parámetro ${User/id} determina el DN del usuario actual).
	
	Este valor debe estar dentro de los nodos especificados por la propiedad raíz-búsqueda del nivel de abstracción del directorio o la búsqueda LDAP fallará.
	
	A continuación mostramos algunos ejemplos de DN válidos (con datos de ejemplo):
	
	◆ Para visualizar la clave de relación del tipo "usuario a usuarios" con el empleado Jack Miller como raíz del organigrama corporativo, tendrá que especificar:
	
	`cn=jmiller,ou=users,ou=sample,o=novell`
	
	◆ Para visualizar la clave de relación del tipo "grupo a usuarios" con el grupo Accounting como raíz del organigrama corporativo, tendrá que especificar:
	
	`cn=Accounting,ou=groups,ou=sample,o=novell`

Profundidad por defecto	Especifica la profundidad del organigrama corporativo cuando se visualiza por primera vez. ◆ 0: sólo se mostrará la raíz ◆ 1: se mostrará la raíz y sus hijos ◆ 2: se mostrará la raíz, sus hijos y sus nietos etc. Si este valor se incrementa a un valor superior a la profundidad máxima (abajo), el valor Profundidad máxima tendrá preponderancia.
Profundidad máxima	Define la profundidad máxima a la que el usuario puede llegar en un organigrama corporativo. No es lo mismo que la capacidad para navegar por un organigrama corporativo restringido por derechos vigentes.
Máscara del organigrama corporativo	Business Card eGuide Novell.com Wired True Blue

Preferencia	Operaciones que puede realizar
Conectar cables a elementos	Permite especificar si las tarjetas del organigrama corporativo están conectadas por cables. False significa que no están conectadas.
Tiempo límite del menú	Tiempo en milisegundos antes de que el menú visualizado actualmente (para los enlaces incorporados) desaparezca.
Presentación del árbol	Permite definir la orientación, distribución y apariencia del organigrama corporativo, por nivel de profundidad. Los primeros *n* valores definirán la orientación, distribución y apariencia de los niveles comprendidos entre 0 y *n-1*. El último valor se utiliza para un nivel de profundidad superior a *n-1*. Los valores deben estar comprendidos entre 0 y 5. Los valores son: 0: la tarjeta se pone encima de una lista vertical de elementos 1: línea por encima de una lista vertical de elementos 2: la tarjeta se pone encima de una lista horizontal de elementos 3: línea por encima de una lista horizontal de elementos 4: la tarjeta se pone delante de una lista vertical de elementos 5: línea por delante de una lista vertical de elementos
Presentación hoja	Permite definir la orientación, distribución y apariencia de la mayor profundidad de una rama del organigrama corporativo.
Anchura mínima del elemento	Este valor se recomienda para redondear una cifra ('altura mín. elemento' * 1.618)
Altura mínima del elemento	Este valor se recomienda para redondear una cifra ('anchura mín. elemento' / 1.618)
Separador para atributos multivalentes	El carácter utilizado como separador de atributos con más de un valor.

Preferencias de diseño del organigrama corporativo

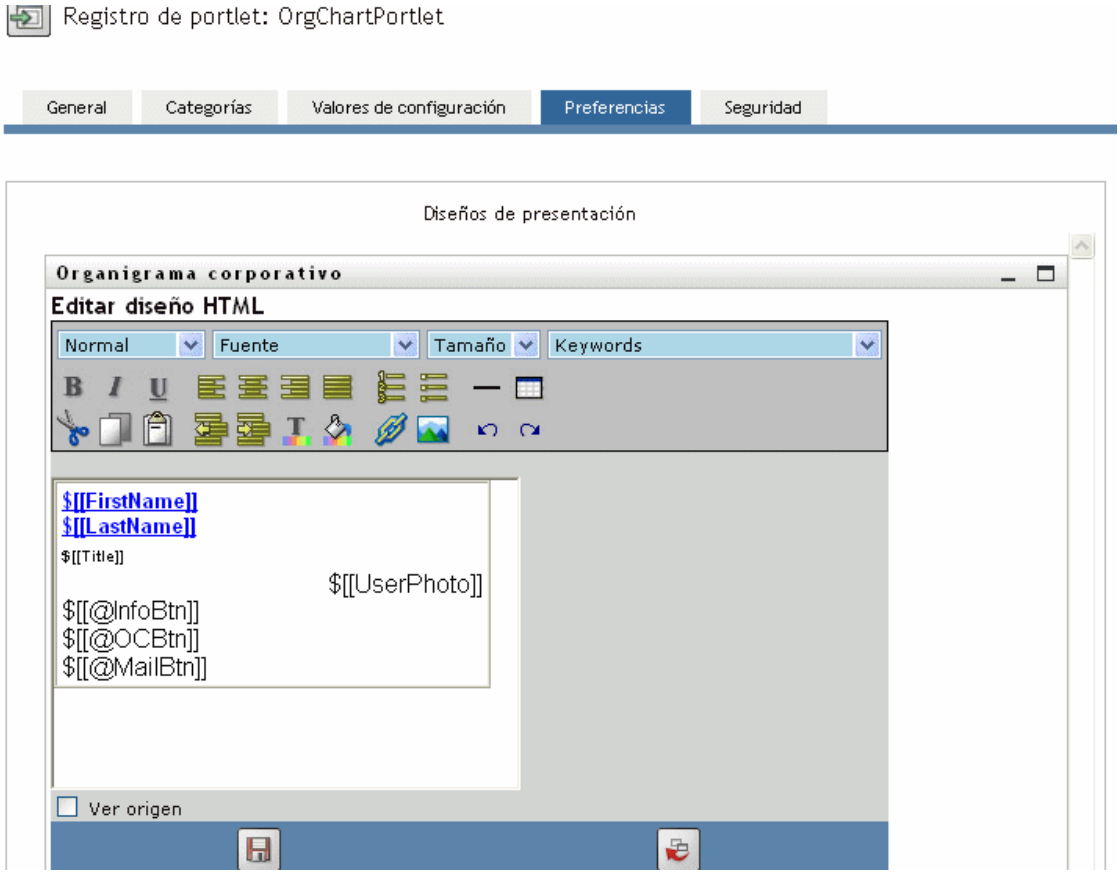
Las preferencias de diseño del organigrama corporativo permiten definir el diseño HTML de la visualización de las entradas del organigrama corporativo. Puede utilizar el editor HTML que elija para efectuar ediciones más precisas. Consulte “Para utilizar un editor externo” en la página 279.



Diseño HTML para tarjetas de presentación: el diseño por defecto.

Diseño HTML para una visualización sencilla: el diseño visualizado cuando la preferencia de presentación del árbol está definida en 1.

Editor HTML Acceda al editor HTML haciendo clic en el botón de edición. El editor HTML tiene la apariencia siguiente:



Utilización del editor HTML

El editor HTML proporciona una interfaz WYSIWYG para definir el diseño de las hojas del organigrama corporativo. Proporciona las funciones típicas de un editor HTML para definir el formato de texto y las listas, especificar anclajes e imágenes, etc. Utilice la lista desplegable de *palabras clave* para colocar atributos, comandos y URL de navegación dentro del área de diseño. Al seleccionar una palabra clave en la lista desplegable, dicha palabra se inserta con la sintaxis adecuada, aunque también puede añadir HTML dentro del área de diseño.

Palabras clave Cuando diseñe la disposición, puede utilizar la lista desplegable de palabras clave para insertar variables que, en el tiempo de ejecución, se sustituirán con valores de atributo específicos. O bien puede escribir referencias a ellas con esta sintaxis:

```
$[[palabra clave]]
```

Donde *palabra clave* es el valor de un atributo de entidad como LastName.

Puede concatenar atributos utilizando la sintaxis siguiente:

```
$[[palabra clave+palabra clave]]
```

Por ejemplo:

```
$[[FirstName+LastName]]
```

Puede concatenar tantos atributos como desee e incluir cadenas entre comillas como se indica a continuación:

```
$[[palabra clave+"texto de ejemplo"+palabra clave]]
```

De esta manera, los valores de las palabras clave y del texto entre comillas se procesarán.

Nota: Cuando una palabra clave está mal escrita en un diseño, se procesará tal cual en el organigrama corporativo (incluido $[[]]).

Funciones del editor de HTML y uso de palabras clave Para utilizar las funciones del editor de HTML y la lista desplegable de palabras clave:

Función	Sugerencia
Botón Insertar enlace	Para insertar un enlace: **En Mozilla:** 1. Resalte el texto que desea convertir en hiperenlace y haga clic en **Insertar enlace**. 2. Escriba la URL y haga clic en **Crear enlace**. 3. Guarde las preferencias. **En IE:** 1. Haga clic en Insertar enlace. 2. Escriba la URL en la ventana emergente. 3. Resalte el texto que desea convertir en hiperenlace y haga clic en **Crear enlace** (en la ventana emergente). 4. Guarde las preferencias. **Nota:** Si la imagen o URL se encuentra en el cuadrante superior izquierdo del editor de HTML, la ventana emergente se superpondrá a él. Dado que dicha ventana no se puede mover, tendrá que crear el texto que desee en otro punto del editor y cortarlo y pegarlo en la ubicación correcta.

Función	Sugerencia
Botón Añadir imagen	**En Mozilla:** 1. Ponga el cursor del ratón donde desee insertar una imagen y haga clic en **Añadir imagen**. 2. Escriba la URL y el texto y haga clic en **Crear imagen** en la ventana emergente. 3. Guarde las preferencias. **En IE:** 1. Haga clic en **Añadir imagen**. 2. Escriba la URL y el texto en la ventana emergente, coloque el cursor del ratón donde desee insertar la imagen, y haga clic en **Crear imagen** en la ventana emergente. 3. Guarde las preferencias. **Nota:** Si la imagen o URL se encuentra en el cuadrante superior izquierdo del editor de HTML, la ventana emergente se superpondrá a él. Dado que dicha ventana no se puede mover, tendrá que crear el texto que desee en otro punto del editor y cortarlo y pegarlo en la ubicación correcta.
Lista desplegable de palabras clave: atributos	Conjunto de atributos disponibles para esta entidad.
Lista desplegable de palabras clave: comandos	Estos comandos permiten que el portlet Organigrama corporativo inicie otros portlets de identidad o funciones incorporadas como IM o herramientas de correo electrónico. ◆ **Botón Acción de IM**: crea un botón para enviar IM ◆ **Botón Acción de correo**: crea un botón para enviar correos electrónicos ◆ **Botón Acción del organigrama corporativo**: crea un botón para cambiar a otra relación, con la instancia de la entidad seleccionada como padre ◆ **Botón Acción de información**: inicia el portlet Información Si desea ver ejemplos de botones generados, consulte “Enlaces incorporados” en la página 266.

Función	Sugerencia

URL	**Enlace URL de navegación del organigrama corporativo**: permite especificar una URL o atributo de entidad que se visualizará como enlace. Cuando el usuario hace clic en el enlace, se vuelve a visualizar el portlet Organigrama corporativo con la entidad pulsada como nodo raíz.
	Restricción:
	Sólo es válido cuando las entidades padre e hijo de una relación son el mismo tipo de objeto. Por ejemplo, en la relación de supervisor-empleado, ambos son usuarios.
	Sugerencias de uso:
	Para utilizar esta palabra clave, debe:
	1. Hacer clic en Ver origen.
	2. Escribir la @palabra clave NavUrl con la sintaxis siguiente:
	`<a href="javascript:$[[@NavUrl]]">`*Texto*`</a>`
	donde *Texto* es el enlace que se visualizará en el tiempo de ejecución o un atributo de entidad. En el ejemplo siguiente, **Click here** se convierte en un enlace donde se puede hacer clic.
	`<a href="javascript:$[[@NavUrl]]">Click here</a>`
	En este ejemplo, el atributo FirstName se convierte en el enlace donde se puede hacer clic:
	`<a href="javascript:$[[@NavUrl]]">$[[FirstName]]</a>`
	Restricción de uso
	Con Internet Explorer, **no puede** utilizar la sintaxis siguiente.
	`<a href="$[[@NavUrl]]">`*someText*`</a>`
	Durante una operación de guardado, Internet Explorer añade:
	`http://context before $[[@NavUrl]]`
	Esto significa que
	`<a href="$[[@NavUrl]]">`*Texto*`</a>`
	se convierte en
	`<a href="http://localhost/.../`

Función	Sugerencia
	Enlace Clic de navegación del organigrama corporativo: utilice esta palabra clave para un evento onClick. (Sólo permite que se actualice el área de portlet del organigrama corporativo, en vez de actualizarse la página completa). **Sugerencias de uso:** Para utilizar esta palabra clave, debe: 1. Hacer clic en Ver origen. 2. Escribir la @palabra clave NavClick con la sintaxis siguiente: `<A href="javascript:return false;" onClick="$[[@NavClick]]">$[[Algún_atributo]]</A>` donde *Algún_atributo* es un atributo de entidad que se convertirá en un enlace donde se puede hacer clic. "javascript:return false;" es obligatorio. Si se omite, se producirá un error.

Para guardar los diseños que defina, haga clic en *Enviar*.

Para utilizar un editor externo Puede utilizar un editor externo HTML:

1. Creando el código fuente HTML para los atributos, comandos y palabras clave de la entidad utilizando el editor de diseño de HTML disponible en las preferencias.
2. Copiando el código fuente HTML en el editor de su elección.
3. Introduciendo los cambios que desee.
4. Volviendo a copiar el código fuente HTML en la preferencia del editor de diseño de HTML cuando haya acabado de editarla.

18.2.3 Carga dinámica de imágenes

Para visualizar imágenes, como fotografías de usuarios, que están almacenadas en el repositorio seguro de identidades, puede añadir el nombre del atributo a la tarjeta de presentación. Por ejemplo, si añade el atributo User Photo al diseño de la tarjeta de presentación, se visualizará la fotografía del usuario.

Si almacena imágenes fuera del repositorio seguro de identidades, necesitará utilizar la etiqueta IMG: del *modo Ver origen* del editor HTML, tal como se indica a continuación:

1. Vaya a las preferencias del portlet Organigrama corporativo y acceda al editor de HTML.
2. Haga clic en *Ver origen*.
3. Utilice la etiqueta IMG: para combinar una ubicación, una clave de atributo y una extensión de archivo, mediante una sintaxis como la que indicamos a continuación:

```
$[[IMG:”URL” + nombre-clave-atributo + ”extensión_archivo”]]
```

En el ejemplo siguiente, se muestra la sintaxis que deberá utilizar si ha almacenado fotografías del empleado como imágenes JPG, según el apellido, en el subdirectorio de imágenes del servidor de la aplicación:

```
$[[IMG:"http://mihost:8080/images/"+Apellido+".jpg"]]
```

En el tiempo de ejecución, el organigrama corporativo concatenará la URL con el atributo LastName y la extensión de archivo .jpg.

Tenga en cuenta que el editor de HTML admite una sintaxis flexible y es compatible con cualquier combinación de texto y atributos, por lo que la sintaxis es:

```
$[[IMG:”texto” + nombre-clave-atributo + ...]]
```

Referencia de los portlets de gestión de contraseñas

19

En este capítulo se describe cómo añadir funciones de autenticación de usuario y de autoservicio de contraseñas a la aplicación de usuario del Gestor de identidades. Los temas son:

19.1 Preparación de la gestión de contraseñas

Para prepararse para dar soporte al autoservicio de contraseñas y a la autenticación de usuario en una aplicación de usuario del Gestor de identidades, deberá saber lo siguiente:

19.1.1 Acerca de las funciones de gestión de contraseñas

Las funciones de gestión de contraseñas admitidas por la aplicación de usuario del Gestor de identidades incluyen *autenticación de usuario* y *autoservicio de contraseñas*. Si utiliza dichas funciones, la aplicación podrá:

- Solicitar información de *entrada a la sesión* (nombre de usuario y contraseña) para autenticarse en Novell eDirectory
- Proporcionar a los usuarios un autoservicio de *cambio de contraseñas*
- Proporcionar a los usuarios un autoservicio de *contraseña olvidada* (incluida la petición de respuestas de verificación, visualización de una sugerencia de contraseña o permiso para cambiar de contraseña, según las necesidades)
- Proporcionar a los usuarios un autoservicio de *respuestas de verificación*
- Proporcionar a los usuarios un autoservicio de *sugerencia de contraseñas*

19.1.2 Configuración necesaria en eDirectory

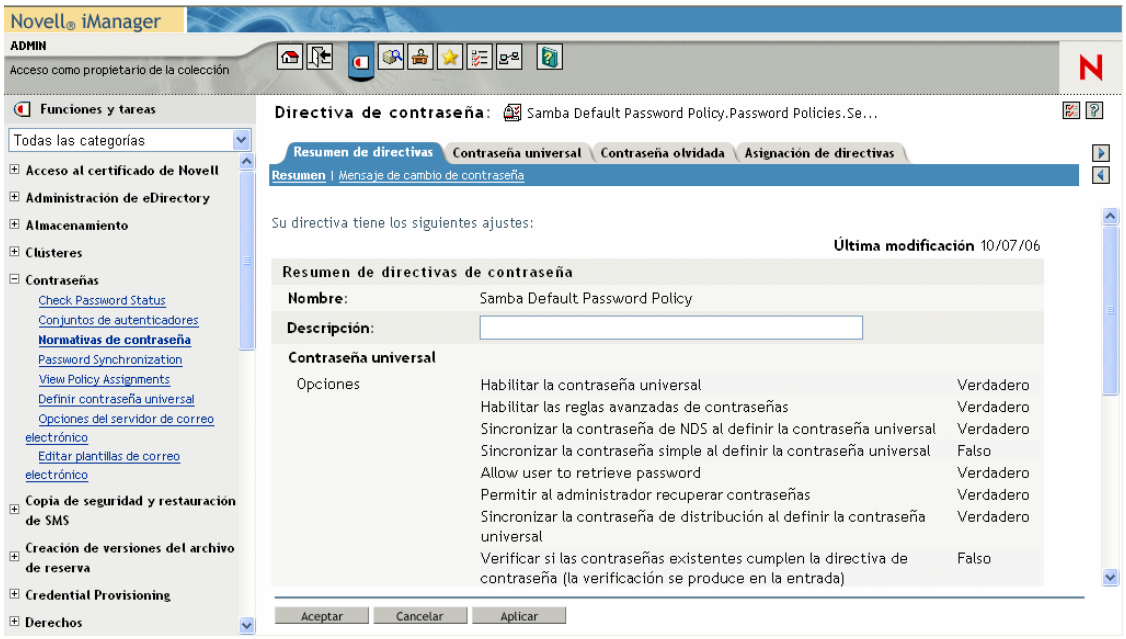
Para poder utilizar la mayoría de las funciones de autenticación de usuario y de autoservicio de contraseñas, deberá ejecutar las tareas siguientes en eDirectory:

- Habilitar *Contraseña Universal*
- Crear una o varias *directivas de contraseña*

- Asignar las políticas de contraseña apropiadas a los *usuarios*

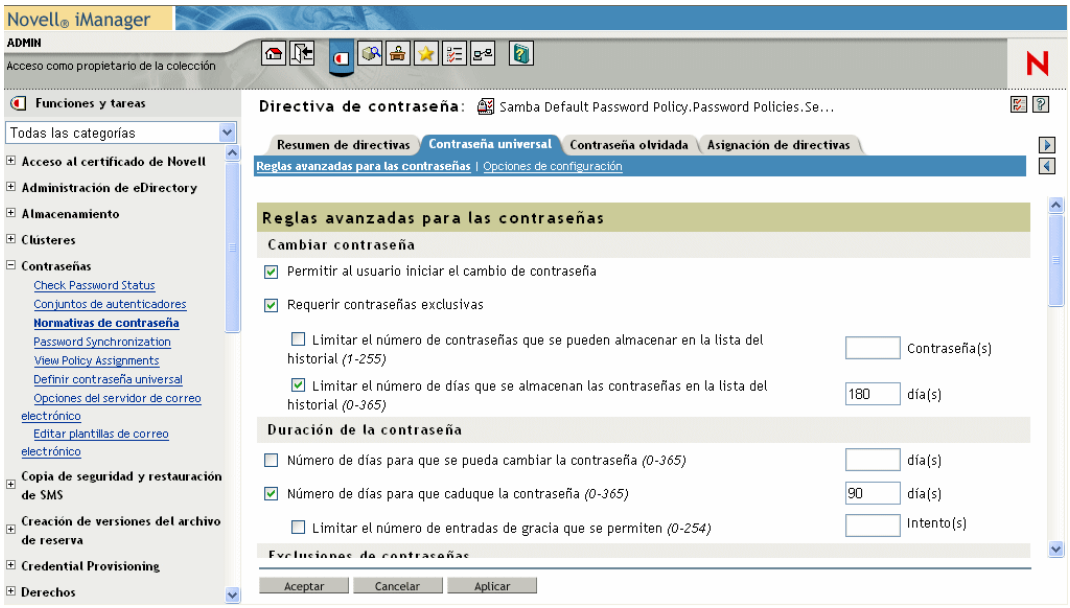
Una directiva de contraseña es un conjunto de reglas definidas por el administrador que especifican los criterios de creación y sustitución de contraseñas de usuario. El Gestor de identidades aprovecha los servicios *NMAS* (autenticación modular) de Novell para aplicar las directivas de contraseña que asigne a los usuarios de eDirectory.

Puede utilizar *Novell iManager* para ejecutar los pasos de configuración necesarios. Por ejemplo, a continuación mostramos cómo alguien ha definido la directiva DocumentationPassword en iManager.

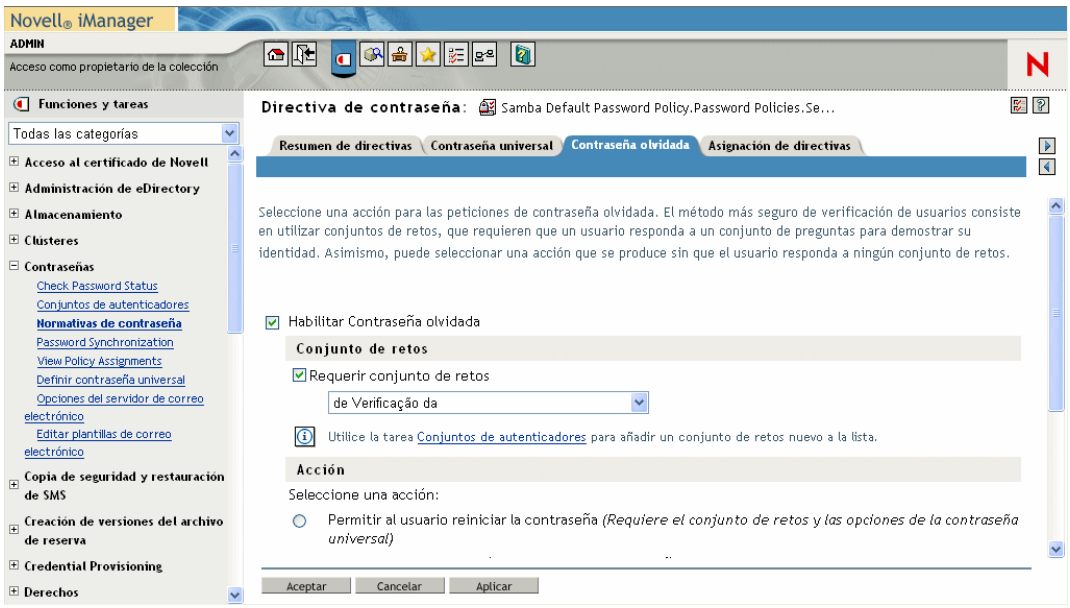


Esta directiva de contraseña especifica:

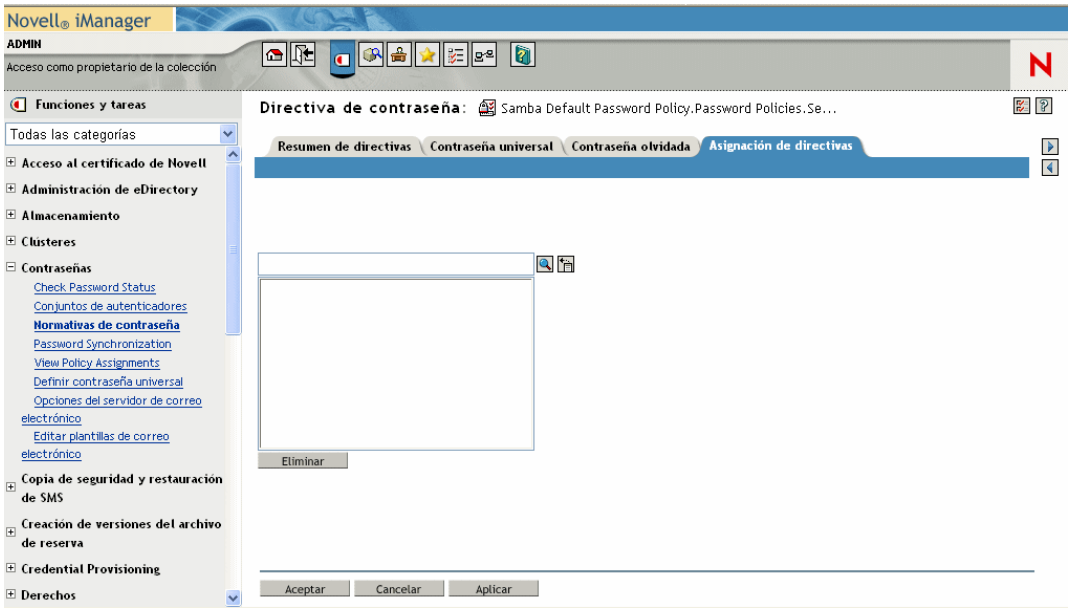
- Valores de *contraseña universal*



- Valores para tratar situaciones de *olvido de contraseñas*



- *Asignaciones* que aplican la directiva a usuarios específicos



Para obtener más información acerca de cómo configurar la contraseña universal y las directivas de contraseña en eDirectory, consulte Novell Identity Manager Administration Guide (http://www.novell.com/documentation/dirxml20/index.html) (Gestor de identidades: Guía de administración).

19.2 Acerca de los portlets de contraseña

Para implementar funciones de autenticación de usuario y de autoservicio de contraseñas en la aplicación de usuario del Gestor de identidades, deberá utilizar los portlets siguientes:

Portlet	Descripción
Sección 19.3, “Portlet Entrada a IDM”, en la página 286	Entrada a IDM proporciona una autenticación de usuario fuerte admitida por el Gestor de identidades (mediante contraseña universal, directivas de contraseña y NMAS). El portlet Entrada a IDM redirige a los otros portlets de contraseña durante el proceso de entrada, según las necesidades.
Sección 19.4, “Portlet Respuesta de Verificación de IDM”, en la página 287	Este portlet de autoservicio permite que los usuarios: • Configuren las respuestas válidas a preguntas de verificación definidas por el administrador, además de configurar preguntas y respuestas de verificación definidas por el usuario. • Cambien las respuestas válidas a preguntas de verificación definidas por el administrador, además de cambiar preguntas y respuestas de verificación definidas por el usuario.
Sección 19.5, “Portlet Definición de sugerencias en IDM”, en la página 289	Este portlet de autoservicio permite que el usuario configure o cambie su sugerencia de contraseña (que se puede visualizar o enviar por correo electrónico como pista en situaciones de olvido de contraseña).

Portlet	Descripción
Sección 19.6, “Portlet Cambiar contraseña IDM”, en la página 290	Este portlet de autoservicio permite que el usuario cambie (reajuste) su contraseña universal, en función de la directiva de contraseña asignada. Utiliza dicha directiva para visualizar las reglas que la nueva contraseña debe cumplir. Si la contraseña universal no está habilitada, este portlet cambiará la contraseña de eDirectory (simple) del usuario, de acuerdo con las restricciones de contraseña del usuario.
Sección 19.7, “Portlet Contraseña olvidada de IDM”, en la página 292	Este portlet de autoservicio utiliza la autenticación de respuesta de verificación para que el usuario pueda obtener información acerca de su contraseña (de NMAS). El resultado, que depende de la directiva de contraseñas asignada, puede incluir: ◆ Visualización de la sugerencia de contraseña del usuario en la pantalla ◆ Envío por correo electrónico de la sugerencia al usuario ◆ Envío por correo electrónico de la contraseña al usuario ◆ Solicitud al usuario que reajuste (cambie) la contraseña

19.2.1 Modos de portlet del autoservicio de contraseñas

Los portlets de autoservicio de contraseñas (Respuesta de verificación de IDM, Definición de sugerencias en IDM y Cambiar contraseña IDM) funcionan en dos modos:

Modo	Descripción	Comportamiento del tiempo de ejecución
Modo autónomo	Los portlets se ejecutan de forma autónoma en las páginas compartidas.	◆ Si el portlet se ejecuta **correctamente**, se visualizará un mensaje de éxito con un enlace para volver a ejecutar la operación. ◆ Si el portlet no se ejecuta **correctamente**, se visualizará un mensaje de error en el formulario existente.
Modo de delegación	Los portlets se visualizan en una página como resultado de una comprobación de validación durante una entrada.	◆ Si el portlet se ejecuta **correctamente**, se redirigirá al usuario a un portlet nuevo o a la página principal de la aplicación de usuario. No se visualizará ningún mensaje de éxito. ◆ Si el portlet no se ejecuta **correctamente**, se visualizará un mensaje de error en el formulario existente.

19.3 Portlet Entrada a IDM

El portlet Entrada a IDM ejecuta una autenticación de usuario muy robusta admitida por el Gestor de identidades (mediante contraseña universal, directivas de contraseña y NMAS). Dicho portlet redirige a otros portlets de contraseña durante el proceso de entrada, según las necesidades.

19.3.1 Requisitos

El portlet Entrada a IDM tiene los requisitos siguientes:

Tema	Requisitos
Directiva de contraseñas	Este portlet no necesita una directiva de contraseñas, a menos que desee utilizar reglas de contraseña avanzadas o deje que los usuarios hagan clic en el enlace **Contraseña olvidada**.
Contraseña universal	Este portlet no necesita que la contraseña universal esté habilitada, a menos que desee utilizar una directiva de contraseña con reglas de contraseña avanzadas.
SSL	Este portlet utiliza SSL, por tanto, asegúrese de que el servidor de aplicación esté correctamente configurado para dar soporte a las conexiones SSL con el dominio LDAP.

19.3.2 Uso

Para utilizar el portlet Entrada a IDM, deberá tener conocimientos acerca de:

- “Cómo Entrada de IDM redirige a otros portlets” en la página 286
- “Uso de entradas de gracia” en la página 287

Cómo Entrada de IDM redirige a otros portlets

En el tiempo de ejecución, el portlet Entrada de IDM redirige a otros portlets de contraseña, según las necesidades para completar el proceso de entrada. Por ejemplo:

Si el usuario	Entrada de IDM redirige a
Hace clic en el enlace **Contraseña olvidada**	Sección 19.7, “Portlet Contraseña olvidada de IDM”, en la página 292
Necesita configurar preguntas y respuestas de verificación	Sección 19.4, “Portlet Respuesta de Verificación de IDM”, en la página 287
Necesita configurar su sugerencia de contraseña	Sección 19.5, “Portlet Definición de sugerencias en IDM”, en la página 289
Necesita reajustar una contraseña no válida	Sección 19.6, “Portlet Cambiar contraseña IDM”, en la página 290

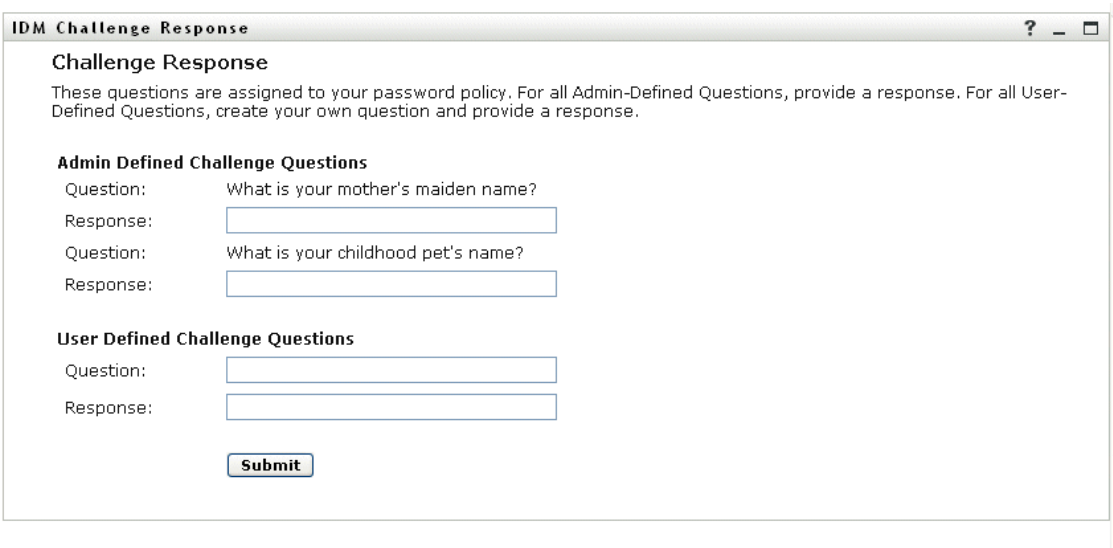
Uso de entradas de gracia

Si utiliza una entrada de gracia, el portlet Entrada a IDM visualiza un mensaje de advertencia que le solicita que cambie la contraseña e indica el número de entradas de gracia que quedan. Si se encuentra en la última entrada, el portlet Entrada de IDM le redirigirá al portlet Cambiar contraseña IDM.

19.4 Portlet Respuesta de Verificación de IDM

Este portlet de autoservicio permite que los usuarios:

- Configuren las respuestas válidas a preguntas de verificación definidas por el administrador, además de configurar preguntas y respuestas de verificación definidas por el usuario.
- Cambien las respuestas válidas a preguntas de verificación definidas por el administrador, además de cambiar preguntas y respuestas de verificación definidas por el usuario.



19.4.1 Requisitos

El portlet Respuesta de verificación de IDM tiene los requisitos siguientes:

Tema	Requisitos
Directiva de contraseñas	Este portlet necesita una directiva de contraseña con la contraseña olvidada habilitada y un conjunto de retos.
Contraseña universal	Este portlet no necesita que la contraseña universal esté habilitada.
Configuración de eDirectory	Este portlet necesita que otorgue derechos de supervisión al administrador de la aplicación de usuario sobre el contenedor en el que reside el usuario que ha entrado. Si se otorgan estos privilegios, el usuario podrá escribir una respuesta de verificación al almacén secreto. Por ejemplo, supongamos que el administrador de dominio LDAP sea cn=admin, ou=sample, n=novell y el usuario entra en la sesión como cn=user1, ou=testou, o=novell. Deberá asignar cn=admin, ou=sample, n=novell como Trustee de **testou** y otorgar derechos de supervisor sobre **[All attribute rights]** (Todos los derechos de atributo).

19.4.2 Uso

Para utilizar el portlet Respuesta de verificación de IDM, deberá tener conocimientos acerca de:

- “Cómo se utiliza Respuesta de verificación de IDM durante la entrada a la sesión” en la página 288
- “Cómo se utiliza Respuesta de verificación de IDM en la aplicación de usuario” en la página 288

Cómo se utiliza Respuesta de verificación de IDM durante la entrada a la sesión

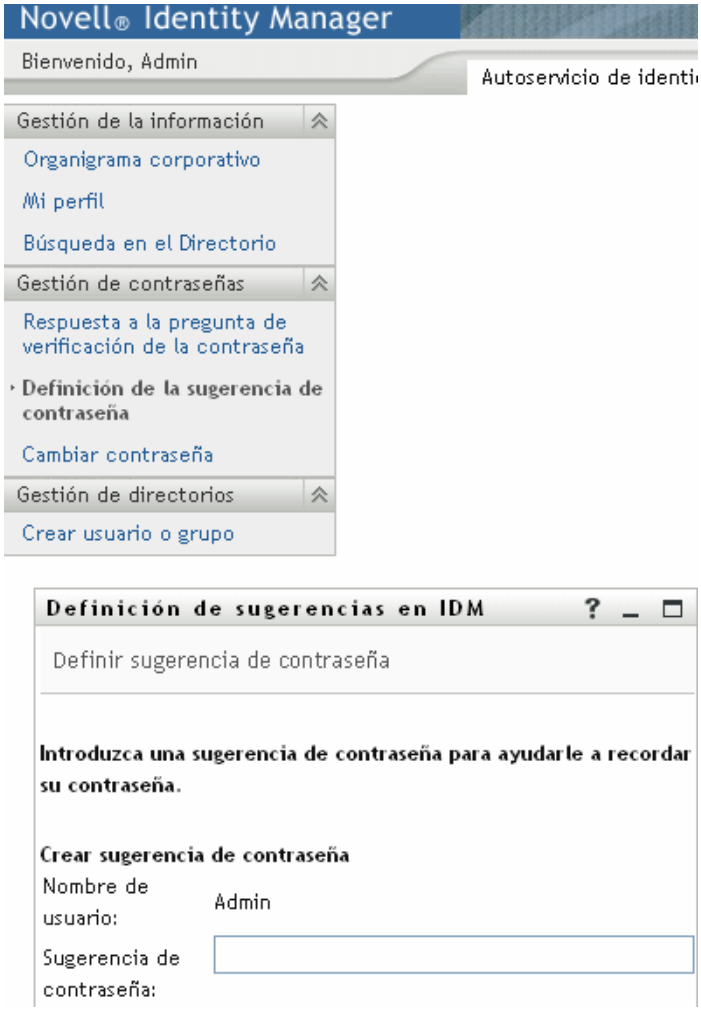
Durante el proceso de entrada a la sesión, Portlet Entrada a IDM (en la página 286) redirige automáticamente hacia el portlet Respuesta de verificación de IDM, siempre que el usuario necesite configurar preguntas y respuestas de verificación (por ejemplo, la primera vez que un usuario intenta entrar en la aplicación después de que un administrador le asigne una directiva de contraseñas en iManager. Dicha directiva ha de tener habilitada la opción de contraseña olvidada y debe incluir un conjunto de retos).

Cómo se utiliza Respuesta de verificación de IDM en la aplicación de usuario

Por defecto, la aplicación de usuario proporciona a los usuarios un autoservicio para cambiar las preguntas y respuestas de verificación.

19.5 Portlet Definición de sugerencias en IDM

Este portlet de autoservicio permite que el usuario configure o cambie su sugerencia de contraseña (que se puede visualizar o enviar por correo electrónico como pista en situaciones de olvido de contraseña).



19.5.1 Requisitos

El portlet Definición de sugerencias en IDM tiene los requisitos siguientes:

Tema	Requisitos
Directiva de contraseñas	Este portlet necesita una directiva de contraseñas con la contraseña olvidada habilitada y un conjunto de retos.
Contraseña universal	Este portlet no necesita que la contraseña universal esté habilitada.

19.5.2 Uso

Para utilizar el portlet Definición de sugerencias en IDM, deberá tener conocimientos acerca de:

- “Cómo se utiliza Definición de sugerencias en IDM durante la entrada a la sesión” en la página 290
- “Uso de Definición de sugerencias en IDM en la página de la aplicación de usuario” en la página 290

Cómo se utiliza Definición de sugerencias en IDM durante la entrada a la sesión

Durante el proceso de entrada a la sesión, Portlet Entrada a IDM (en la página 286) redirige automáticamente hacia el portlet Definición de sugerencias en IDM, siempre que el usuario necesite configurar su sugerencia de contraseña (por ejemplo, la primera vez que un usuario intenta entrar en la aplicación después de que un administrador le asigne una directiva de contraseñas en iManager. La directiva de contraseñas tendrá la opción de contraseña olvidada habilitada y la acción definida en *Enviar la sugerencia por correo electrónico al usuario* o *Mostrar la sugerencia en la página*).

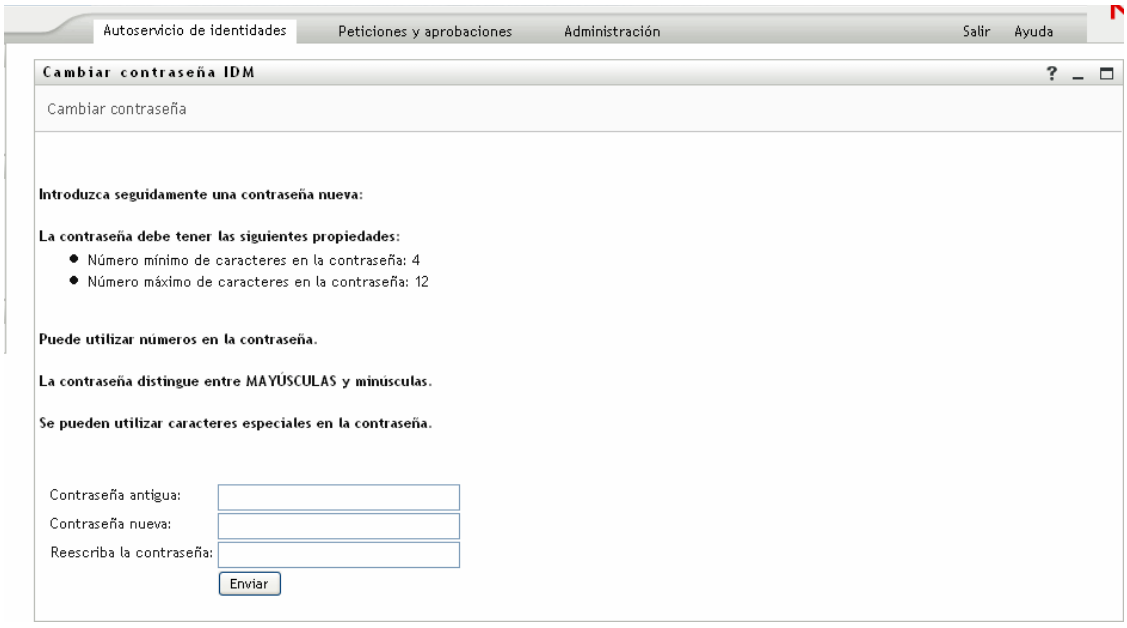
Uso de Definición de sugerencias en IDM en la página de la aplicación de usuario

Por defecto, la aplicación de usuario proporciona a los usuarios un autoservicio para cambiar su sugerencia de contraseña.

19.6 Portlet Cambiar contraseña IDM

Este portlet de autoservicio permite que el usuario cambie (reajuste) su contraseña universal, en función con la directiva de contraseña asignada. Utiliza dicha directiva para visualizar las reglas que la nueva contraseña debe cumplir.

Si la contraseña universal no está habilitada, este portlet cambiará la contraseña (simple) de eDirectory del usuario, de acuerdo con las restricciones de contraseña del usuario.



19.6.1 Requisitos

El portlet Cambiar contraseña IDM tiene los requisitos siguientes:

Tema	Requisitos
Configuración del nivel de abstracción del directorio	Este portlet no necesita configuración del nivel de abstracción del directorio.
Directiva de contraseñas	Este portlet no necesita una directiva de contraseñas, a menos que desee utilizar reglas de contraseña avanzadas (con la contraseña universal habilitada).
Contraseña universal	Para utilizar este portlet para una contraseña universal, el valor **Permitir que el usuario inicie un cambio de contraseña** debe estar habilitado en las reglas de contraseña avanzadas de la directiva de contraseña asignada del usuario. Para utilizar este portlet para una contraseña de eDirectory (simple) el valor **Permitir al usuario cambiar la contraseña** debe estar habilitado en las restricciones de contraseña del usuario.

19.6.2 Uso

Para utilizar el portlet Cambiar contraseña IDM, deberá tener conocimientos acerca de:

- “Cómo se utiliza Cambiar contraseña IDM durante la entrada a la sesión” en la página 291
- “Uso de Cambiar contraseña IDM en la aplicación de usuario” en la página 292

Cómo se utiliza Cambiar contraseña IDM durante la entrada a la sesión

Durante el proceso de entrada a la sesión, Portlet Entrada a IDM (en la página 286) redirige automáticamente hacia el portlet Cambiar contraseña IDM, siempre que el usuario necesite reajustar una contraseña no válida (por ejemplo, la primera vez que un usuario intenta entrar en una aplicación después de que un administrador implemente una directiva de contraseñas que necesite que los usuarios reajusten sus contraseñas).

Portlet Contraseña olvidada de IDM (en la página 292) también redirige a Cambiar contraseña IDM automáticamente si la directiva de contraseñas asignada del usuario especifica que debe ejecutarse un reajuste de la contraseña en los casos de olvido de la contraseña.

Uso de Cambiar contraseña IDM en la aplicación de usuario

Por defecto, la aplicación de usuario proporciona a los usuarios un autoservicio para cambiar contraseñas mediante el portlet Cambiar contraseña IDM. Por ejemplo:

19.7 Portlet Contraseña olvidada de IDM

Este portlet de autoservicio utiliza la autenticación de respuesta de verificación para que el usuario pueda obtener información acerca de su contraseña. El resultado, que depende de la directiva de contraseñas asignada, puede incluir:

- Visualización de la sugerencia de contraseña del usuario en la pantalla
- Envío por correo electrónico de la sugerencia al usuario
- Envío por correo electrónico de la contraseña al usuario
- Solicitud al usuario que reajuste (cambie) la contraseña

19.7.1 Requisitos

El portlet Contraseña olvidada de IDM tiene los requisitos siguientes:

Tema	Requisitos
Directiva de contraseñas	Este portlet necesita una directiva de contraseñas con la contraseña olvidada habilitada y un conjunto de retos.
Contraseña universal	Este portlet no necesita que la contraseña universal esté habilitada, (a menos que desee admitir las acciones contraseña olvidada siguientes: reajustar la contraseña o enviar la contraseña por correo electrónico al usuario).

19.7.2 Uso

Para utilizar el portlet Contraseña olvidada de IDM, deberá tener conocimientos acerca de:

- “Cómo se utiliza Contraseña olvidada de IDM durante la entrada a la sesión” en la página 293
- “Configuración del entorno para acciones de correo electrónico” en la página 294
- “Preferencias para Contraseña olvidada de IDM” en la página 294

Cómo se utiliza Contraseña olvidada de IDM durante la entrada a la sesión

Durante el proceso de entrada a la sesión, Portlet Entrada a IDM (en la página 286) redirige al portlet Contraseña olvidada de IDM si el usuario hace clic en el enlace *Contraseña olvidada*. Cuando se visualiza Contraseña olvidada de IDM, ejecuta las acciones siguientes:

1. Solicita el *nombre de usuario*.
2. Redirige a Portlet Entrada a IDM (en la página 286) para ejecutar *autenticación de /respuesta de verificación* para dicho usuario.
3. Ejecuta la *acción de contraseña olvidada* especificada en la directiva de contraseña asignada al usuario. Realiza una de las acciones siguientes:
   - *Redirige* a Portlet Cambiar contraseña IDM (en la página 290) para que el usuario pueda reajustar su contraseña
   - *Envía por correo electrónico* la contraseña o sugerencia al usuario
   - *Visualiza* la contraseña

Nota: El portlet Contraseña olvidada de IDM no está pensado para un uso autónomo. Esto significa que no debe planearse añadirlo a una página compartida de la aplicación de usuario, ya que ello supondría un riesgo potencial para la seguridad, ya que algunas personas podrían cambiar la

contraseña en una máquina desatendida sin que lo sepa el usuario o sin que éste haya dado su permiso.

Configuración del entorno para acciones de correo electrónico

Si desea admitir las acciones de correo electrónico por contraseña olvidada, deberá asegurarse de que el *servidor de notificaciones por correo electrónico* esté correctamente configurado:

1. Utilice un navegador Web para acceder a *iManager* en el servidor de eDirectory y entre como *administrador*.
2. Vaya a *Funciones y tareas> Contraseñas* y seleccione *Opciones del servidor de correo electrónico*.
3. Especifique los valores apropiados y haga clic en *Aceptar*.

El portlet Contraseña olvidada de IDM utiliza dos *plantillas de correo electrónico*. En iManager las encontrará en *Funciones y tareas>Contraseñas>Editar plantillas de correo electrónico*. Se denominan:

- Petición de sugerencia de contraseña
- Su petición de contraseña

El contenido de estas plantillas se puede cambiar según las necesidades de su aplicación (aunque no se puede cambiar la estructura).

Preferencias para Contraseña olvidada de IDM

El portlet Contraseña olvidada de IDM proporciona las preferencias siguientes:

Preferencia	Información
login-sequence	La secuencia de entrada a sesión de NMAS que se utilizará. En esta versión, el portlet sólo admite **Respuesta de verificación**.
ldap-sslport	El puerto ldap seguro que se utilizará. El valor por defecto es **636**.
allow-wildcard	Indica si el usuario puede poner comodines al introducir el nombre de usuario. El valor por defecto es **false**.
encoding	La codificación de caracteres que se utilizará. El valor por defecto es **utf-8**.

Referencia del portlet Lista de búsqueda

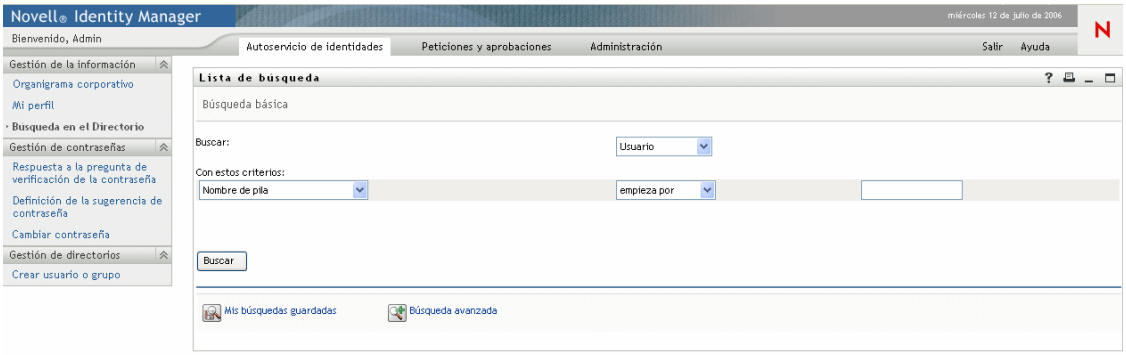
20

En este capítulo se describe cómo configurar y personalizar el portlet *Lista de búsqueda* para utilizarlo con la aplicación de usuario del Gestor de identidades. Los temas son:

20.1 Acerca de la Lista de búsqueda

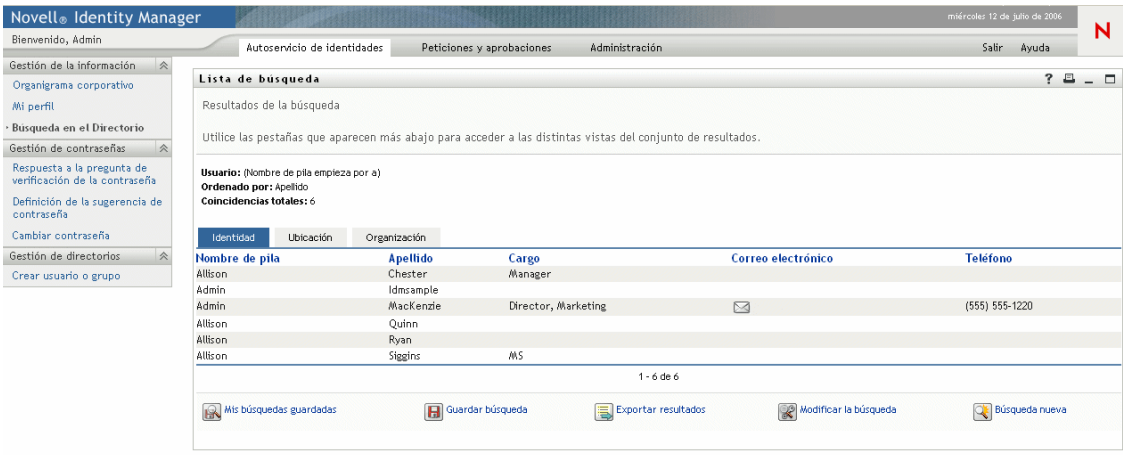
El portlet *Lista de búsqueda* permite que los usuarios busquen y visualicen el contenido del repositorio seguro de identidades. Se trata de la base de la acción *Búsqueda en el Directorio* de la pestaña Autoservicio de identidades de la aplicación de usuario del Gestor de identidades. La acción Búsqueda en el Directorio está configurada para permitir que los usuarios busquen usuarios, grupos y grupos de tareas, aunque puede modificarla para cambiar el ámbito de los atributos y objetos que se pueden buscar.

En el ejemplo siguiente se muestra cómo la acción Búsqueda en el Directorio permite que los usuarios definan los criterios de búsqueda.



Elemento de interfaz de usuario	Descripción
Buscar	Los usuarios seleccionan el tipo de objeto que se buscará. Para obtener más información acerca de cómo definir el contenido de la lista, consulte Sección 20.2.2, “Configuración de las preferencias de la lista de búsqueda”, en la página 302.
Con estos criterios	Los usuarios definen los criterios de búsqueda seleccionando atributos y buscando operadores en la lista desplegable. Cuando el usuario selecciona Búsqueda avanzada, puede especificar varias filas y varios bloques de grupos de criterios que pueden convertirse en inclusivos (AND) o exclusivos (OR). Para obtener más información acerca de cómo definir los atributos que se pueden buscar, consulte Sección 20.2.2, “Configuración de las preferencias de la lista de búsqueda”, en la página 302.
Buscar	Ejecuta los criterios de búsqueda especificados. Para obtener más información acerca de cómo definir la búsqueda por defecto, consulte Sección 20.2.2, “Configuración de las preferencias de la lista de búsqueda”, en la página 302.
Mis búsquedas guardadas 	Permite que el usuario ejecute, edite o suprima una búsqueda seleccionada y guardada previamente.
Búsqueda avanzada 	Al igual que el botón Buscar, permite que el usuario añada filas o bloques de criterios de búsqueda, pero en una búsqueda avanzada, puede especificar varias filas o bloques de grupos de criterios de búsqueda que pueden convertirse en inclusivos (AND) o exclusivos (OR). Para obtener más información acerca de cómo definir los atributos que se pueden buscar, consulte Sección 20.2.2, “Configuración de las preferencias de la lista de búsqueda”, en la página 302.

Este ejemplo muestra cómo se visualiza el portlet (con datos de ejemplo) después de que se introduzcan los criterios de búsqueda *Nombre empieza por A*:



Puede configurar el portlet Lista de búsqueda para utilizar cualquiera de las funciones siguientes:

Elemento de interfaz de usuario	Descripción
Pestañas Identidad, Ubicación, Organización	El usuario puede hacer clic en cualquiera de estas pestañas para ver la lista de resultados visualizada de diferentes formas. Para obtener más información acerca de formatos, consulte Sección 20.1.1, “Acerca de los formatos de visualización de la lista de resultados”, en la página 298.
Mis búsquedas guardadas 	Permite que el usuario seleccione una búsqueda guardada previamente.
Guardar búsqueda 	Permite que los usuarios guarden criterios de búsqueda y vuelvan a ejecutar las búsquedas guardadas cuando lo necesiten. Las búsquedas se guardan en el atributo srvprvQueryList del usuario conectado actualmente.
Exportar resultados 	Permite que los usuarios exporten los resultados de la búsqueda a otro formato.

Elemento de interfaz de usuario	Descripción
Modificar la búsqueda 	Permite que los usuarios cambien los criterios de búsqueda.
Búsqueda nueva 	Permite que el usuario defina una nueva búsqueda.

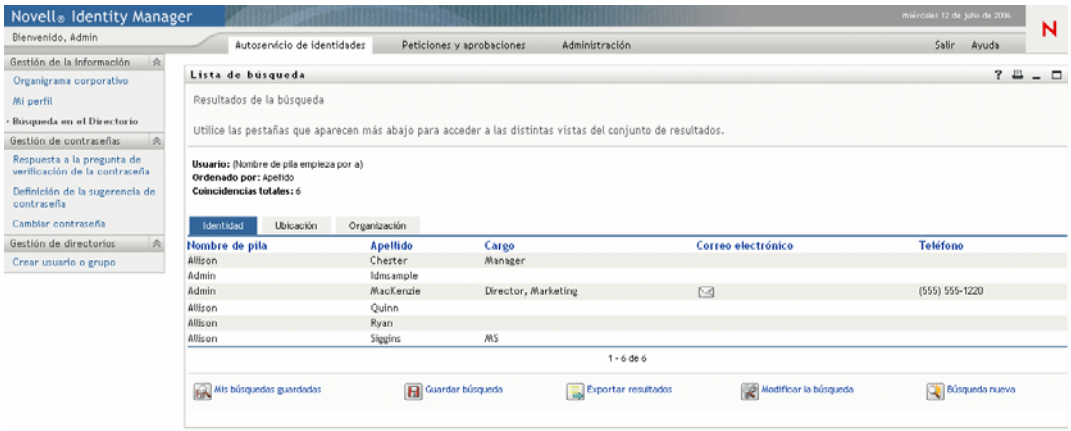
Por defecto, Lista de búsqueda también permite a los usuarios finales:

- Imprimir los resultados de la búsqueda
- Iniciar el correo electrónico desde la lista de resultados
- Iniciar el portlet Información desde la lista de resultados

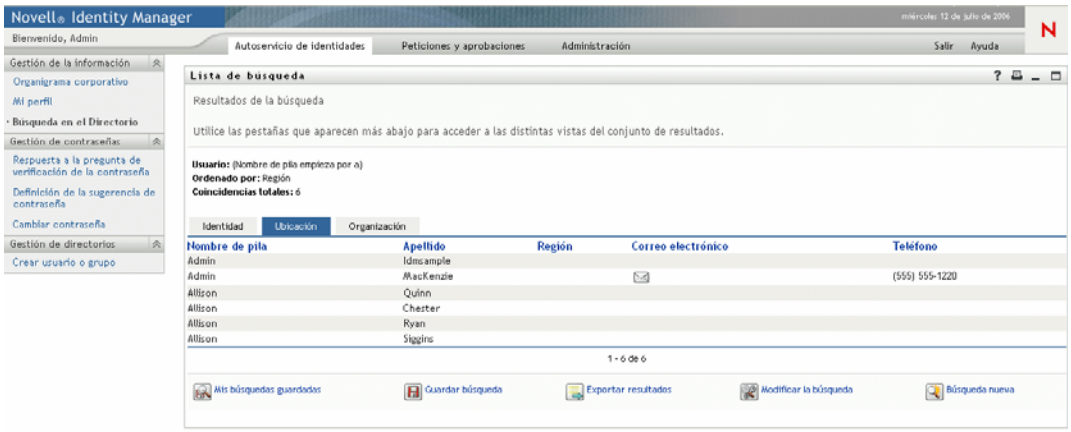
20.1.1 Acerca de los formatos de visualización de la lista de resultados

Se puede definir cómo se mostrarán al usuario final los datos devueltos por la búsqueda en el repositorio seguro de identidades. Dichos datos se pueden organizar en uno o varios de los tipos de páginas siguientes:

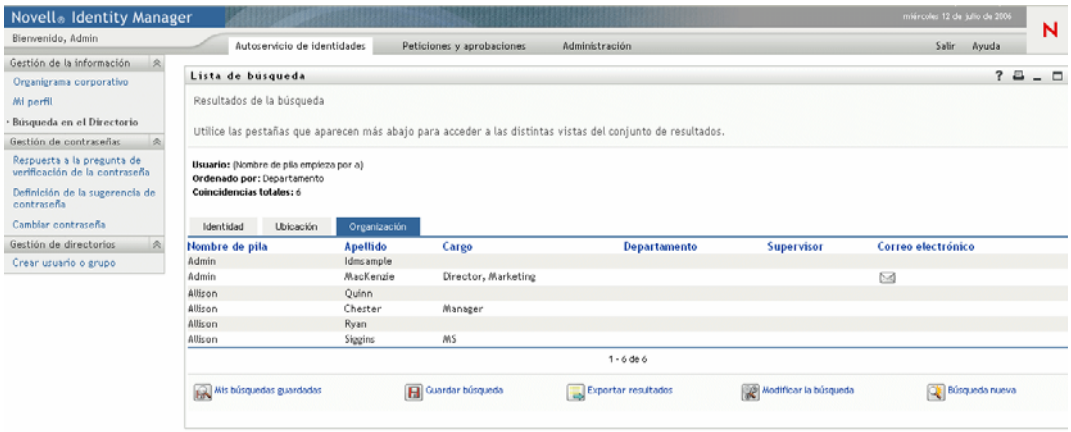
- *Páginas de identidad*: normalmente incluyen información de contacto, como la que mostramos a continuación:



- *Páginas de ubicación*: normalmente incluyen información de ubicación, como la que mostramos a continuación:



- *Páginas de organización*: normalmente incluyen información de la jerarquía organizativa, como la que mostramos a continuación:



Puede definir otros formatos de la lista de resultados utilizando las preferencias complejas del portlet. Por ejemplo, si el esquema del repositorio de identidades incluía información acerca de las habilidades o certificaciones de los empleados, puede configurar una lista de resultados para visualizar esta información.

Según cómo configure el portlet, los usuarios finales podrán:

- Elegir los tipos de objetos del repositorio seguro de identidades en los que efectuarán la búsqueda (como, por ejemplo, usuarios y grupos)
- Especificar los *criterios* de la búsqueda (como el nombre empieza por, el apellido incluye, etc.)
- Seleccionar el *formato de visualización* de los resultados de la búsqueda
- Cambiar el *orden de clasificación*

20.2 Configuración del portlet Lista de búsqueda

Para configurar el portlet Lista de búsqueda deberá ejecutar una serie de pasos como los siguientes:

Paso	Tarea	Descripción
1	Definir: ◆ Las entidades y atributos sobre los que dará permiso de búsqueda a los usuarios ◆ Cómo visualizará la lista de resultados	Puede utilizar la acción Búsqueda en Directorio predefinida que se instala con la aplicación de usuario del Gestor de identidades, tal cual. Puede modificarla o crear una propia. Si desea obtener más información, consulte Sección 20.2.2, “Configuración de las preferencias de la lista de búsqueda”, en la página 302.
2	Verificar que el conjunto de entidades y atributos de búsqueda estén definidos en el nivel de abstracción del directorio.	Si desea obtener más información, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.
3	Determinar cómo desea que los usuarios accedan al portlet.	¿Desea que los usuarios lancen este portlet desde una página ya existente o desde una nueva? Para obtener más información acerca de las páginas, consulte Capítulo 7, “Administración de páginas”, en la página 135.
4	Definir las preferencias del portlet	Las preferencias del portlet de la lista de búsqueda permiten definir: ◆ Los atributos que se visualicen en cada formato de lista de resultados ◆ Qué formato de visualización de la lista de resultados producirá una búsqueda ◆ El orden de clasificación por defecto de los formatos de la lista de resultados Si desea obtener más información, consulte Sección 20.2.2, “Configuración de las preferencias de la lista de búsqueda”, en la página 302
5	Probar los valores	Verifique que las listas de resultados muestren los atributos deseados.
6	Defina los derechos de eDirectory y establezca los índices que sean necesarios para mejorar el rendimiento	Derechos de eDirectory: Para ejecutar una búsqueda ◆ El usuario que ejecute la búsqueda debe tener derechos de **Browse** (Examinación) sobre cualquier usuario u objeto donde se busque. Para guardar una búsqueda (en el caso de los usuarios no administrativos): ◆ **Trustee** de la unidad administrativa y de la organización en la que ejecutarán la búsqueda. ◆ **Usuario** necesita derechos de escritura, derechos sobre sí mismo y derecho de Supervisión. **Mejora del rendimiento:** el rendimiento de la búsqueda se puede mejorar añadiendo un índice de valor de eDirectory al atributo en el que se basa la búsqueda.

Para obtener más información acerca de cómo definir los diversos formatos de visualización de la lista de resultados, consulte Sección 20.2.2, “Configuración de las preferencias de la lista de búsqueda”, en la página 302.

20.2.1 Configuración del nivel de abstracción del directorio

Las entidades y atributos que se pueden seleccionar en la lista desplegable de criterios de búsqueda y los datos devueltos por las búsquedas del repositorio seguro de identidades, deben estar definidos en el nivel de abstracción del directorio. La tabla siguiente muestra las propiedades que deben definirse para las entidades y atributos utilizados por la lista de búsqueda.

Tipo de definición	Configuración	Valor del nivel de abstracción del directorio
entity	view	Seleccionado (true)
attribute	enable	Seleccionado (true)
	search	Seleccionado (true) Cuando el valor sea false, no se podrá definir una búsqueda en este atributo, ni incluirlo en el formato de la lista de resultados
	hide	No seleccionado (false) Todos los atributos que tengan search seleccionado (true) deben tener también definido hide como no seleccionado (false) ya que el portlet Lista de búsqueda no examina el valor de la propiedad hide durante la búsqueda (ya que obstaculiza el rendimiento). Supongamos que User1 define el atributo HomePhone como hide=true (en eDirectory). HomePhone se puede buscar, por lo que Lista de búsqueda recupera el registro, pero no examina los valores de los atributos restantes (repercutiría sobre el rendimiento). Si otro usuario buscase una correspondencia exacta para el atributo HomePhone, el registro oculto se mostraría en la lista de resultados.

Otros valores del nivel de abstracción del directorio Los tipos de datos, tipos de formato, filtros y ámbito de búsqueda del nivel de abstracción del directorio también repercuten sobre el portlet Lista de búsqueda. El tipo de datos y de formato repercuten sobre la apariencia, mientras que el filtro y el ámbito de búsqueda repercuten sobre el volumen de datos devuelto.

Si desea obtener más información, consulte Sección 4.3, “Funcionamiento de las entidades y los atributos”, en la página 87.

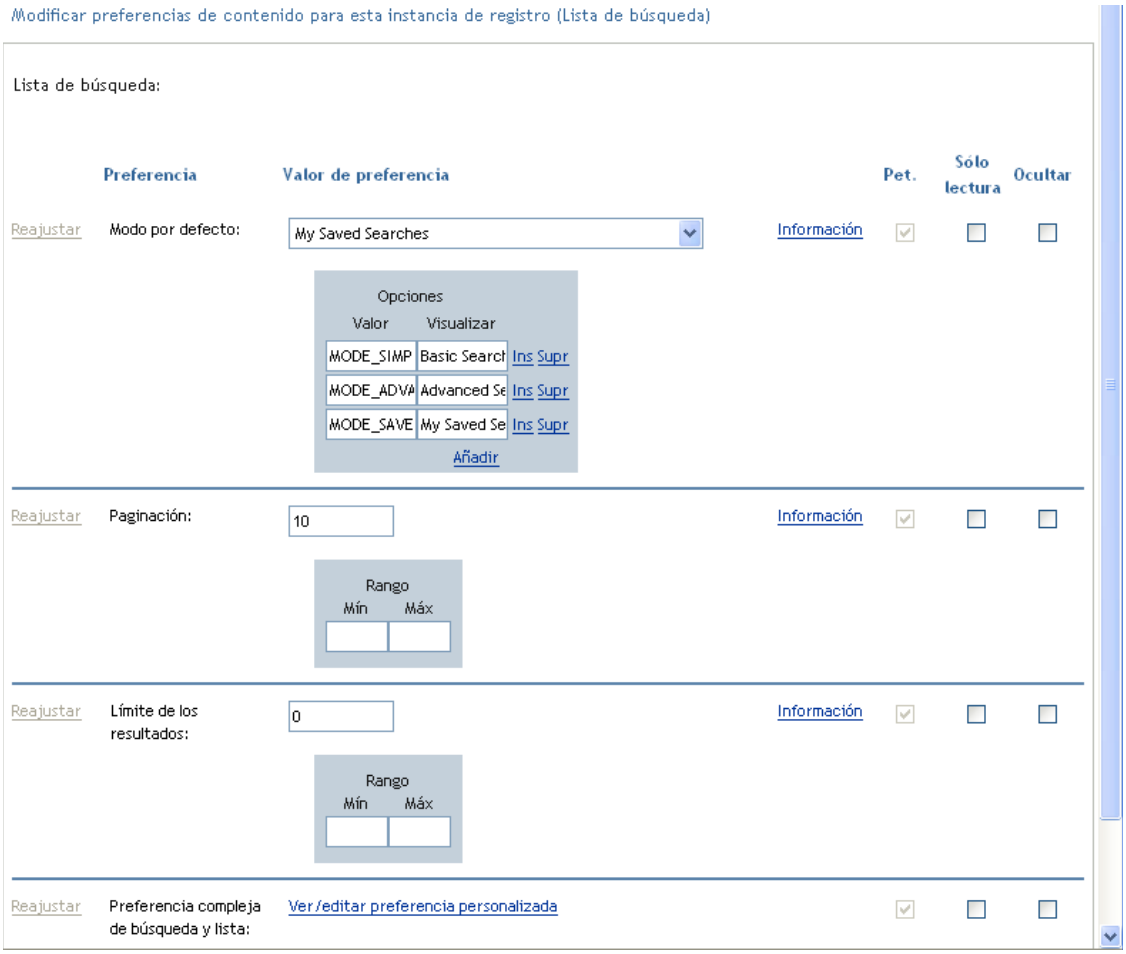
20.2.2 Configuración de las preferencias de la lista de búsqueda

Se definen dos tipos de preferencias:

- “Preferencias de búsqueda” en la página 303
- “Preferencias de formato de Lista de resultados” en la página 305

Preferencias de búsqueda

Las preferencias de búsqueda están contenidas en una única página de preferencias:



A continuación, definimos las preferencias de búsqueda:

Preferencia	Operaciones que puede realizar

Modo por defecto	Especificar cómo desea que el portlet se visualice cuando un usuario acceda por primera vez a él. Los valores son:
	
	Búsqueda básica: permite que los usuarios introduzcan un único criterio de búsqueda. Por ejemplo:
	
	`El nombre empieza por A`
	
	Búsqueda avanzada: permite que los usuarios definan varios criterios en uno o varios bloques de búsqueda. Los usuarios pueden utilizar los operadores lógicos "and" y "or" dentro de los criterios de búsqueda o en los bloques de búsqueda. Por ejemplo, los usuarios pueden crear una búsqueda como la siguiente:
	
	`(Nombre empieza por A o Nombre empieza por B) y (Región = Nordeste o Región = Sureste)`
	
	O
	
	`(Nombre empieza por A y Nombre empieza por B) o (Nombre empieza por B y Apellido empieza por A )`**`Mis búsquedas guardadas:`** `muestra una lista de las búsquedas que el usuario conectado actualmente ha guardado. Las búsquedas se guardan en el atributo srvprvQueryList del usuario.`
	
	Nota: Los usuarios pueden acceder a cualquiera de estos modos en el tiempo de ejecución, ejecutando o editando una búsqueda o haciendo clic en un botón en la parte inferior del portlet.

Paginación	Número máximo de filas que se muestra a la vez.
Límite de resultados	Número máximo de coincidencias que devuelve la búsqueda. Si el valor está definido en 0, el máximo adoptará el valor del nivel de abstracción del directorio.
Preferencia compleja de búsqueda y lista	Haga clic para ajustar: ◆ Las entidades que se buscarán ◆ El tipo de resultado definido ◆ Los atributos que se incluirán en las páginas y el orden en que aparecerán Por defecto, todos los objetos listados en el nivel de abstracción del directorio que tengan el atributo view=true, se incluirán en la búsqueda. La lista de atributos de la entidad se obtiene de los atributos listados en el nivel de abstracción del directorio, cuya definición sea enable=true.

Preferencias de formato de Lista de resultados

La página de preferencias complejas permite definir las entidades que se incluirán en la búsqueda y cómo dar formato a la lista de resultados. La página de preferencias por defecto tiene una apariencia como la que mostramos a continuación:

Las preferencias complejas son:

Preferencia	Operaciones que puede realizar
Definición de entidad	Todos los objetos que se puedan buscar (view=true) tienen en esta página de preferencias un bloque de definición de entidad correspondiente. Utilice estas preferencias para: ◆ Definir los objetos incluidos en la búsqueda. ◆ Modificar las definiciones de formato de la lista de resultados (como añadir y eliminar los atributos que se visualizan y su orden de clasificación por defecto). ◆ Eliminar los objetos que no desee incluir en la búsqueda, haciendo clic en el botón de supresión que aparece en la línea de Definición de entidad. De esta manera, eliminará el bloque completo de definición de la entidad. Más tarde, puede volver a añadir el objeto a la búsqueda, haciendo clic en **Añadir definición de entidad** (situado en la parte inferior de la página) y completando los paneles de selección del asistente. **Sugerencia:** Si un objeto no aparece en la lista, pero está listado en el nivel de abstracción del directorio, compruebe el modificador **view** (en el objeto Entidad). Si está definido en false, los portlets de identidad no podrán utilizar la entidad.
Mostrar correo electrónico como icono	Cuando esté definido en true y la lista de resultados tenga especificado un atributo Email, se visualizará como un icono. Cuando esté definido en false, el atributo Email mostrará la dirección completa de correo electrónico. El atributo email (ya sea texto o icono) es un enlace de correo sobre el que se puede hacer clic.
Tipos de lista de resultado (valor por defecto)	Especifica el formato por defecto de la lista de resultados de la entidad actual. El valor por defecto se utiliza únicamente cuando el usuario actual no ha seleccionado otro formato.
Bloque de formato de visualización de la lista de resultados	Especifica el formato de visualización (como páginas de identidad, ubicación o de organización) e incluye el conjunto de atributos que se incluirán para el tipo. **Para eliminar un tipo de lista de resultado:** ◆ Haga clic en el botón de supresión que aparece junto a Tipo de lista de resultado. Esto eliminará de la búsqueda, el tipo de página y todos los atributos asociados. **Para añadir una página de conjunto de resultados:** ◆ Haga clic en el botón de expansión y seleccione el formato de conjunto de resultados en la lista de opciones.

Preferencia	Operaciones que puede realizar
Atributos	Especifica el conjunto de atributos que se visualizarán para un formato de visualización concreto. **Para añadir o eliminar un atributo:** ◆ Haga clic en el botón Modificar atributos. ◆ Para añadir un atributo, selecciónelo (en la lista de atributos disponibles). ◆ Haga clic en la flecha para moverlo a la lista Seleccionado. Ejecute la operación inversa para eliminar un atributo de la lista de resultados. ◆ Para reordenar la lista de atributos, haga clic en las flechas hacia arriba y hacia abajo situadas a la derecha de la lista seleccionada. ◆ Haga clic en **Enviar**. **Tipos de atributos y datos**: los tipos de datos del atributo influyen sobre la forma en que se visualizan. Por ejemplo, si un atributo se define como subtipo de la lista local o la lista global, los posibles valores se mostrarán en un recuadro de lista desplegable de las pantallas de criterios de búsqueda básica o avanzada. Si el tipo es DN, se visualizará un botón de historial y un botón de búsqueda para permitir que los usuarios seleccionen un valor en las pantallas de criterios de búsqueda básica o avanzada, y el DN se determinará en una pantalla fácil en la lista de resultados. Los tipos y subtipos de datos también restringen el operador de comparaciones que se muestra para el usuario, para asegurarse de que sólo se construyen comparaciones válidas. Si desea obtener más información, consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.
Orden del bloque de formato de visualización de la lista de resultados	El orden de clasificación de la lista de resultados se basa en este atributo y sólo entra en vigor si el tipo de conjunto de resultados no es el formato de visualización de la sesión de usuario actual. **Atributos multivalentes y monovalentes**: el número de registros visualizados en la lista de resultados dependerá de que el atributo de clasificación sea multivalente o monovalente. Por lo general, la clasificación en los atributos multivalentes dará como resultado más registros, aunque el número total de coincidencias siga siendo el mismo. Esto se debe a que cada valor de un atributo multivalente se muestra por si mismo en una línea.

Cumplimentación del panel de preferencias

Para verificar que ha enviado entradas válidas, haga clic en *Enviar*. Si una entrada no es válida, verá un mensaje de error en la parte superior de la página de preferencias. Cuando haya solucionado todos los errores, haga clic en *Regresar a la vista de lista* y, a continuación, en *Guardar preferencias*.

Diseño y gestión de peticiones de provisión

V

En estos capítulos se describe cómo utilizar las funciones del módulo de provisión del Gestor de identidades.

Introducción a la provisión basada en el flujo de trabajo

21

En este capítulo se ofrece una descripción general de la provisión basada en el flujo de trabajo. Los temas son:

21.1 Acerca de la provisión basada en el flujo de trabajo

Una función clave del Gestor de identidades es la *provisión basada en el flujo de trabajo*, que es el proceso de gestionar el acceso de usuarios a los recursos seguros de una organización. Entre estos recursos se pueden incluir entidades digitales tales como las cuentas de usuario, equipos y bases de datos. En esta versión, los recursos aprovisionados se asignan a los derechos del Gestor de identidades.

El Gestor de identidades puede atender una amplia gama de *peticiones de provisión*. Dichas peticiones son acciones de usuarios o del sistema cuyo objetivo es otorgar acceso a recursos de la organización (o revocarlo). Los puede iniciar directamente el usuario final a través de la aplicación de usuario del Gestor de identidades o indirectamente en respuesta a eventos que se producen en el repositorio seguro de identidades (eDirectory).

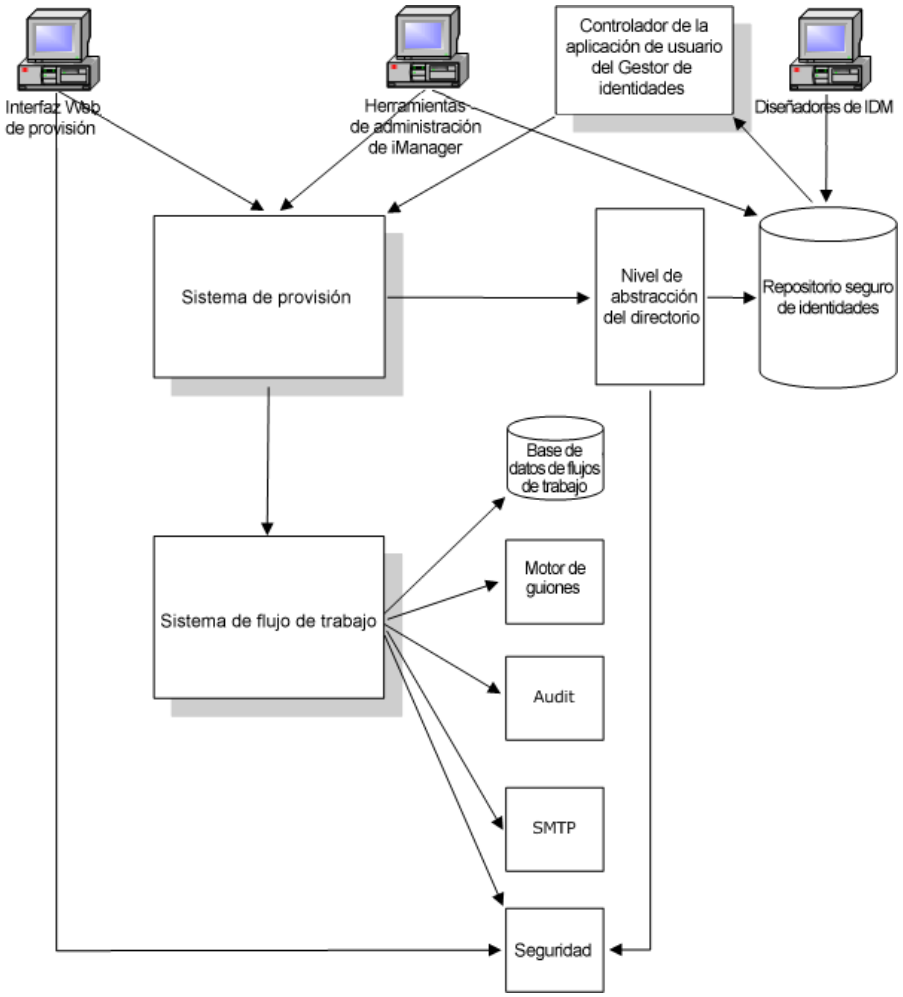
Cuando una petición de provisión requiere permiso de una o varias personas de una organización, la petición inicia un flujo de trabajo. El flujo de trabajo coordina las *aprobaciones* necesarias para cumplir la petición. Algunas peticiones de provisión requieren la aprobación de una sola persona, mientras que otras requieren la aprobación de varias personas. En algunos casos, una petición se puede cumplir sin ningún tipo de aprobación.

Algunos flujos de trabajo requieren que el proceso sea *secuencial*, en el que cada paso de aprobación se ejecute secuencialmente. Otros flujos de trabajo dan soporte a un modo de proceso *paralelo*. Cuando defina una petición de proceso, debe especificar si desea que el flujo de trabajo admita el proceso secuencial o paralelo.

El Gestor de identidades proporciona un conjunto de herramientas basadas en Web que el administrador puede utilizar para crear funciones de provisión en la aplicación de usuario. Dichas herramientas le proporcionan la capacidad de configurar peticiones de provisión y de gestionar flujos de trabajo en proceso. Para configurar una petición de provisión, el administrador crea una *definición de petición de provisión* que vincula el recurso a un flujo de trabajo.

21.1.1 Arquitectura de alto nivel

El diagrama siguiente muestra la arquitectura de alto nivel del sistema de provisión basado en el flujo de trabajo incluido con el Gestor de identidades:



En las secciones siguientes se describe cada uno de los componentes de esta arquitectura.

Interfaz Web de provisión

La aplicación de usuario del Gestor de identidades proporciona una interfaz Web a través de la cual, los usuarios finales pueden enviar peticiones de provisión y gestionar estas peticiones una vez han sido enviadas. La aplicación de usuario también proporciona al administrador de la aplicación de usuario o a un supervisor de la organización, la capacidad de asignar delegados y apoderados (proxy) a flujos de trabajo de provisión.

Sugerencia: Las acciones de flujo de trabajo y de provisión están disponibles en la pestaña *Peticiones y aprobaciones* de la aplicación de usuario del Gestor de identidades.

Si desea más información acerca de delegados y apoderados (proxy), consulte Sección 21.3, “Seguridad de la provisión”, en la página 321. Para obtener información completa acerca de cómo

trabajar con la aplicación de usuario, consulte *Aplicación de usuario del Gestor de identidades: Guía del usuario*.

Herramientas de administración de iManager

iManager proporciona módulos auxiliares que puede utilizar para configurar y gestionar peticiones de provisión y sus flujos de trabajo asociados.

Para configurar una petición de provisión, es preciso asociarla a un recurso aprovisionado, especificar las características de tiempo de ejecución del flujo de trabajo asociado y habilitarla para utilizarla. Una vez se ha iniciado una petición de provisión, puede utilizar iManager para ver el estado del proceso de flujo de trabajo, reasignar actividades dentro del flujo de trabajo o terminar el flujo de trabajo en caso de que se bloquee.

Controlador de la aplicación de usuario del Gestor de identidades

Además de dar soporte a las peticiones de recursos de provisión del usuario final, el Gestor de identidades permite iniciar peticiones de provisión como respuesta a eventos que se producen en eDirectory. El *controlador de la aplicación de usuario* del Gestor de identidades escucha los eventos y responde iniciando las peticiones de provisión correspondientes. A su vez, dichas provisiones pueden iniciar flujos de trabajo que gestionen el proceso de aprobación. Por ejemplo, el Gestor de identidades, si está configurado para ello, admitirá un caso en el que la adición de un nuevo usuario en eDirectory inicie automáticamente una petición de provisión y un flujo de trabajo designados previamente.

Sistema de provisión

El sistema de provisión ejecuta todo el proceso necesario para iniciar y cumplir las peticiones de provisión. Si una petición necesita una o varias aprobaciones, el sistema de provisión llama, a su vez, al sistema de flujo de trabajo para iniciar el proceso de flujo de trabajo. Una vez otorgadas las aprobaciones necesarias, el sistema de provisión aporta el recurso tal como se ha solicitado.

El sistema de provisión mantiene información acerca de las peticiones de provisión disponibles y pendientes del repositorio seguro de identidades (eDirectory).

Para iniciar una petición o ejecutar el proceso necesario para cumplir una petición, el sistema accede al repositorio seguro de identidades a través del nivel de abstracción del directorio.

Si desea información acerca del nivel de abstracción del directorio , consulte Capítulo 4, “Configuración del nivel de abstracción del directorio”, en la página 75.

Sistema de flujo de trabajo

Cuando una petición de provisión necesita una o varias aprobaciones, el sistema de provisión coordina el proceso de aprobación. En el curso del proceso, interactúa con los componentes siguientes:

- Base de datos de flujos de trabajo
- Motor de guiones
- Audit
- SMTP
- Sistema de seguridad

Base de datos de flujos de trabajo

Para realizar el seguimiento del estado de los flujos de trabajo en proceso, el sistema de flujo de trabajo almacena la información en una base de datos. Dicha base de datos mantiene información acerca de las instancias de procesos de flujos de trabajo, de las listas de trabajo (colas) y de los receptores de flujos de trabajo. Además, almacena los comentarios añadidos durante la ejecución de un proceso de flujo de trabajo.

Motor de guiones

El sistema de flujo de trabajo llama al motor de guiones siempre que un flujo de trabajo incluye una expresión dinámica que debe evaluarse. Las expresiones dinámicas pueden incluir variables, funciones y operadores, así como referencias a entidades del nivel de abstracción del directorio.

Novell Audit

Para registrar información acerca del estado de un proceso de flujo de trabajo, el sistema de flujo de trabajo interactúa con Novell Audit. En el curso del proceso, un flujo de trabajo puede registrar información acerca de diversos eventos que se producen. A continuación, los usuarios pueden utilizar las herramientas de generación de informes de Novell Audit para mirar los datos de registro.

Para obtener información acerca de cómo configurar el registro, consulte Capítulo 5, “Configuración de las entradas”, en la página 119. Para obtener información acerca de cómo controlar los niveles de registro de los mensajes que desea que la aplicación de usuario del Gestor de identidades genere, consulte Capítulo 12, “Configuración del registro”, en la página 213.

SMTP

A menudo, un proceso de flujo de trabajo envía notificaciones por correo electrónico a diversos puntos en el transcurso de ejecución. Por ejemplo, se puede enviar un mensaje de correo electrónico cuando se asigna una actividad de flujo de trabajo a un receptor nuevo.

Un administrador puede editar una plantilla de correo electrónico en iManager y utilizar dicha plantilla en un proceso de flujo de trabajo. En el tiempo de ejecución, el sistema de flujo de trabajo la recupera de eDirectory y sustituye las etiquetas con el texto dinámico adecuado para la notificación.

Las notificaciones por correo electrónico se gestionan mediante protocolo simple de transferencia de correo (SMTP)

Si desea información sobre los pasos de configuración básicos de la notificación por correo electrónico, consulte Sección 23.3, “Configuración del servidor de correo electrónico”, en la página 356 y Sección 23.4, “Funcionamiento con las plantillas de correo electrónico instaladas”, en la página 357. Si desea información sobre cómo configurar la notificación por correo electrónico de un flujo de trabajo, consulte “Configuración de las actividades del flujo de trabajo” en la página 338.

Seguridad

El sistema de seguridad gestiona todos los aspectos relativos a la seguridad de una aplicación de provisión basada en flujos de trabajo.

Para obtener más información acerca de la seguridad de los flujos de trabajo, consulte Sección 21.3, “Seguridad de la provisión”, en la página 321.

21.1.2 Ejemplo de provisión y de flujo de trabajo

Supongamos que un usuario necesita una cuenta en un sistema de TI. Para configurar la cuenta, el usuario inicia una petición a través de la aplicación de usuario del Gestor de identidades. Dicha petición inicia un flujo de trabajo, que coordina un proceso de aprobación. Una vez otorgadas las aprobaciones necesarias, la petición se cumple. El proceso tiene tres pasos básicos, tal como se indica a continuación.

Paso 1: Inicio de la petición

En la aplicación de usuario Gestor de identidades, el usuario examina una lista de recursos por *categoría* y selecciona una para la provisión. En el repositorio seguro de identidades, el *recurso aprovisionado* seleccionado se asocia a una *definición de petición de provisión*. La definición de petición de provisión es el objeto más prominente de un sistema de provisión. Asocia un recurso aprovisionado a un *flujo de trabajo* y actúa como medio a través del cual el proceso de flujo de trabajo se expone al usuario final. La definición de la petición de provisión proporciona toda la información necesaria para mostrar el *formulario de petición inicial* al usuario y para iniciar el flujo que sigue a la petición inicial.

En este ejemplo, el usuario selecciona el recurso Cuenta nueva. Cuando el usuario inicia la petición, la aplicación Web recupera el formulario inicial de la petición y la descripción de los *datos iniciales de la petición* asociados del Sistema de provisión el cual, a su vez, obtiene estos objetos de la definición de petición de provisión.

Cuando se inicia una petición de provisión, el Sistema de provisión realiza un seguimiento del iniciador y del destinatario. El *iniciador* es la persona que ha realizado la petición. El *destinatario* es la persona para la que se ha realizado la petición. En algunos casos, el iniciador y el destinatario pueden ser la misma persona.

Cada petición de provisión tiene una *operación* asociada. La operación especifica si el usuario desea *otorgar* o *revocar* el recurso.

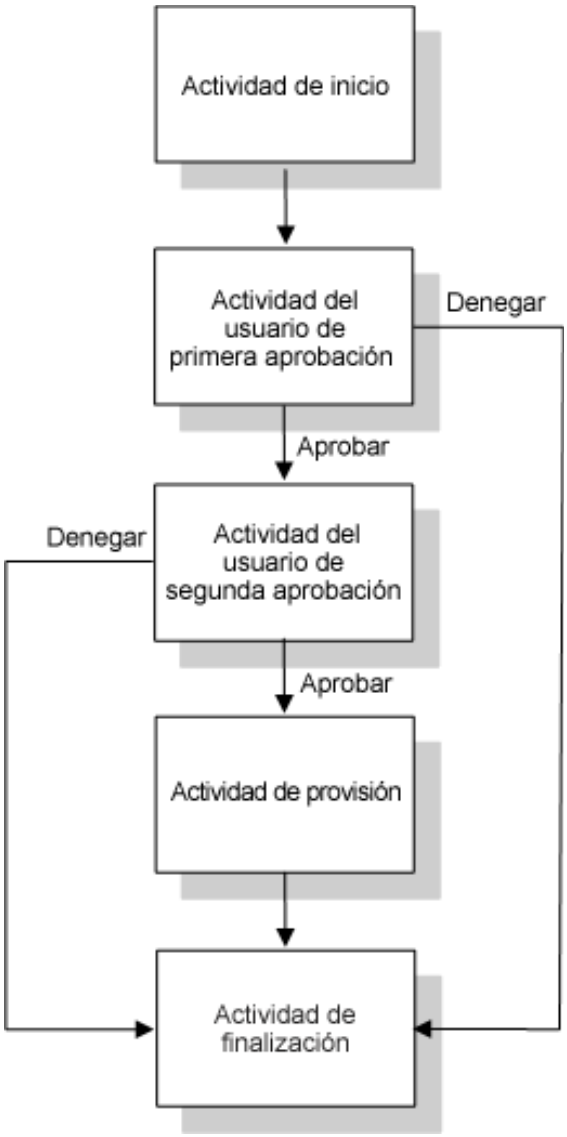
Paso 2: Aprobación de la petición

Una vez el usuario ha iniciado una petición, el Sistema de provisión inicia el proceso de flujo de trabajo. El *proceso de flujo de trabajo* coordina las aprobaciones. En este ejemplo, se necesitan dos niveles de aprobación; uno del gestor del usuario y otro del supervisor del gestor. Si algún usuario del flujo de trabajo rechaza la aprobación, el flujo terminará y se denegará la petición.

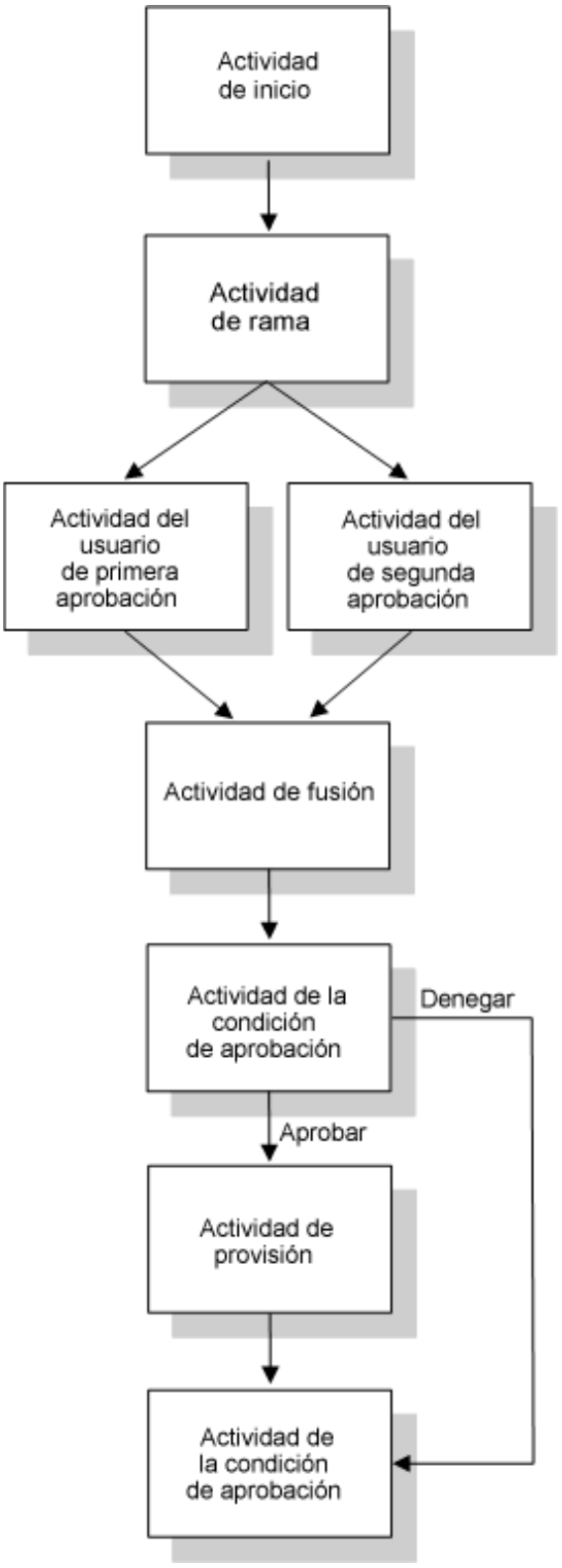
Nota: El Gestor de identidades se entrega con un conjunto de plantillas de provisión que admiten un máximo de cinco niveles de aprobación del flujo de trabajo. En una versión de seguimiento del Gestor de identidades, el entorno de diseño basado en Eclipse proporciona las herramientas que permiten crear procesos de flujo de trabajo personalizados propios. Si desea más información acerca de las plantillas que se entregan con esta versión, consulte Sección 22.2, “Funcionamiento con las plantillas instaladas”, en la página 326.

Los flujos de trabajo pueden procesar las aprobaciones de forma secuencial o paralela. En un *flujo de trabajo secuencial*, cada tarea de aprobación debe procesarse antes de que empiece la tarea de aprobación siguiente. En un *flujo de trabajo paralelo*, los usuarios pueden trabajar simultáneamente en las tareas de aprobación.

Flujo secuencial A continuación, mostramos el patrón de diseño básico de un flujo de trabajo secuencial con dos aprobaciones:



Flujo paralelo A continuación, mostramos el patrón de diseño básico de un flujo de trabajo paralelo con dos aprobaciones:



Nota: Las etiquetas de visualización (Primera aprobación, Segunda aprobación, etc.) se pueden cambiar fácilmente para adaptarlas a los requisitos de la aplicación. En el caso de los flujos

paralelos, puede especificar etiquetas que no impliquen un proceso secuencial. Por ejemplo, puede asignar etiquetas como Una de tres aprobaciones paralelas, Dos de tres aprobaciones paralelas, etc.

La definición de flujo de trabajo está formada por los componentes siguientes

Componentes del proceso	Descripción
Actividades	Una actividad es un objeto que representa una tarea. La actividad puede presentar información al usuario y responder a las interacciones de éste o ejecutar funciones en segundo plano que el usuario no puede ver. En los ejemplos de flujo de trabajo anteriores, las actividades se presentan por recuadros. En la aplicación de usuario del Gestor de identidades, las actividades de usuario que gestionan el proceso de aprobación se denominan **tareas**. Un usuario final puede ver la lista de tareas de su cola, haciendo clic en **Mis tareas** en el grupo de acciones **Mi trabajo**. Para ver qué actividades del flujo de trabajo se han procesado para una tarea determinada, el usuario puede seleccionar la tarea y hacer clic en el botón **Ver historial de comentarios** del formulario Información de la tarea. Para ver qué actividades del flujo de trabajo se han procesado para una petición de provisión determinada, el usuario puede hacer clic en **Mis peticiones**, seleccionar la petición y hacer clic en el botón **Ver comentario e historial del flujo** del formulario Información de la petición. Si desea información acerca de las acciones **Mis tareas** y **Mis peticiones**, consulte *Aplicación de usuario del Gestor de identidades: Guía del usuario*.
Enlaces	Los enlaces vinculan entre sí las actividades de un flujo de trabajo. Un enlace representa la vía que debe seguirse entre dos actividades. Una actividad puede tener varios enlaces de entrada y varios enlaces de salida. Cuando una actividad tiene más de un enlace de salida, el enlace seleccionado dependerá del **resultado** de la actividad. El resultado es el resultado final del proceso efectuado por la actividad. Por ejemplo, una actividad Usuario puede tener el resultado aprobado o denegado, según la **acción** que ejecute el usuario. En los ejemplos de flujo de trabajo anteriores, los enlaces se representan mediante flechas.

Actividad de inicio El proceso del flujo de trabajo empieza por la ejecución de la *actividad de inicio*. Esta actividad inicializa un documento de trabajo con los datos de la petición inicial. Asimismo, asocia varios valores del sistema como el iniciador y el destinatario, para que se puedan utilizar en las expresiones de guión.

Actividades de usuario Cuando finaliza la ejecución de la actividad de inicio, el Sistema de flujo de trabajo remite el proceso a la primera *actividad de usuario* en el flujo. Una actividad de usuario es una actividad que admite interacciones del usuario. Para gestionar dichas interacciones, la actividad muestra un formulario que permite que el usuario actúe en la petición. En los ejemplos de flujo de trabajo anteriores, `First approval` (Primera aprobación) y `Second approval` (Segunda aprobación) son ejemplos de actividades de usuario. Las etiquetas de visualización de las actividades de usuario se pueden localizar para satisfacer requisitos internacionales.

Una actividad de usuario puede admitir una o varias de las *acciones* siguientes:

- Reclamar
- Aprobar
- Denegar
- Rechazar
- Reasignar (disponible únicamente para los supervisores administrativos y los administradores de la aplicación de usuario)

Nota: Los campos y los botones del formulario varían en función del recurso solicitado y de cómo se ha configurado el flujo de trabajo. Por ejemplo, la acción *Rechazar*, no tiene soporte de varias de las plantillas que se entregan con el producto.

Una actividad de usuario puede tener cinco *resultados* posibles:

- Aprobado
- Denegado
- Rechazado
- Error
- Tiempo límite

Nota: Los resultados Error y Tiempo límite pueden producirse sin que el usuario haya llevado a cabo ninguna acción.

Si el usuario aprueba la petición, el flujo de trabajo remite el control a su siguiente actividad. Si no se necesita ninguna aprobación más, se aprovisionará el recurso. Si el usuario deniega la petición, el elemento de trabajo se remite a la actividad siguiente del flujo de trabajo y la petición se denegará. Por otra parte, el usuario puede volver a asignar la tarea (si es supervisor administrativo o administrador de la aplicación de usuario), lo que pondrá el elemento de trabajo en la cola de otro usuario.

Nota: Las plantillas de petición de provisión están configuradas para terminar un proceso de flujo de trabajo cuando se deniega una petición. Cuando se produce esta situación, el elemento de trabajo se remite a la actividad de finalización, que termina el flujo.

El usuario al que se ha asignado una actividad de usuario se denomina *receptor*. Al receptor, se le puede notificar la tarea asignada mediante correo electrónico. Para realizar el trabajo asociado a la actividad, el receptor puede hacer clic en la URL en el correo electrónico, encontrar la tarea en la lista de trabajo (cola) y reclamarla.

The addressee must respond to a User activity within a specified amount of time, or the activity times out.El receptor debe responder a una actividad de usuario en un plazo de tiempo estipulado o la actividad alcanzará su tiempo límite.Normalmente, el *intervalo de tiempo límite* se expresa en horas o días, a fin de que el usuario disponga de tiempo suficiente para responder.

Cuando una actividad alcanza su tiempo límite, el proceso del flujo de trabajo puede intentar volver a completar la actividad, en función de los *reintentos* especificados. En ocasiones, el proceso de flujo de trabajo puede estar configurado para pasar la actividad que ha alcanzado su tiempo límite a otro usuario. En dicho caso, la actividad se reasigna a un receptor nuevo (por ejemplo, al supervisor

del usuario) para dar a este usuario la oportunidad de finalizar el trabajo de la actividad. En caso de que el último reintento alcance su tiempo límite, la actividad se puede marcar como aprobada o denegada, en función de cómo se haya configurado el flujo de trabajo.

Actividades condicionales Durante su ejecución, un proceso de flujo de trabajo puede realizar una prueba y ver cuál será el resultado para saber qué deberá efectuar a continuación. La *actividad condicional* permite esta capacidad. Las actividades condicionales utilizan una expresión de guión para definir la condición que se va a evaluar. En los ejemplos de flujo de trabajo que mostramos más arriba, `Approval Condition` (Condición de aprobación) es un ejemplo de actividad condicional.

Las actividades condicionales admiten tres *resultados* posibles:

- Verdadero
- Falso
- Error

Actividades de fusión y de ramificación En un flujo de trabajo que admita procesos paralelos, la *actividad de ramificación* permite que dos usuarios actúen en paralelo, en áreas diferentes del elemento de trabajo. Una vez los usuarios han finalizado el trabajo, la *actividad de fusión* sincronizará las ramas de entrada del flujo.

Actividad de provisión La *actividad de provisión* completa la petición de provisión. Esta actividad se ejecuta sólo si se han dado todas las aprobaciones necesarias.

Para obtener información acerca del paso de provisión, consulte "Paso 3: Cumplimiento de la petición" en la página 320.

Actividad de finalización La *actividad de finalización* es la actividad que pone fin a un flujo de trabajo. Una vez se han completado todas las actividades de un flujo y se dispone de su resultado final, se ejecuta la actividad de finalización. El Sistema de flujo de trabajo puede determinar el estado final del proceso examinando los enlaces de la actividad de finalización. Por lo general, cuando un enlace de aprobación llega a la actividad de finalización, el estado del flujo es *aprobado*. Si algún otro resultado (denegación, tiempo límite o error) lleva a la actividad de finalización, el flujo general del estado será *denegado*.

Cuando un proceso de flujo de trabajo llega a la actividad de finalización con el estado de aprobado, el proceso de aprobación estará completo y se podrá completar la petición de provisión.

Paso 3: Cumplimiento de la petición

Una vez aprobada una petición de provisión, el Sistema de flujo de trabajo puede iniciar el paso de *provisión*. En este punto, el control se devuelve al sistema de provisión.

Para cumplir la petición de provisión, el sistema de provisión puede ejecutar un derecho del Gestor de identidades o manipular directamente un objeto de eDirectory y sus atributos. Durante el paso de provisión, se crean todos los objetos relacionados y se registran los resultados de la acción de provisión en el destinatario, tal como se describe en la definición de los datos de provisión. En función de si el usuario solicitó una operación de otorgar o revocar, esto puede implicar definir o eliminar el valor de un atributo en el destinatario, o añadir un elemento a un atributo multivalente o eliminar un elemento de un atributo multivalente del destinatario. Los atributos implicados son atributos de eDirectory (posiblemente están disponibles después de añadir una clase auxiliar al destinatario). Los valores de atributo en sí pueden ser simples o de un tipo complejo que permita que el sistema de provisión especifique el valor de subatributos internos.

21.2 Administración y configuración de la provisión

Para configurar una definición de petición de provisión, es preciso utilizar iManager para asociar dicha definición a un recurso aprovisionado, especificar las características de tiempo de ejecución del flujo de trabajo asociado y habilitarla para su uso. El Gestor de identidades se entrega con un conjunto de flujos de trabajo y de definiciones de peticiones de provisión implantado previamente. Puede utilizar dicho conjunto como *plantillas* para crear su propio sistema de provisión. Las plantillas instaladas son fáciles de utilizar y poseen una flexibilidad que les permite responder a las necesidades de una amplia gama de entornos empresariales. Para configurar el sistema, primero deben definirse los objetos nuevos basándose en las plantillas instaladas y después es preciso personalizarlos para que se adapten a las necesidades de la organización.

Una vez configurada la definición de petición de provisión, puede utilizar iManager para ver el estado de los procesos de flujo de trabajo en curso, reasignar actividades dentro de los flujos de trabajo o terminar un flujo de trabajo en caso de que éste se bloquee.

Si desea obtener más información acerca de cómo utilizar iManager para gestionar y configurar la provisión, consulte Capítulo 22, “Configuración de las definiciones de peticiones de provisión”, en la página 325 y Capítulo 23, “Gestión de los flujos de trabajo de provisión”, en la página 347.

21.3 Seguridad de la provisión

Cuando un usuario se registra en la aplicación de usuario del Gestor de identidades, el sistema de usuario lo autentica y define los controles de acceso que permiten proteger los objetos de flujo de trabajo y de provisión contra un uso no autorizado. De esta manera, se garantiza que el usuario sólo vea las definiciones de petición de provisión sobre las que tiene otorgado derecho de acceso. Además de ejecutar servicios de autenticación y de autorización para la aplicación de usuario, el sistema de seguridad se encarga de gestionar las asignaciones de apoderados (proxy) y delegados.

- Un *delegado* es un usuario autorizado a realizar trabajo de otro usuario. Una asignación de delegado se aplica a una definición de petición de provisión concreta.
- Un *apoderado (proxy)* es un usuario autorizado a realizar cualquier trabajo de uno o varios usuarios, grupos o contenedores. A diferencia de las asignaciones de delegado, las asignaciones de apoderado (proxy) no dependen de las definiciones de peticiones de provisión y, por lo tanto, se aplican a todos los trabajos y valores.

Si el registro está habilitado, las acciones que llevan a cabo apoderados (proxy) o delegados se registran junto con las acciones llevadas a cabo por otros usuarios. Cuando un apoderado (proxy) o un delegado lleva a cabo una acción, el mensaje de registro indica claramente que la acción la ha llevado a cabo un apoderado (proxy) o un delegado de otro usuario. Además, cada vez que se define una asignación de apoderado (proxy) o de delegado, se registra también el evento.

Si se configura una definición de petición de provisión para generar notificaciones por correo electrónico, los apoderados (proxy) y los receptores recibirán las notificaciones por correo electrónico. Los delegados no se incluyen en las notificaciones por correo electrónico.

Funciones de seguridad del flujo de trabajo El sistema de seguridad reconoce las funciones de seguridad siguientes:

Función	Descripción	Derechos
Administrador de la aplicación de usuario	Usuario superAdmin con derechos administrativos completos.	El administrador de la aplicación de usuario tienen permiso para ejecutar las tareas siguientes en **iManager**: ◆ Configurar las peticiones de provisión ◆ Gestionar los flujos de trabajo que ya se están procesando El administrador de la aplicación de usuario tiene permiso para ejecutar estas tareas dentro de la **aplicación de usuario**: ◆ Ver y editar todas las tareas de todas las colas de flujos de trabajo. ◆ Definir las asignaciones de apoderados (proxy) y delegados para cualquier usuario del sistema. ◆ Ver la información oculta (atributos ocultos) de cualquier usuario del sistema. ◆ Crear supervisores de grupos de tareas y asignarlos a grupos. El administrador de la aplicación de usuario es el único usuario que puede crear y asignar supervisores de grupos de tareas. **Nota:** La pestaña **Administración** de la aplicación de usuario del Gestor de identidades proporciona herramientas para asignar derechos de administración de la aplicación de usuario. Para utilizar dicha pestaña, es preciso registrarse como el usuario que, en el momento de la instalación, se especificó como administrador de la aplicación de usuario. Para obtener información detallada acerca de las funciones de seguridad de la aplicación de usuario, consulte Capítulo 11, “Configuración de la seguridad”, en la página 209.

Función	Descripción	Derechos
Supervisor administrativo	Supervisor de un empleado. Cada usuario tiene únicamente un supervisor administrativo. **Sugerencia:** También se puede considerar que el supervisor administrativo es un tipo de gestor administrativo.	El supervisor administrativo tiene permiso para: ◆ Ver todas las tareas que se encuentran en las colas de trabajo de su equipo. Esta función se aplica a un único nivel de la jerarquía de gestión, por lo que el supervisor del supervisor administrativo no puede ver las tareas de los empleados directos del supervisor administrativo. ◆ Editar tareas para empleados directos, salvo en el caso de que un empleado directo tenga una tarea asignada a un grupo cuyo supervisor de grupos de tareas no sea el supervisor administrativo. En dicho caso, el supervisor administrativo podrá ver la tarea, pero no editarla. Si se traspasa la actividad, las tareas pasarán al supervisor de grupos de tareas y no al supervisor administrativo. ◆ Reclamar tareas y cancelar la reclamación de tareas, así como reasignar tareas a miembros de su equipo. ◆ Definir relaciones de apoderado (proxy) y delegado para sí mismo y para los miembros de su equipo. ◆ Ver los atributos ocultos de los miembros de su equipo.

Función	Descripción	Derechos
Supervisor de grupos de tareas	Responsabilidad proporcionada por el usuario sobre un conjunto de tareas asociado a un grupo de tareas. Un grupo de tareas es una extensión del objeto Grupo LDAP. Cada grupo de tareas puede tener únicamente un supervisor de grupos de tareas. El administrador de la aplicación de usuario asigna los supervisores de grupos de tareas. Cuando se asigna una tarea a un grupo, el atributo srvrprvTaskManager para el grupo contiene el DN del usuario que es el supervisor de grupos de tareas designado. A fin de mejorar el rendimiento, los supervisores de grupos de tareas también están identificados mediante un atributo en el objeto Usuario. El atributo srvprvIsTaskManager se define en true para un usuario que sea supervisor de grupos de tareas designado.	El supervisor de grupos de tareas tiene permiso para: ◆ Ver y editar todas las tareas asignadas a un grupo del cual sea el líder designado. El supervisor de grupos de tareas **no** tiene permiso para: ◆ Crear recursos ni retraer peticiones. ◆ Definir relaciones de apoderados (proxy) o delegados. ◆ Ver los atributos ocultos de los miembros de su equipo.

Nota: Todos los usuarios pueden ver los atributos ocultos asociados a su propia identidad.

Definición de las relaciones de apoderados (proxy) y delegados. Para definir una asignación de apoderado (proxy) para un usuario, utilice la página *Asignaciones de apoderado (proxy) del equipo* en la pestaña *Peticiones y aprobaciones* de la interfaz de usuario del Gestor de identidades. Para definir una asignación de delegado para un usuario, utilice la página *Asignaciones del delegado del equipo* que también está disponible en la pestaña *Peticiones y aprobaciones*.

Creación de supervisores de grupos de tareas Para definir un supervisor de grupos de tareas, utilice la página *Crear usuario o grupo* de la pestaña *Autoservicio de identidades* de la interfaz de usuario del Gestor de identidades.

Para obtener información completa acerca de cómo definir los supervisores de grupos de tareas, apoderados (proxy) y delegados, consulte el manual *Aplicación de usuario del Gestor de identidades: Guía del usuario*.

Configuración de las definiciones de peticiones de provisión

22

En este capítulo se proporcionan instrucciones para configurar definiciones de petición de provisión. Los temas son:

22.1 Acerca del módulo auxiliar de configuración de peticiones de provisión

Para configurar una definición de petición de provisión, debe utilizar el módulo auxiliar de configuración de peticiones de provisión en iManager. Este módulo auxiliar permite asociar la definición de petición de provisión a un recurso aprovisionado, especificar las características de tiempo de ejecución del flujo de trabajo asociado y habilitarla para su uso. En esta versión, los recursos aprovisionados se asignan a los derechos del Gestor de identidades.

Nota: También puede ejecutar definiciones de peticiones de provisión que se asignan directamente a atributos del repositorio seguro de identidades. No obstante, las plantillas instaladas no admiten este tipo de recurso, ya que están basados en derechos.

Puede encontrar el módulo auxiliar de configuración de peticiones de provisión en la *categoría Gestor de identidades* de iManager. El módulo auxiliar incluye la *tarea Peticiones de provisión* de la *función Configuración de la petición de provisión*. La tarea Peticiones de provisión está formada por los paneles siguientes:

Panel	Descripción
Selección del controlador de provisión	Da la oportunidad de seleccionar un controlador de la aplicación de usuario del Gestor de identidades. El controlador contiene un conjunto de definiciones de petición de provisión definido previamente, por lo que deberá elegir un controlador antes de empezar a configurar las peticiones de provisión.

Panel	Descripción
Configuración de la petición de provisión	Proporciona herramientas que permiten: ◆ Examinar las definiciones de petición de provisión disponibles y seleccionar una para configurar ◆ Crear una definición de petición de provisión basada en una definición existente ◆ Definir las propiedades de una definición de petición de provisión ◆ Asignar la definición de petición de provisión a un recurso aprovisionado ◆ Editar los valores de receptor y de tiempo límite de cada actividad del flujo de trabajo asociado Si selecciona crear una petición de provisión nueva o editar una ya existente, el módulo auxiliar ejecutará el **Asistente de configuración de petición de provisión**.

22.2 Funcionamiento con las plantillas instaladas

El Gestor de identidades se entrega con un conjunto de flujos de trabajo y de definiciones de peticiones de provisión implantado previamente. Puede utilizar dicho conjunto como *plantillas* para crear su propio sistema de provisión. Para configurar el sistema, defina los objetos nuevos basándose en las plantillas instaladas y después personalícelos para que se adapten a las necesidades de la organización.

Las plantillas instaladas permiten determinar el número de pasos de aprobación necesarios para que la petición se cumpla. Puede configurar una petición de provisión para que:

- No necesite ninguna aprobación
- Necesite un paso de aprobación
- Necesite dos pasos de aprobación
- Necesite tres pasos de aprobación
- Necesite cuatro pasos de aprobación
- Necesite cinco pasos de aprobación

También puede especificar si desea admitir el proceso secuencial o paralelo y si desea aprobar o denegar la petición, en caso de que el flujo de trabajo alcance el tiempo límite durante el proceso.

Para obtener más información acerca de los patrones de diseño de flujos de trabajo, consulte Sección 21.1.2, “Ejemplo de provisión y de flujo de trabajo”, en la página 315.

El Gestor de identidades se entrega con las plantillas siguientes:

Plantilla	Descripción
Aprobación de autoprovisión	Permite que una petición de provisión se cumpla sin ningún tipo de aprobación.

Plantilla	Descripción
Aprobación en un paso (aprobación al alcanzar el tiempo límite)	Necesita una única aprobación para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente.
Aprobación secuencial en dos pasos (aprobación al alcanzar el tiempo límite)	Necesita dos aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos secuenciales.
Aprobación secuencial en tres pasos (aprobación al alcanzar el tiempo límite)	Necesita tres aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos secuenciales.
Aprobación secuencial en cuatro pasos (aprobación al alcanzar el tiempo límite)	Necesita cuatro aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos secuenciales.
Aprobación secuencial en cinco pasos (aprobación al alcanzar el tiempo límite)	Necesita cinco aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos secuenciales.
Aprobación en un paso (denegación al alcanzar el tiempo límite)	Necesita una única aprobación para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos secuenciales.
Aprobación secuencial en dos pasos (denegación al alcanzar el tiempo límite)	Necesita dos aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos secuenciales.
Aprobación secuencial en tres pasos (denegación al alcanzar el tiempo límite)	Necesita tres aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos secuenciales.
Aprobación secuencial en cuatro pasos (denegación al alcanzar el tiempo límite)	Necesita cuatro aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos secuenciales.

Plantilla	Descripción
Aprobación secuencial en cinco pasos (denegación al alcanzar el tiempo límite)	Necesita cinco aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos secuenciales.
Aprobación paralela en dos pasos (aprobación al alcanzar el tiempo límite)	Necesita dos aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos paralelos.
Aprobación paralela en tres pasos (aprobación al alcanzar el tiempo límite)	Necesita tres aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos paralelos.
Aprobación paralela en cuatro pasos (aprobación al alcanzar el tiempo límite)	Necesita cuatro aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos paralelos.
Aprobación paralela en cinco pasos (aprobación al alcanzar el tiempo límite)	Necesita cinco aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, dicha actividad aprobará la petición y se remitirá el elemento de trabajo a la actividad siguiente. Esta plantilla admite los procesos paralelos.
Aprobación paralela en dos pasos (denegación al alcanzar el tiempo límite)	Necesita dos aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos paralelos.
Aprobación paralela en tres pasos (denegación al alcanzar el tiempo límite)	Necesita tres aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos paralelos.
Aprobación paralela en cuatro pasos (denegación al alcanzar el tiempo límite)	Necesita cuatro aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos paralelos.
Aprobación paralela en cinco pasos (denegación al alcanzar el tiempo límite)	Necesita cinco aprobaciones para que la petición de provisión se cumpla. Si una actividad alcanza el tiempo límite, el flujo de trabajo denegará la petición. Esta plantilla admite los procesos paralelos.

Flujos de trabajo y recursos aprovisionados Todas las definiciones de petición de provisión tienen un enlace preconfigurado con un flujo de trabajo y un recurso aprovisionado. Puede cambiar

el recurso aprovisionado asociado a la definición de petición, pero no el flujo de trabajo ni su topología.

Categorías de peticiones de provisión Cada una de las plantillas de petición de provisión está también enlazada con una *categoría*. Las categorías son una forma útil de organizar las peticiones de provisión para el usuario final. La categoría por defecto de todas las plantillas de petición de provisión es *Derechos*. La clave de categoría, que es el valor del atributo srvprvCategoryKey, es *derechos* (minúsculas).

Puede crear sus propias categorías utilizando el editor del nivel de abstracción del directorio. Si crea una categoría nueva, asegúrese de que la clave de categoría (el valor de srvprvCategoryKey) esté en minúsculas. Esto es imprescindible para asegurarse de que las categorías funcionen correctamente en la aplicación de usuario del Gestor de identidades.

Para obtener información acerca de cómo crear categorías de provisión, consulte Sección 4.4, “Funcionamiento con listas”, en la página 104.

22.3 Configuración de una definición de una petición de provisión

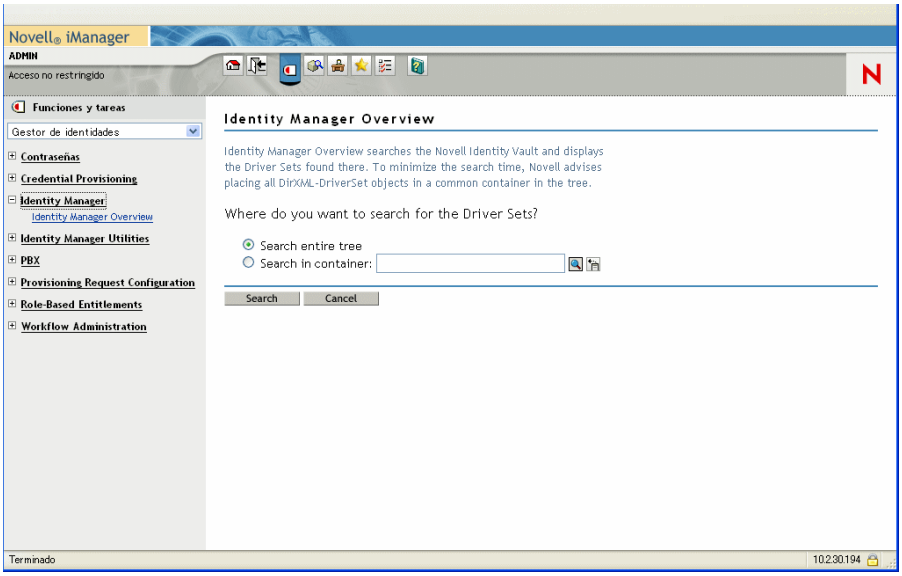
Antes de configurar una definición de petición de provisión, debe seleccionar el controlador de la aplicación de usuario del Gestor de identidades que contiene la definición. Una vez seleccionado el controlador, puede crear una definición de petición de provisión nueva o bien editar una ya existente. También puede suprimir definiciones de petición de provisión, cambiar el estado de una definición de petición o definir los derechos de una definición de petición.

22.3.1 Selección del controlador

Para seleccionar un controlador de la aplicación de usuario del Gestor de identidades:

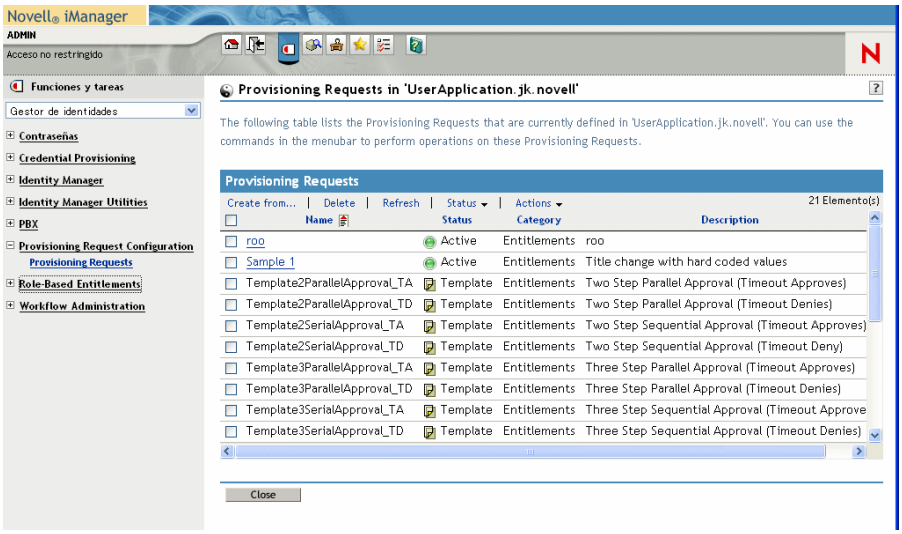
1. Seleccione la categoría *Gestor de identidades* en iManager.
2. Abra la función *Configuración de la petición de provisión*.
3. Haga clic en la tarea *Peticiones de provisión*.

iManager muestra la pantalla Controlador de la aplicación de usuario.



4 Especifique el nombre del controlador en el campo *Controlador de la aplicación de usuario* y haga clic en *Aceptar*.

iManager muestra el panel Configuración de la petición de provisión. Dicho panel muestra una lista de definiciones de petición de provisión disponibles.



Las plantillas instaladas aparecerán en texto oscuro con el estado de *Plantilla*. Las definiciones de petición que son plantillas no muestran enlaces de hipertexto, ya que son de sólo lectura.

Nota: Si las definiciones de petición se han configurado para utilizar texto localizado, los nombres y descripciones de dichas definiciones mostrarán texto adecuado para la configuración regional actual.

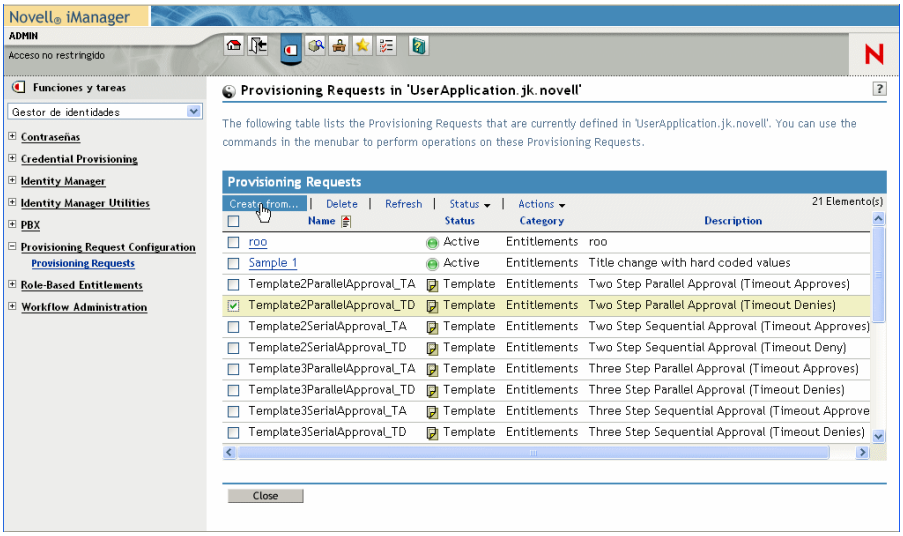
Cambio del controlador Cuando haya seleccionado un controlador, dicho controlador permanecerá en vigor mientras dure la sesión de iManager, a menos que seleccione otro controlador. Para

seleccionar otro controlador, haga clic en el comando *Acciones* y seleccione *Seleccionar el controlador de la aplicación de usuario* en el menú *Acciones*.

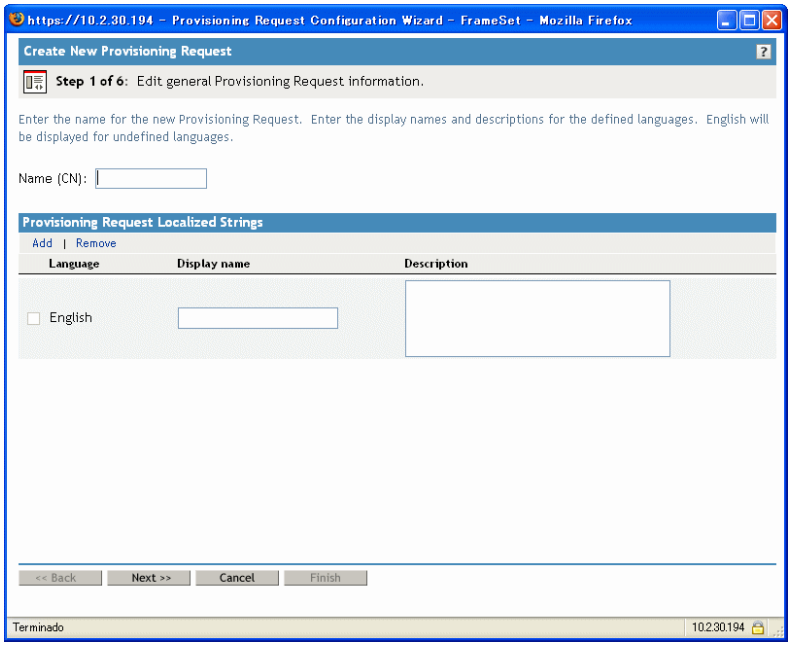
22.3.2 Creación o edición de una petición de provisión

Para crear una petición de provisión nueva:

1. Haga clic en el nombre de la petición de provisión que desee utilizar como plantilla en el panel Configuración de la petición de provisión.
2. Haga clic en el comando *Crear a partir de* del panel Configuración de la petición de provisión.



Aparecerá la primera página del asistente de configuración de petición de provisión nueva.



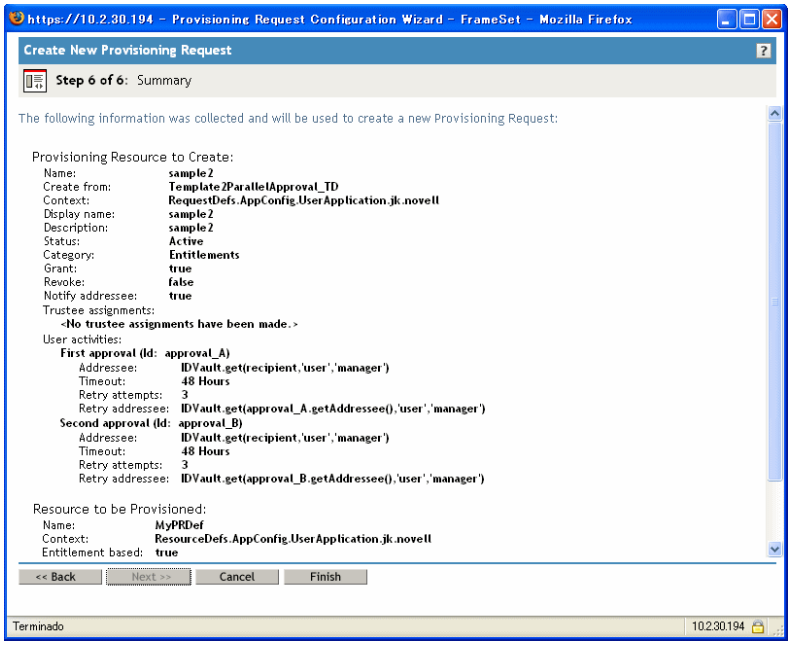
3. Escriba un nombre común para el objeto nuevo en el campo *Nombre*.

4. Por cada idioma que desee admitir en la aplicación, escriba el texto localizado en los campos *Mostrar nombre* y *Descripción* en *Cadenas localizadas de la petición de provisión*. Este texto se utilizará para identificar la petición de provisión en toda la aplicación de usuario.
5. Para añadir un idioma nuevo a la lista, haga clic en *Añadir* y seleccione el idioma deseado.

   Nota: Por defecto, las peticiones de provisión que se acaban de crear sólo admiten inglés.

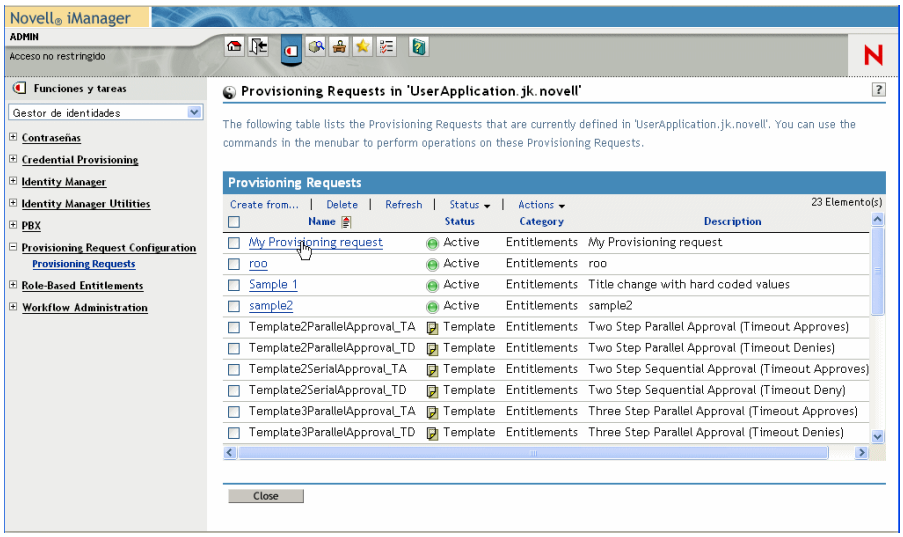
6. Haga clic en *Siguiente*.
7. Especifique el recurso aprovisionado de la definición de petición, tal como se describe en "Especificación del recurso aprovisionado" en la página 334.
8. Configure las actividades del flujo de trabajo asociadas a la definición de petición, tal como se describe en "Configuración de las actividades del flujo de trabajo" en la página 338.
9. Especifique los derechos de acceso de la definición de petición, tal como se describe en "Especificación de los derechos de acceso de la petición de provisión" en la página 342.
10. Especifique el estado inicial de la definición de petición, tal como se describe en "Especificación del estado inicial de la petición de provisión" en la página 343.

11 Revise los valores y haga clic en *Finalizar*.



Para editar una petición de provisión existente:

1 Haga clic en el nombre de la petición de provisión en el panel Configuración de la petición de provisión.



Las peticiones de provisión que sean plantillas no se pueden editar. Las definiciones de petición que tengan el estado de plantilla no muestran enlaces de hipertexto, ya que son de sólo lectura.

Nota: Si las definiciones de petición son numerosas, puede ordenar la lista por una columna en concreto, como el nombre o la descripción. Para ordenar según una columna en concreto, sólo tiene que hacer clic en el título de la columna.

---

2 Por cada idioma que desee admitir en la aplicación, haga clic en la casilla de verificación situada al lado del idioma de la lista que se encuentra en *Cadenas localizadas de la petición de provisión* y escriba el texto localizado en los campos *Mostrar nombre* y *Descripción*. Este texto se utilizará para identificar la petición de provisión en toda la aplicación de usuario.

3 Para añadir un idioma nuevo a la lista, haga clic en *Añadir* y seleccione el idioma deseado.

Nota: Por defecto, las peticiones de provisión que se acaban de crear sólo admiten inglés.

---

4 Haga clic en *Siguiente*.

5 Especifique el recurso aprovisionado de la definición de petición, tal como se describe en "Especificación del recurso aprovisionado" en la página 334.

6 Configure las actividades del flujo de trabajo asociadas a la definición de petición, tal como se describe en "Configuración de las actividades del flujo de trabajo" en la página 338.

7 Especifique los derechos de acceso de la definición de petición, tal como se describe en "Especificación de los derechos de acceso de la petición de provisión" en la página 342.

8 Especifique el estado inicial de la definición de petición, tal como se describe en "Especificación del estado inicial de la petición de provisión" en la página 343.

9 Revise los valores y haga clic en *Finalizar*.

Especificación del recurso aprovisionado

En esta sección se proporcionan instrucciones para especificar un recurso aprovisionado basado en un derecho. No proporciona información de tipo conceptual acerca de los derechos ni instrucciones para crear y utilizar dichos derechos.

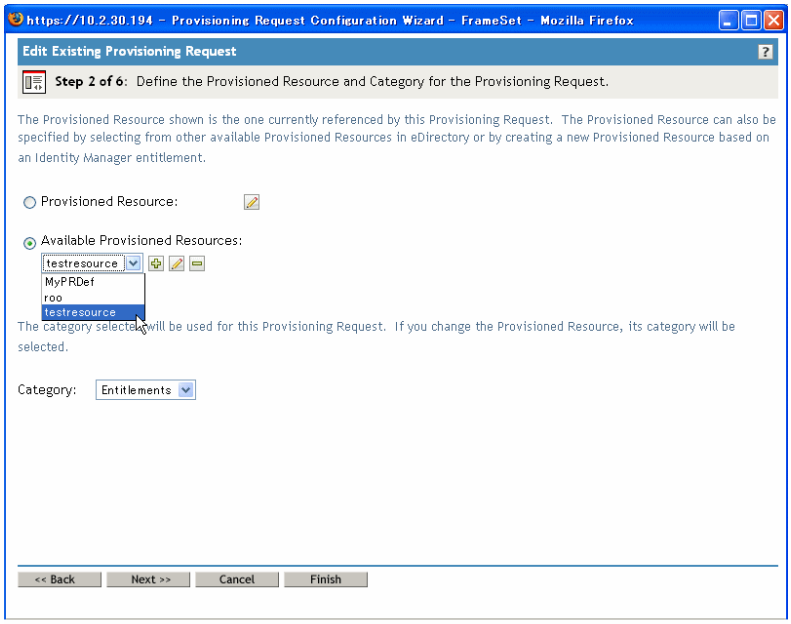
Para obtener información completa acerca de los derechos, consulte <*z-DocTitleInVariable*>*Novell Identity Manager: Administration Guide* (Gestor de identidades <z-DocTitleInVariable>: Guía del administrador).

Para especificar el recurso aprovisionado:

1 Para utilizar el destino asociado en ese momento a la definición de petición, seleccione el botón circular *Recurso aprovisionado*.

El botón circular Recurso aprovisionado está seleccionado por defecto si edita una definición de petición que se refiere a un recurso válido. Si define una petición de provisión nueva, este botón circular no está seleccionado.

2 Para asociar la definición de petición a otro recurso definido previamente en el controlador seleccionado actualmente, seleccione el botón circular *Recursos aprovisionados disponibles* y seleccione un destino en la lista desplegable.



Nota: Si la definición de petición estaba asociada a un recurso que no es un derecho, no tendrá permiso para cambiar el recurso.

3 Seleccione una categoría para la definición de recurso aprovisionado de la lista desplegable *Categoría*.

El valor por defecto de la categoría es el de la categoría del recurso aprovisionado seleccionado actualmente. Siempre que cambie el recurso aprovisionado, cambiará también la categoría de la definición de petición, a fin de que coincida con la categoría del recurso. Si desea asignar otra categoría a la definición de petición, seleccione la categoría en la lista desplegable Categoría.

4 Para crear un recurso nuevo basado en un derecho del Gestor de identidades, haga clic en el botón +.

Para editar un recurso que ya existe, haga clic en el botón de la pluma.

Para definir las características del recurso, siga los pasos que indicamos a continuación:

4a Especifique el nombre del recurso en el campo *Nombre (CN)*.

4b Seleccione una categoría para el recurso en la lista desplegable *Categoría*.

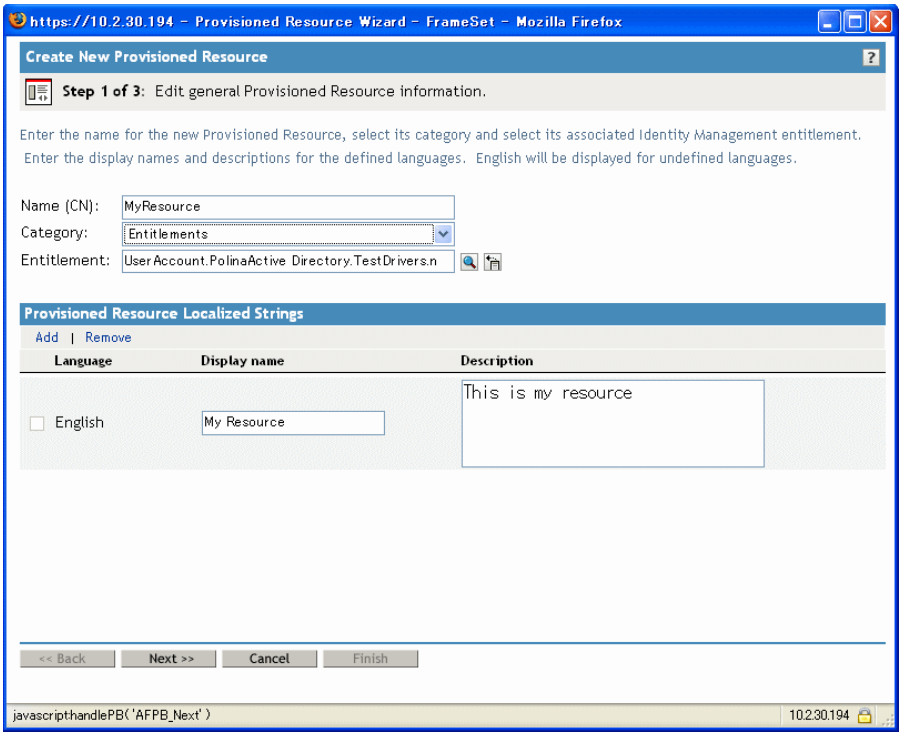
4c Especifique el derecho en el campo *Derecho*.

4d Por cada idioma que desee admitir en la aplicación, haga clic en la casilla de verificación situada al lado del idioma de la lista que se encuentra en *Cadenas localizadas del recurso aprovisionado* y escriba el texto localizado en los campos *Mostrar nombre* y *Descripción*.

Este texto se utilizará para identificar el recurso de provisión en toda la aplicación de usuario.

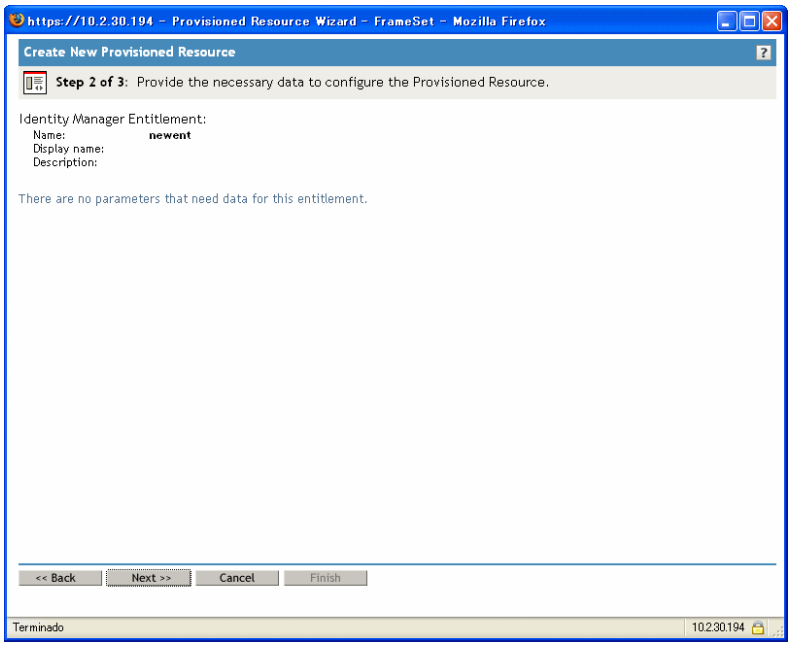
4e Para añadir un idioma nuevo a la lista, haga clic en *Añadir* y seleccione el idioma deseado.

Nota: Por defecto, los recursos de provisión que se acaban de crear sólo admiten inglés.



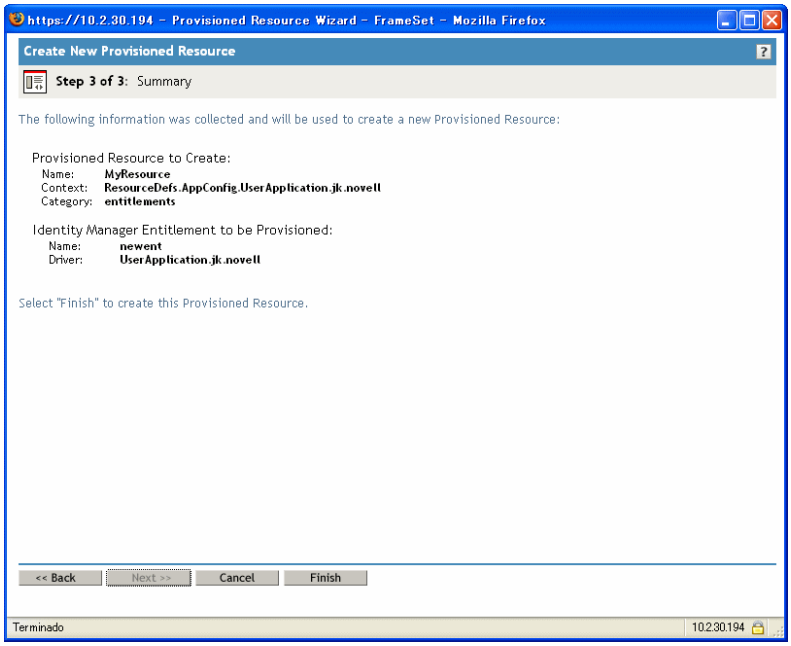
5 Haga clic en *Siguiente*.

El asistente para recursos aprovisionados mostrará una pantalla para permitir que el usuario suministre los datos de todos los parámetros necesarios para el derecho.



6 Si el derecho no necesita ningún parámetro de derecho, haga clic en *Siguiente*.

El asistente para crear un recurso aprovisionado nuevo mostrará la página Resumen, que proporciona información acerca del recurso que está definiendo.

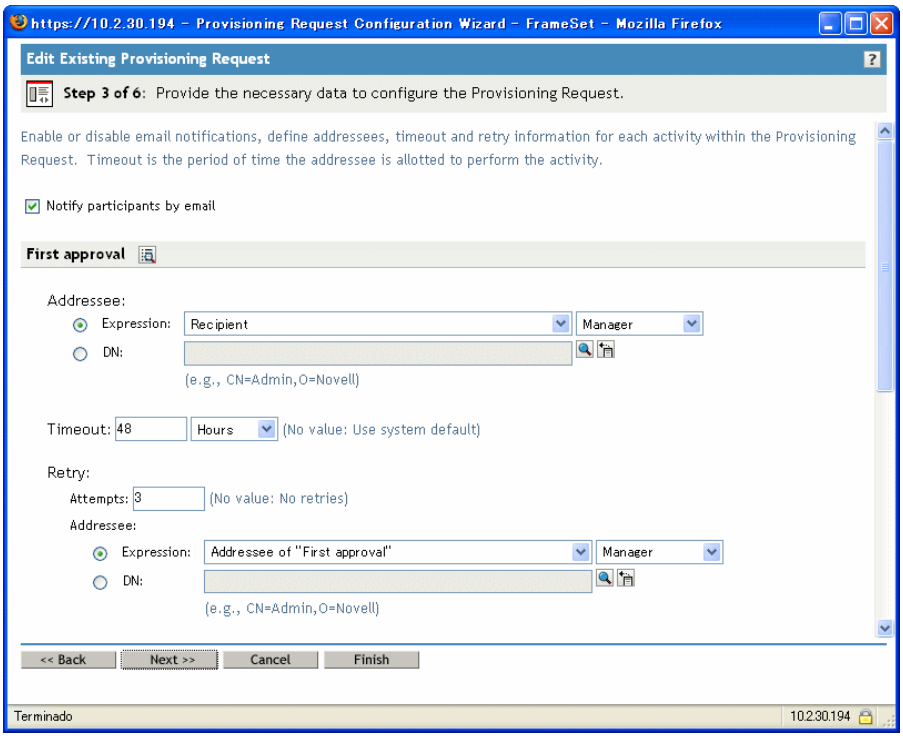


7 Haga clic en *Finalizar*.

Configuración de las actividades del flujo de trabajo

Para configurar las actividades del flujo de trabajo asociado:

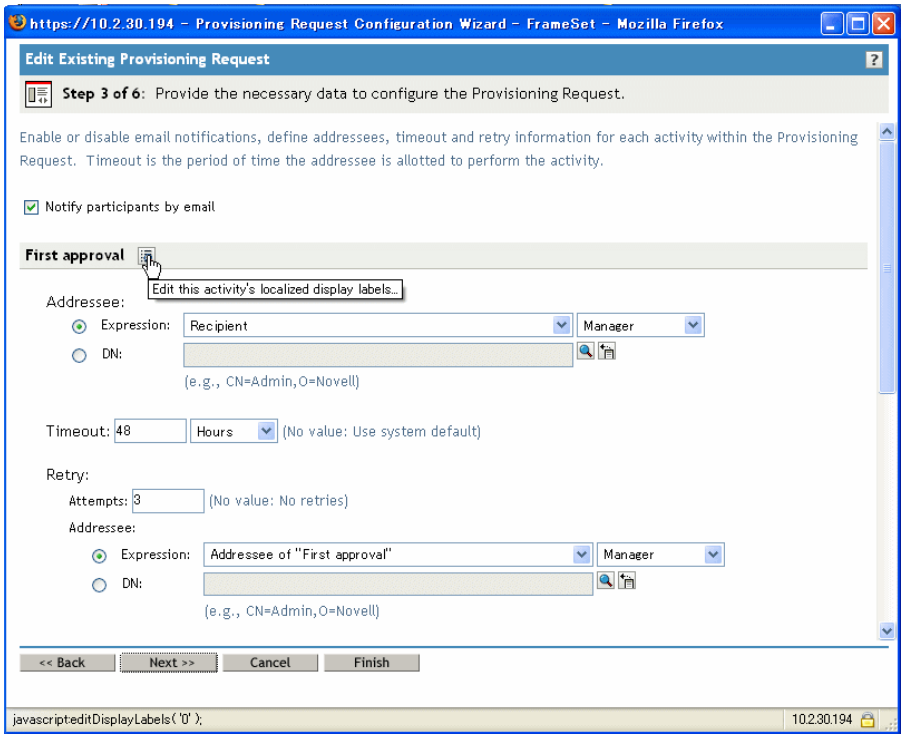
1 Especifique si desea que el receptor de cada actividad reciba una notificación por correo electrónico, seleccionando o deseleccionando la casilla de verificación *Notificar a los participantes a través del correo electrónico*.



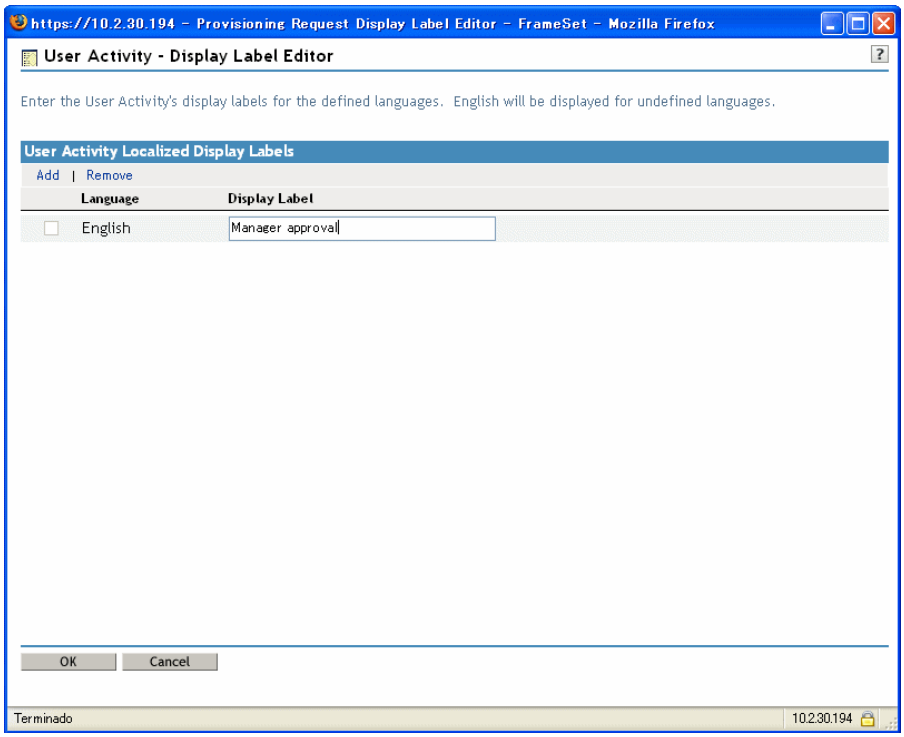
Nota: Si selecciona la casilla de verificación *Notificar a los participantes mediante correo electrónico* y el receptor tiene un apoderado (proxy) designado, también se enviará una notificación por correo electrónico al apoderado (proxy). Los delegados no se incluyen en las notificaciones por correo electrónico.

---

2 En cada actividad del flujo de trabajo, tiene la oportunidad de cambiar la etiqueta de visualización haciendo clic en el icono situado al lado del nombre de la actividad (en este caso, First Approval (Primera aprobación)).



Escriba la etiqueta de visualización en el campo *Etiqueta de visualización* y haga clic en *Aceptar*.



Nota: Las etiquetas de visualización por defecto (First approval (Primera aprobación), Second approval (Segunda aprobación), etc.) denotan que las aprobaciones se procesan de forma secuencial. En el caso de los flujos paralelos, puede especificar etiquetas que no impliquen un proceso secuencial. Por ejemplo, puede asignar etiquetas como One of Three Parallel Approvals (Una de tres aprobaciones paralelas), Two of Three Parallel Approvals (Dos de tres aprobaciones paralelas), etc.

3 Por cada actividad del flujo de trabajo, proporcione también la información siguiente:

Campo	Descripción
Expresión del receptor	Permite especificar una expresión dinámica que identifica el receptor de la actividad. El receptor se determina en el tiempo de ejecución, basándose en cómo se evalúa la expresión. El **primer término** de la expresión de un receptor puede ser cualquiera de los valores siguientes: ◆ `Iniciador` ◆ `Destinatario` ◆ `Addressee of` *activity_name* (Receptor de nombre_de_la_actividad) Por cada actividad del flujo de trabajo (salvo en el caso de la actividad que está configurando actualmente) se lista un `Addressee of` *activity_name* (Receptor de nombre_de_la_actividad) diferente en la lista desplegable Expresión. El *activity_name* (nombre_de_la_actividad) es la etiqueta de visualización especificada para la actividad o el nombre por defecto, si no ha especificado ninguna etiqueta de visualización. El **segundo término** de la expresión de un receptor puede ser alguno de los valores siguientes: ◆ `Supervisor` ◆ `<Sin atributos>` **Nota:** El atributo `Supervisor` está disponible automáticamente, ya que se ha definido anteriormente en la entidad Usuario del nivel de abstracción. Puede haber otros atributos (además de Supervisor) que se pueden seleccionar, si cumplen los requisitos siguientes: ◆ Deben estar definidos en la entidad Usuario del nivel de abstracción ◆ Deben tener un único valor ◆ Deben tener un tipo de datos DN
DN del receptor	Permite especificar el nombre completo de un usuario, un grupo o un grupo de tareas. **Nota:** Si desea que los supervisores de grupos de tareas puedan buscar tareas por grupo de tareas (en la acción My Team Tasks (Las tareas de mi equipo) en la aplicación de usuario), deberá especificar que el grupo de tareas es el receptor.

Campo	Descripción
Tiempo límite	Permite especificar el período de tiempo que se asigna al receptor para que complete la tarea. El intervalo de tiempo límite se aplica cada vez que el receptor ejecuta la actividad. Especifique un valor en segundos, minutos, horas o días.
Intentos	Permite especificar cuántas veces se reintentará la actividad si se alcanza el tiempo límite. Cuando una actividad alcanza su tiempo límite, el proceso del flujo de trabajo puede intentar volver a completar la actividad, en función de los reintentos especificados para la actividad. En cada reintento, el proceso de flujo de trabajo puede pasar la actividad a otro usuario. En dicho caso, la actividad se vuelve a asignar a otro receptor (por ejemplo, el supervisor del usuario) para dar al usuario la oportunidad de finalizar el trabajo de la actividad. En caso de que el último reintento alcance su tiempo límite, la actividad se puede marcar como aprobada o denegada, en función de cómo se haya configurado el flujo de trabajo.
Expresión del receptor de reintento	Permite especificar una expresión dinámica que identifique el usuario que recibirá la tarea en caso de que se alcance el tiempo límite. El receptor se determina en el tiempo de ejecución, basándose en cómo se evalúa la expresión. El **primer término** de la expresión de un receptor puede ser cualquiera de los valores siguientes: ◆ `approval.getAddressee()` ◆ `Iniciador` ◆ `Destinatario` ◆ `Receptor de` *nombre_de_la_actividad* La opción `approval.getAddressee()` obtiene el receptor actual. Por cada actividad del flujo de trabajo (incluida la actividad que está configurando actualmente) se lista un `Receptor de` *nombre_de_la_actividad* diferente en la lista desplegable Expresión. El *nombre_de_la_actividad* es la etiqueta de visualización especificada para la actividad o el nombre por defecto, si no ha especificado ninguna etiqueta de visualización. El **segundo término** de la expresión de un receptor puede ser alguno de los valores siguientes: ◆ `Supervisor` ◆ `<Sin atributos>` Si selecciona la opción `approval.getAddressee()` y, a continuación, selecciona `Supervisor`, cada reintento se escalará a otro supervisor en un nivel superior en la organización. Por consiguiente, asegúrese de que el número de reintentos esté definido en una cantidad adecuada para la organización. En cualquier caso, los reintentos no deben superar el número de niveles de supervisión que están por encima del receptor actual.

Campo	Descripción
DN del receptor del reintento	Permite especificar el nombre completo de un usuario o grupo que deba obtener esta tarea en caso de que se haya alcanzado el límite de reintentos.

4 Cuando acabe de configurar una actividad, probablemente deba desplazarse para ver otras actividades para el flujo.

5 Haga clic en *Siguiente*.

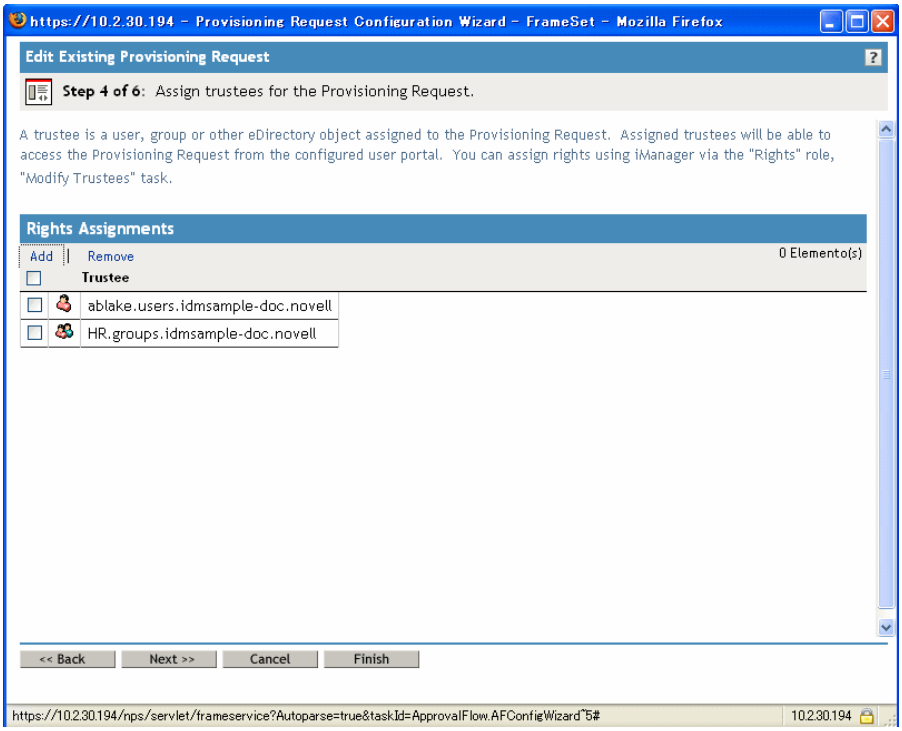
Nota: El número de actividades que puede configurar varía en función de la plantilla de flujo de trabajo asignada a la definición de petición. El número y el tipo de parámetros de derechos varían en función del recurso aprovisionado asociado a la petición.

Especificación de los derechos de acceso de la petición de provisión

Para especificar los derechos de acceso de una petición de provisión:

1 Para añadir un usuario, grupo u otro objeto de eDirectory a la lista de Trustees de esta definición de petición, haga clic en *Añadir* y seleccione el objeto.

Cuando haya añadido el objeto, éste se incluirá en la lista de Trustees.



2 Para eliminar un usuario, grupo u otro objeto, seleccione el elemento en la lista *Trustee* y haga clic en *Eliminar*.

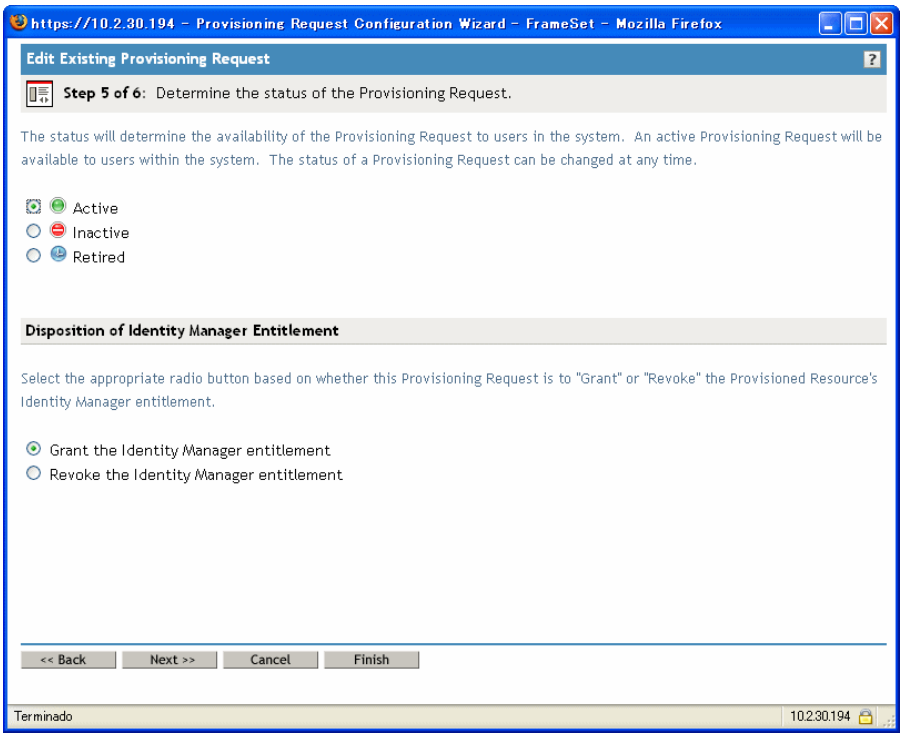
3 Haga clic en *Siguiente*.

Especificación del estado inicial de la petición de provisión

Para definir el estado inicial de la petición de provisión:

1 Haga clic en el botón circular correspondiente al estado deseado:

Estado	Descripción
Activo	Disponible para utilizarlo.
Inactivo	No se puede utilizar temporalmente. Éste es el valor por defecto.
Retirado	Inhabilitado temporalmente.



2 Haga clic en el botón circular correspondiente a la acción correcta (Otorgar o Revocar).

3 Haga clic en *Siguiente*.

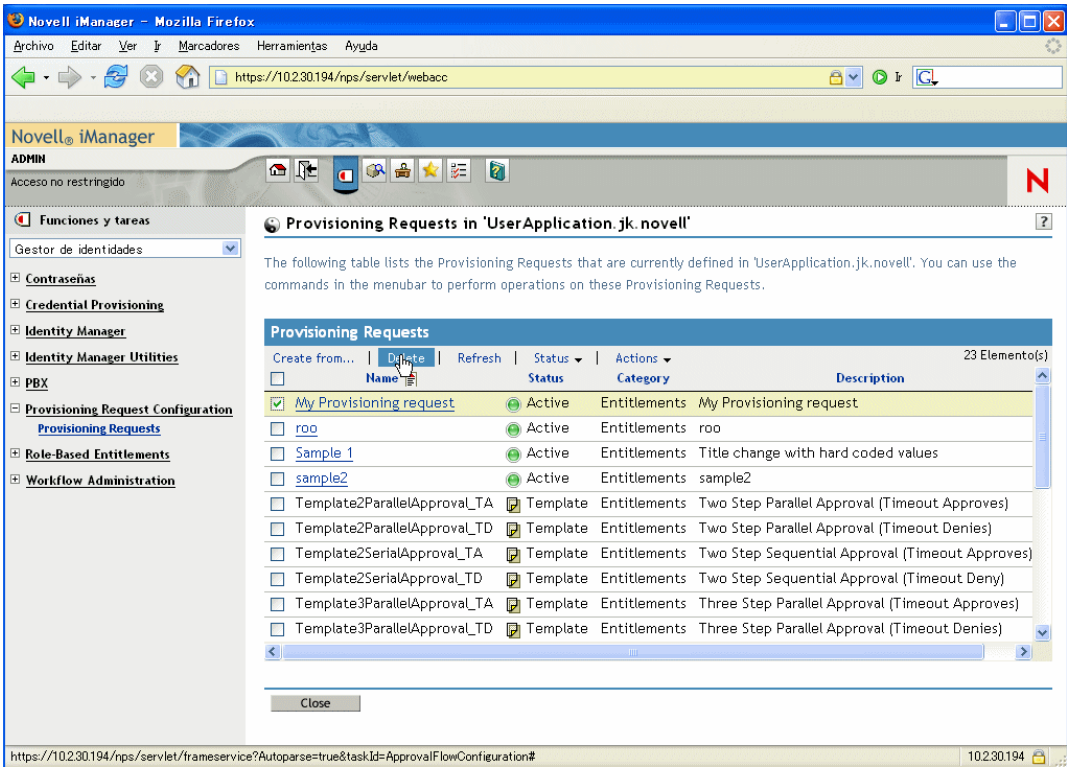
22.3.3 Supresión de una petición de provisión

Para suprimir una petición de provisión:

1 Seleccione la petición de provisión que desea suprimir haciendo clic en la casilla de verificación situada al lado del nombre.

Las peticiones de provisión que sean plantillas no se pueden suprimir.

2 Haga clic en el comando *Suprimir* del panel Configuración de la petición de provisión.

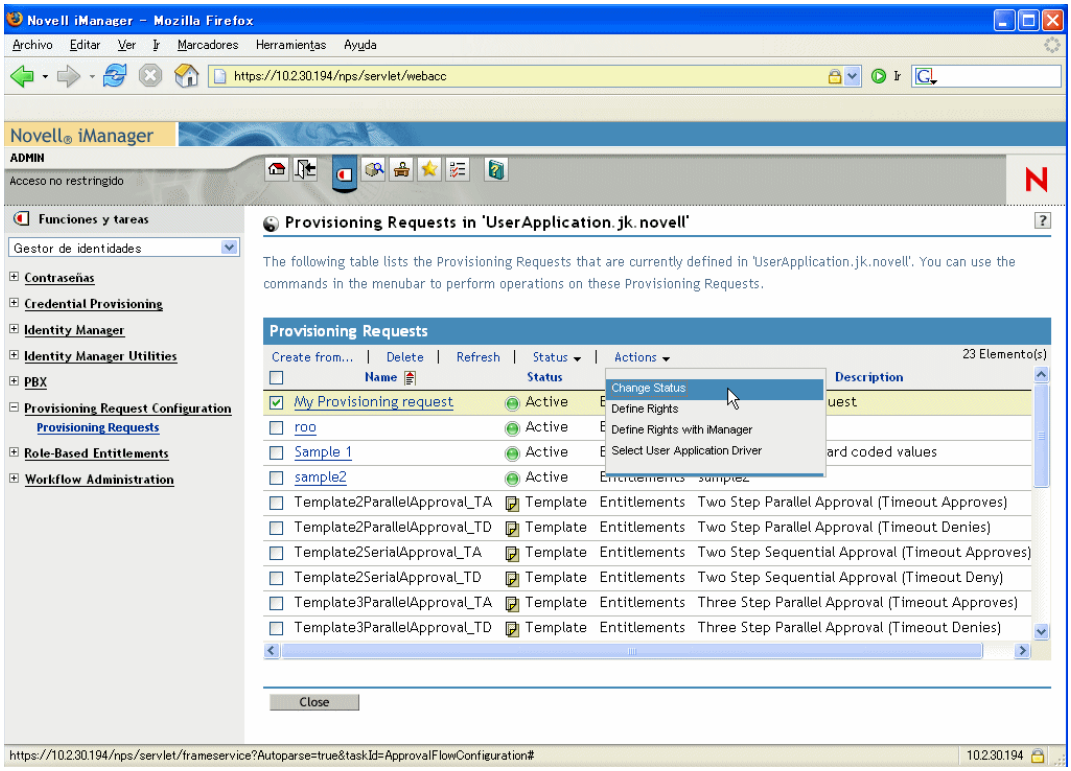


22.3.4 Cambio del estado de una petición de provisión existente

Para cambiar el estado de una petición de provisión existente:

1 Seleccione la petición de provisión cuyo estado desea cambiar, haciendo clic en la casilla de verificación situada al lado del nombre.

2 Haga clic en el comando *Cambiar estado* del panel Configuración de la petición de provisión.



3 Haga clic en el estado, en el menú Estado:

Estado	Descripción
Activo	Disponible para utilizarlo.
Inactivo	No se puede utilizar temporalmente.
Retirado	Inhabilitado temporalmente.

4 Haga clic en el botón circular correspondiente a la acción correcta (Otorgar o Revocar).

5 Haga clic en *Finalizar*.

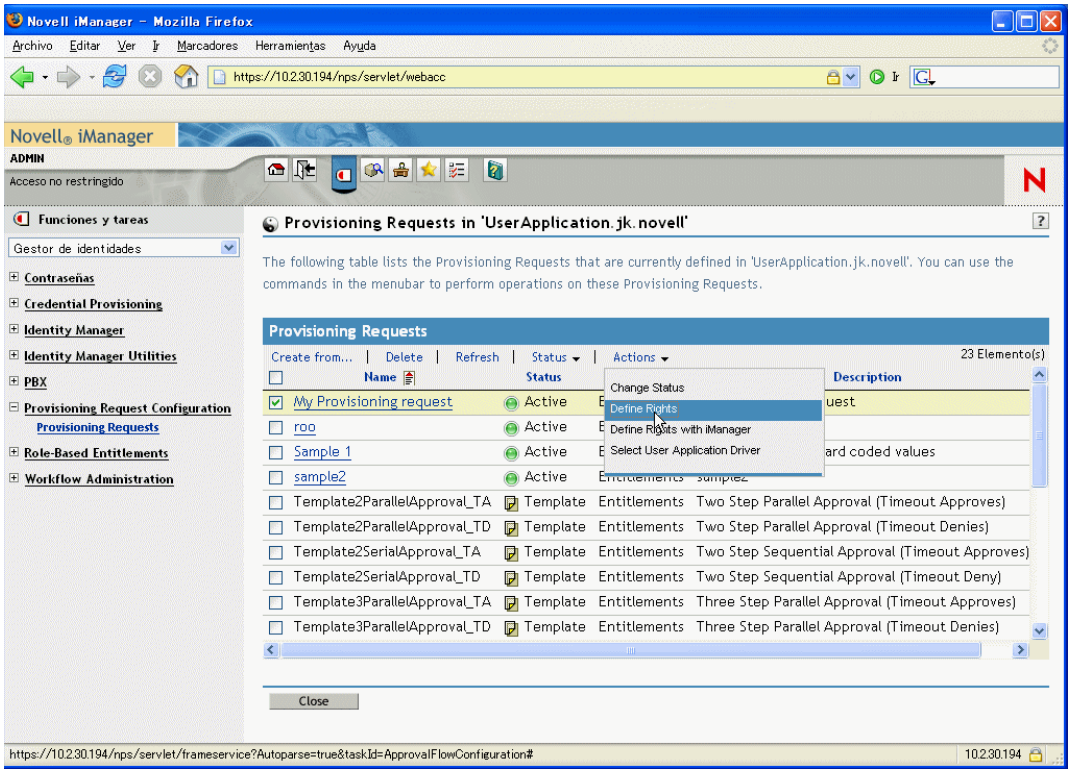
22.3.5 Definición de derechos en una petición de provisión existente

Para definir derechos en una petición de provisión existente:

1 Seleccione la petición de provisión cuyos derechos desea definir, haciendo clic en la casilla de verificación situada al lado del nombre.

2 Haga clic en el comando *Acciones* del panel Configuración de la petición de provisión.

3 Haga clic en el comando *Definir derechos* del menú Acciones.



4 Siga los pasos que se presentan en "Especificación de los derechos de acceso de la petición de provisión" en la página 342.

Para definir derechos en una petición de provisión con iManager:

1 Seleccione la petición de provisión cuyos derechos desea definir, haciendo clic en la casilla de verificación situada al lado del nombre.

2 Haga clic en el comando *Acciones* del panel Configuración de la petición de provisión.

3 Haga clic en el comando *Definir derechos con iManager* del menú Acciones.

Gestión de los flujos de trabajo de provisión

23

En este capítulo se ofrecen instrucciones para gestionar los flujos de trabajo de provisión en el tiempo de ejecución. También se proporcionan instrucciones para configurar la notificación por correo electrónico de los flujos de trabajo de provisión.

Los temas son:

23.1 Acerca del módulo auxiliar de administración del flujo de trabajo

El módulo auxiliar de administración de flujos de trabajo en iManager proporciona una interfaz basada en explorador que permite ver el estado de los procesos de flujo de trabajo, reasignar actividades dentro de un flujo de trabajo o terminar un flujo de trabajo en caso de que éste se bloquee.

Puede encontrar el módulo auxiliar de administración del flujo de trabajo en la categoría *Gestor de identidades* de iManager. El módulo auxiliar incluye la *tarea Flujos de trabajo* de la *Función Administración de flujo de trabajo*.

La función Administración de flujo de trabajo también incluye las tareas de las *Plantillas de correo electrónico* y de las *opciones de Servidor de correo electrónico*. Estas tareas son accesos directos a otras tareas listadas en la función *Contraseñas*.

Acerca de la tarea Flujos de trabajo La tarea Flujos de trabajo está formada por los paneles siguientes:

Panel	Descripción
Flujos de trabajo	Proporciona la interfaz de usuario principal para administrar los flujos de trabajo de provisión. La interfaz muestra una lista de los flujos de trabajo que se están procesando en esos momentos y permite ejecutar diversas acciones en dichos flujos de trabajo. Cuando inicie por primera vez la tarea Flujos de trabajo, el panel Flujos de trabajo necesitará que seleccione un controlador de la aplicación de usuario del Gestor de identidades. El controlador apunta a un servidor de flujo de trabajo. Antes de entrar en el servidor y empezar a administrar el flujo de trabajo, deberá seleccionar un controlador. Cuando haya seleccionado un controlador, podrá especificar los criterios de búsqueda para seleccionar los flujos de trabajo que va a gestionar.
Información del flujo de trabajo	Proporciona una interfaz de usuario de sólo lectura par ver información acerca de un flujo de trabajo específico.

23.2 Gestión de los flujos de trabajo

En esta sección se incluyen procedimientos para gestionar flujos de trabajo de provisión mediante el módulo auxiliar de administración de flujos de trabajo.

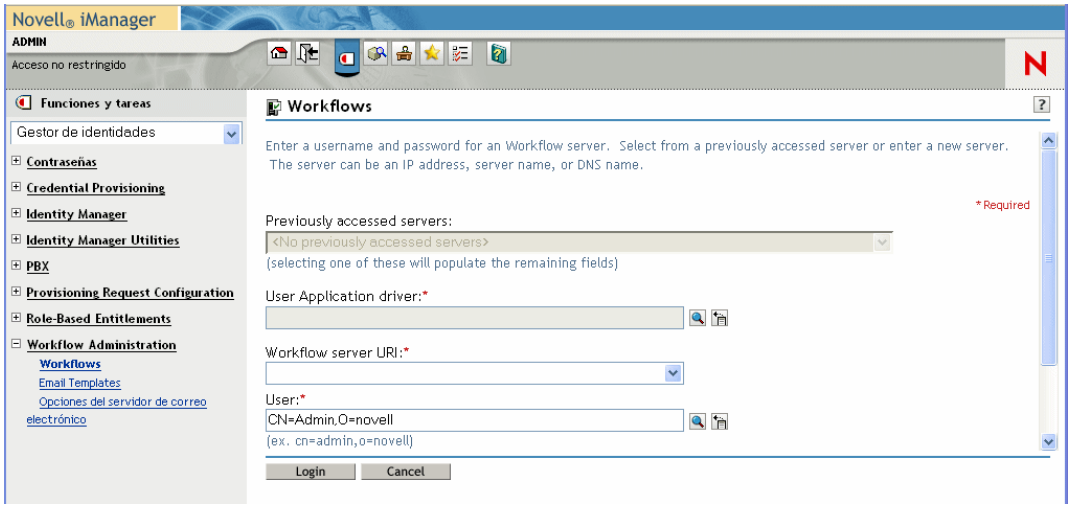
23.2.1 Conexión a un servidor de flujo de trabajo

Para poder empezar a gestionar flujos de trabajo, es preciso conectarse a un servidor de flujo de trabajo. Si el controlador de la aplicación de usuario está asignado a un único servidor de flujo de trabajo, puede simplemente especificar el nombre del controlador que va a utilizar. Si el controlador está asociado a varios servidores de flujo de trabajo, deberá seleccionar el servidor de flujo de trabajo de destino.

Para conectarse a un servidor de flujo de trabajo:

1. Seleccione la categoría Gestor de identidades en iManager.
2. Abra la función *Administración de flujo de trabajo*.
3. Haga clic en la tarea *Flujos de trabajo*.

iManager muestra la pantalla Flujos de trabajo.

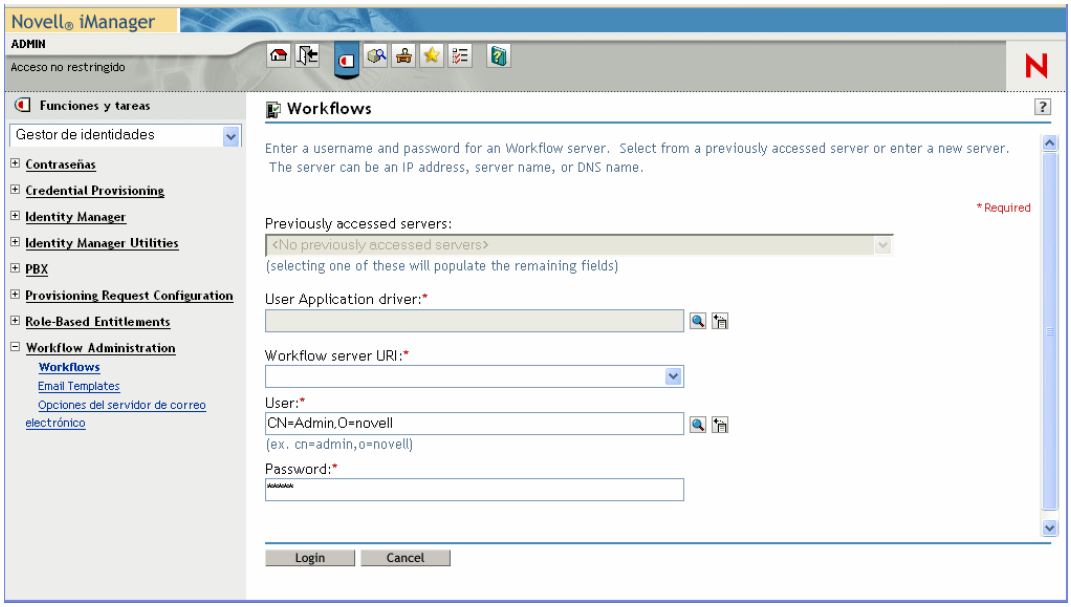


4 Si ha accedido anteriormente al servidor de flujo de trabajo de destino, puede seleccionar dicho servidor en la lista desplegable *Servidores a los que se ha accedido previamente*.

iManager se encargará de rellenar los campos restantes de la pantalla.

5 Si todavía no ha accedido a un servidor de flujo de trabajo, especifique el nombre del controlador en el campo *Controlador de la aplicación de usuario* y haga clic en *Aceptar*.

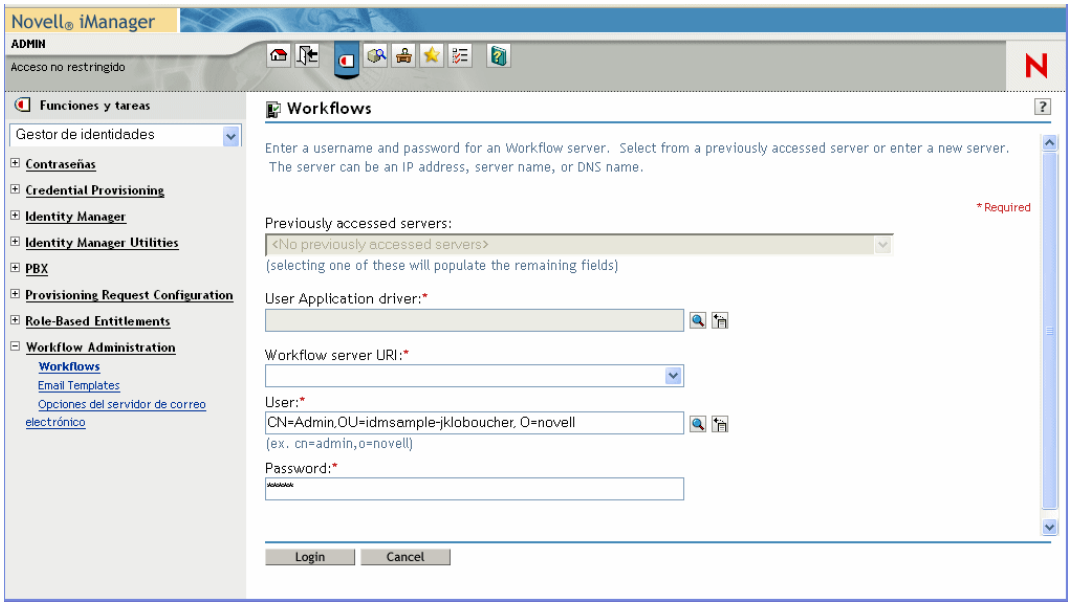
iManager se encargará de rellenar los campos restantes de la pantalla.



6 Si el controlador está asociado a varios servidores de flujo de trabajo, seleccione el servidor de destino en el campo *URI de servidor de flujo de trabajo*.

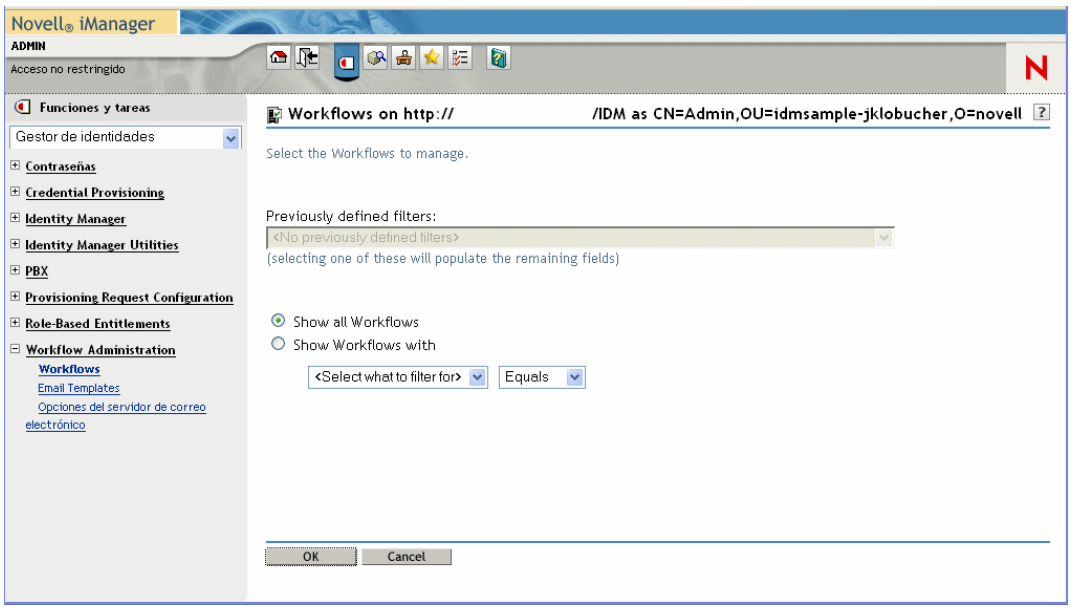
7 Puede también cambiar el nombre de usuario del campo *Usuario* y la contraseña del campo *Contraseña*.

El usuario tiene que ser el administrador de la aplicación de usuario. Por defecto, el nombre de usuario está definido en el usuario que está conectado actualmente en iManager. Si dicho usuario no es el administrador, deberá cambiar el nombre de usuario. Por ejemplo, puede que quiera modificar el usuario para que apunte al administrador de la aplicación de usuario del idmsample test OU, tal como se muestra a continuación:



8 Haga clic en *Entrar*.

El módulo auxiliar de administración del flujo de trabajo mostrará una página que permite especificar un filtro para encontrar flujos de trabajo:

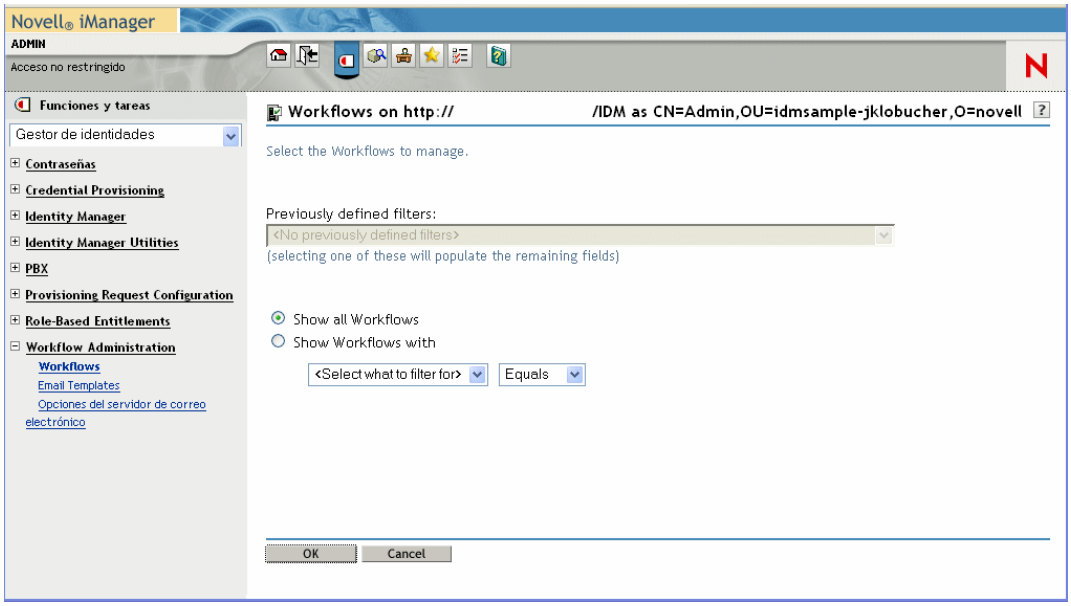


23.2.2 Detección de flujos de trabajo que cumplan los criterios de búsqueda

Si el servidor de flujo de trabajo de destino tiene un gran número de procesos de flujo de trabajo, probablemente desee filtrar la lista de flujos de trabajo que ve en iManager. Para ello, puede especificar criterios de búsqueda.

Para especificar criterios de búsqueda para filtrar la lista de flujos de trabajo:

1 Seleccione el botón circular *Mostrar flujos de trabajo con*.



Nota: Por defecto, está seleccionado el botón circular *Mostrar todos los flujos de trabajo*. No cambie el valor por defecto si desea ver la lista completa de flujos de trabajo del servidor.

2 Seleccione el atributo para el que desee especificar criterios.

Atributo	Descripción
Hora de creación	Hora de inicio del flujo de trabajo.
Iniciador	Nombre de usuario del peticionario.
Destinatario	Nombre de usuario del destinatario.
Estado de proceso	Estado del proceso de flujo de trabajo en general (Completado, En ejecución o Terminado).
Estado de aprobación	Estado del proceso de aprobación (Aprobado, Denegado o Retraído).
Estado del derecho	Estado del derecho iniciado por la petición de provisión (Error, Grave, Correcto, Desconocido o Advertencia).

3 Seleccione un operador:

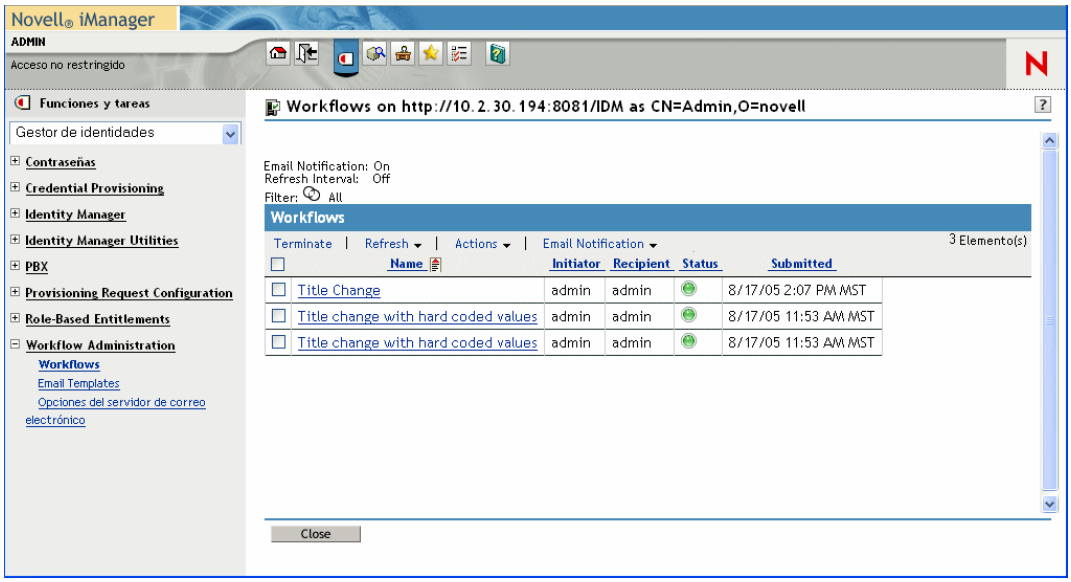
Operador	Comentario
Igual a	Todos los atributos lo admiten.
Antes	Sólo lo admite el atributo Hora de creación.
Después	Sólo lo admite el atributo Hora de creación.
Entre	Sólo lo admite el atributo Hora de creación.

4 Especifique un valor en el campo situado bajo el atributo y el operador.

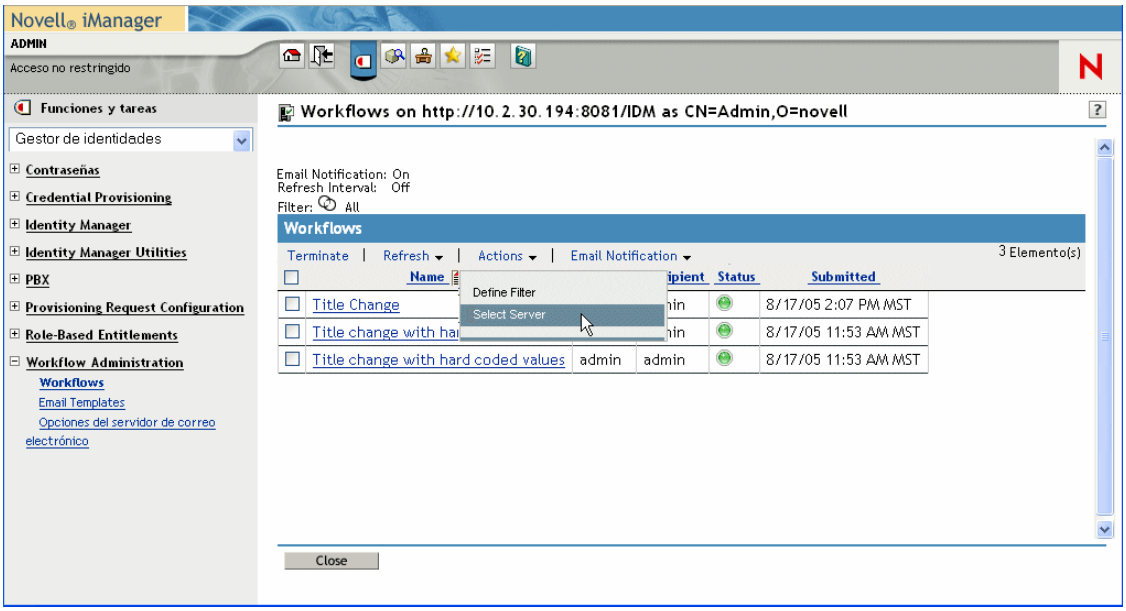
Para Hora de creación, puede utilizar el control de fecha y hora para seleccionar el valor. Para Iniciador y Destinatario, puede utilizar el Historial de objeto o el Selector de objetos para especificar un valor. Para el resto de atributos, seleccione un valor en la lista desplegable.

5 Haga clic en *Aceptar*.

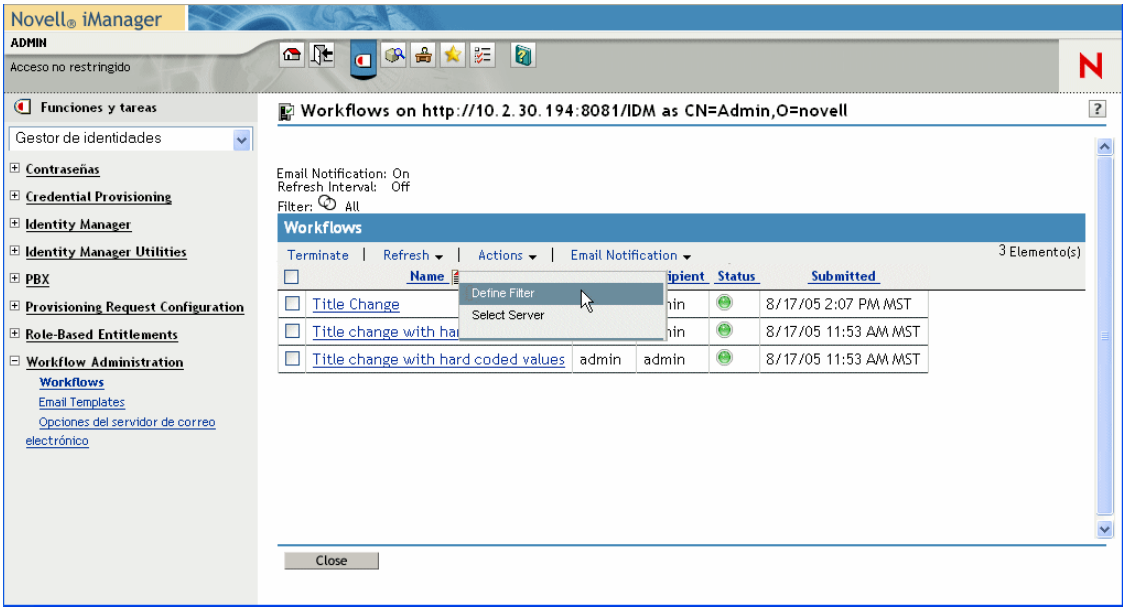
iManager mostrará los flujos de trabajo que ha seleccionado en el panel Flujos de trabajo.



Cambio del servidor de destino y del filtro Cuando haya seleccionado un servidor de flujo de trabajo, la selección permanecerá en vigor mientras dure la sesión de iManager, a menos que seleccione otro servidor. Para seleccionar otro servidor, haga clic en el comando *Acciones* y seleccione *Seleccionar servidor* en el menú *Acciones*.



Para especificar otros criterios de búsqueda, seleccione *Definir filtro* en el menú *Acciones*.



23.2.3 Control de la visualización de los flujos de trabajo activos

El panel Flujos de trabajo lista los flujos de trabajo que cumplen los criterios de búsqueda especificados. Además de filtrar la lista, puede controlar la visualización. Por ejemplo, puede especificar la frecuencia de actualización de la lista y ordenar la lista por una columna en concreto.

Actualización de la lista de flujos de trabajo

Cuando el servidor de flujo de trabajo está muy ocupado, la lista de flujos de trabajo activos puede cambiar con frecuencia. En dicho caso, puede que desee actualizar la lista de flujos de trabajo activos que se ejecutan en el servidor.

Para actualizar la lista de flujos de trabajo:

1. Haga clic en el comando *Actualizar* del panel Flujos de trabajo.
2. Especifique el intervalo de actualización que desea utilizar seleccionando una de las opciones siguientes en el menú Actualizar:
   - **2a** Actualizar desactivado
   - **2b** Actualizar ahora
   - **2c** 10 segundos
   - **2d** 30 segundos
   - **2e** 60 segundos
   - **2f** 5 minutos

Clasificación de la lista de flujos de trabajo

Si el volumen de definiciones de petición es elevado, puede ordenar la lista por una columna en concreto, como el nombre o la descripción.

Para clasificar la lista de flujos de trabajo:

1. Haga clic en el título de la columna de clasificación.

23.2.4 Terminación de una instancia de flujo de trabajo

En caso de que no desee que una instancia de flujo de trabajo siga procesando, puede terminar el flujo de trabajo.

Para terminar una instancia de proceso de flujo de trabajo:

1. Seleccione el flujo de trabajo en el panel Flujos de trabajo haciendo clic en la casilla de verificación situada al lado del nombre del flujo de trabajo.
2. Haga clic en el comando *Terminar* del panel Flujos de trabajo.

23.2.5 Visualización de información de una instancia de flujo de trabajo

Cuando haya visualizado un conjunto de flujos de trabajo que están ejecutándose en un servidor determinado, puede seleccionar una instancia de flujo de trabajo para ver más información acerca de un proceso en ejecución.

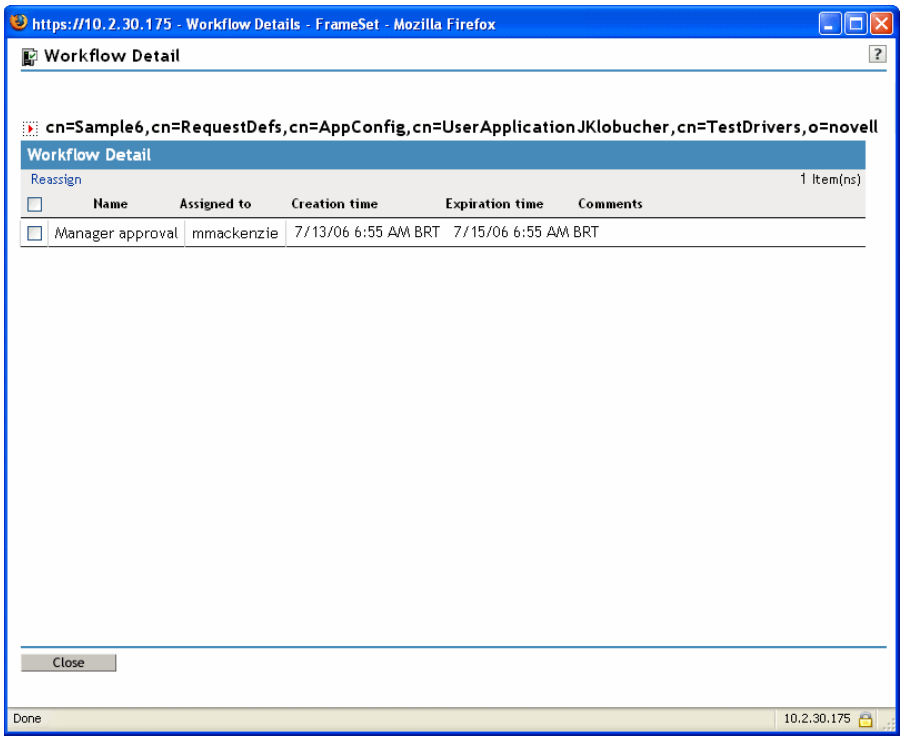
Nota: Si una instancia de flujo de trabajo utiliza un patrón de diseño de proceso en serie, la visualización mostrará una única actividad como actual, ya que sólo un usuario puede actuar en el

elemento de trabajo en cualquier momento. No obstante, si el flujo de trabajo gestiona proceso en paralelo y ramificación, es posible que haya varias actividades para una instancia de flujo de trabajo.

Para ver la información de una instancia de flujo de trabajo concreta:

1 Haga clic en el nombre de la instancia de flujo de trabajo en el panel Flujos de trabajo.

iManager muestra la pantalla Información del flujo de trabajo.



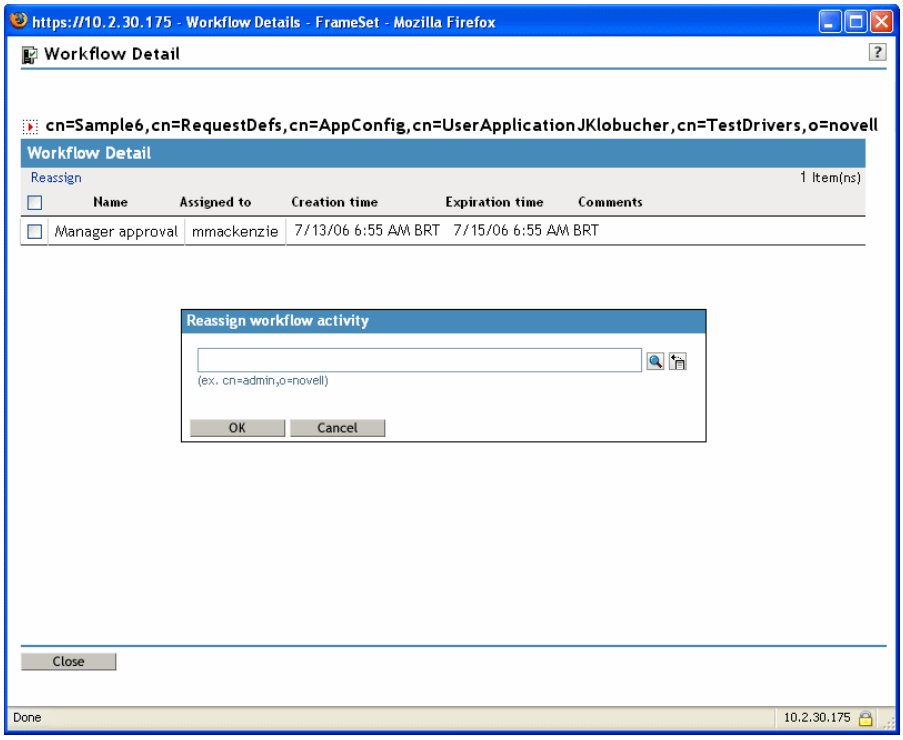
23.2.6 Reasignación de una instancia de flujo de trabajo

En caso de que una instancia de flujo de trabajo quede bloqueada, puede reasignar el elemento de trabajo a otro usuario o grupo.

Para reasignar una instancia de flujo de trabajo:

1 Seleccione la actividad actual asociada al flujo de trabajo haciendo clic en la casilla de verificación situada al lado del nombre en el panel Información del flujo de trabajo.

2 Haga clic en el comando *Reasignar* del panel Información del flujo de trabajo.



3 Seleccione el usuario o el grupo al que desee reasignar el elemento de trabajo.

23.3 Configuración del servidor de correo electrónico

A menudo, un proceso de flujo de trabajo envía notificaciones por correo electrónico en diversos puntos en el transcurso de su ejecución. Por ejemplo, se puede enviar un mensaje de correo electrónico cuando un usuario asigna una actividad de flujo de trabajo a un receptor nuevo.

Antes de poder aprovechar todas las ventajas que aportan las capacidades de notificación por correo electrónico del Gestor de identidades, debe configurar el servidor de correo electrónico SMTP. Para ello, deberá utilizar la tarea de las *opciones de Servidor de correo electrónico* de la función *Administración de flujo de trabajo* en iManager.

Nota: Esta tarea es un acceso directo a la tarea de las *opciones del servidor de correo electrónico* que se encuentra en la función *Contraseñas*.

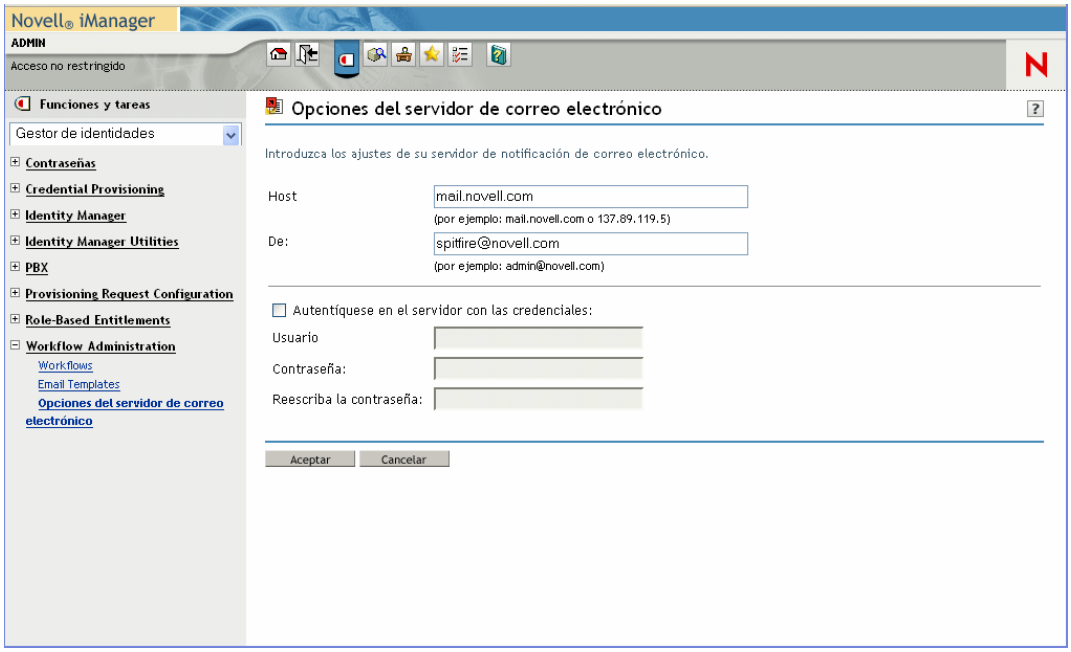
Para configurar el servidor de correo electrónico:

1 Seleccione la categoría Gestor de identidades en iManager.

2 Abra la función *Administración de flujo de trabajo*.

3 Haga clic en la tarea de las *opciones del servidor de correo electrónico*.

iManager muestra la pantalla de opciones del servidor de correo electrónico.



4 Escriba el nombre (o dirección IP) del servidor host en el campo *Nombre del host*.

5 Escriba la dirección de correo electrónico del remitente en el campo *De*.

Cuando el destinatario abra el correo electrónico, este texto se mostrará en el campo De del encabezado del correo electrónico. Dependiendo de la configuración del servidor de correo, es posible que el texto de este campo tenga que coincidir con un remitente válido del sistema para que el servidor de correo pueda realizar búsquedas inversas o autenticación. Un ejemplo sería helpdesk@company.com en vez de un texto descriptivo del tipo "Administrador de la contraseña".

6 Si su servidor requiere autenticación antes de enviar correo electrónico, seleccione la casilla de verificación *Autenticación en el servidor mediante credenciales* y especifique el nombre de usuario y la contraseña.

7 Cuando haya acabado, haga clic en *Aceptar*.

23.4 Funcionamiento con las plantillas de correo electrónico instaladas

El Gestor de identidades se entrega con una plantilla de correo electrónico diseñada específicamente para provisiones basadas en flujos de trabajo. Dicha plantilla se denomina *Nueva petición de provisión* y todas las plantillas de petición de provisión que se entregan con el producto están asociadas a ella. Por consiguiente, todas las definiciones de petición nuevas que cree utilizarán esta plantilla de correo electrónico.

Puede editar la plantilla Nueva petición de provisión para cambiar el contenido y formato de los mensajes de correo electrónico, pero no puede crear plantillas de correo electrónico nuevas.

Para editar la plantilla Nueva petición de provisión, deberá utilizar la tarea *Plantillas de correo electrónico* que se encuentra en la función *Administración de flujo de trabajo* en iManager.

Nota: Esta tarea es un acceso directo a la tarea *Editar plantillas de correo electrónico* que se encuentra en la función *Contraseñas*.

23.4.1 Formato y contenido por defecto

A continuación, mostramos cómo queda la plantilla Nueva petición de provisión después de instalar el producto:

```
Estimado $userFirstName$, se ha enviado una petición de provisión
nueva que necesita su aprobación. Nombre de la petición:
$requestTitle$ Enviada por: $initiatorFullName$ Destinatario:
$recipientFullName$ Revise los detalles de esta petición en
$PROTOCOL$://$HOST$:$PORT$/$TASK_DETAILS$ para llevar a cabo la acción
adecuada. Puede revisar una lista de todas las peticiones pendientes de
su aprobación en $PROTOCOL$://$HOST$:$PORT$/$TASKLIST_CONTEXT$.
```

La plantilla identifica la definición de petición de provisión que ha activado el mensaje de correo electrónico. Además, incluye una URL que redirige el receptor a la tarea que necesita la aprobación, así como otra URL que visualiza la lista completa de tareas que el usuario tiene pendientes.

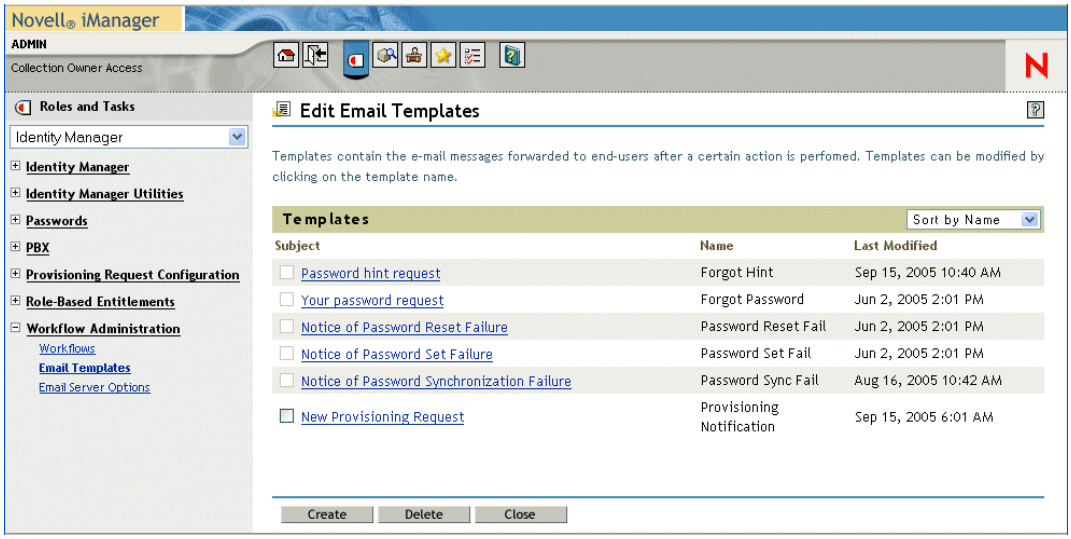
23.4.2 Edición de la plantilla

Puede cambiar el contenido o formato de la plantilla Nueva petición de provisión. No obstante, tenga en cuenta que la plantilla se aplica a todas las peticiones de provisión de la aplicación de usuario del Gestor de identidades, por lo que deberá estar seguro de que las ediciones son adecuadas para todos los usuarios y tareas del flujo de trabajo.

Para editar la plantilla:

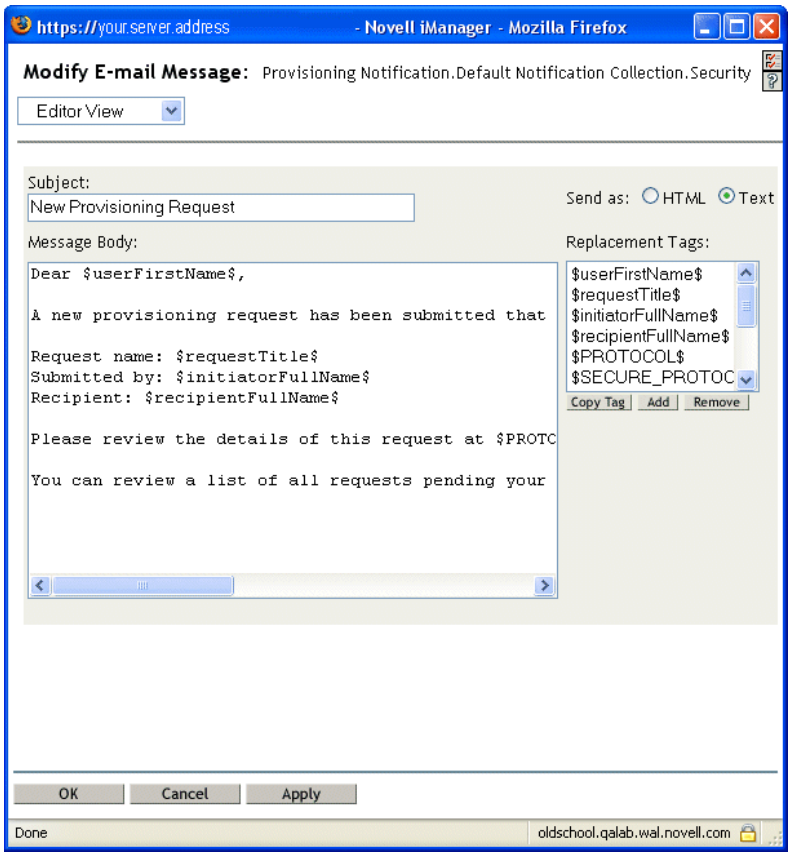
1. Seleccione la categoría Gestor de identidades en iManager.
2. Abra la función *Administración de flujo de trabajo*.
3. Haga clic en la tarea *Plantillas de correo electrónico*.

iManager mostrará la pantalla Editar plantillas de correo electrónico.



4 Haga clic en *Nueva petición de provisión* en la lista de plantillas.

iManager mostrará la pantalla Modificar mensaje de correo electrónico.



5 Introduzca los cambios en el recuadro del *cuerpo del mensaje*.

6 Si es preciso, copie una o varias de las etiquetas suministradas en el cuadro de lista Etiquetas de sustitución para incluir texto dinámico en el cuerpo del mensaje.

A continuación, describimos brevemente las etiquetas de sustitución:

Etiqueta	Descripción
$userFirstName$	El nombre del receptor.
$requestTitle$	Nombre de visualización de la definición de la petición de provisión.
$initiatorFullName$	Nombre completo del iniciador.
$recipientFullName$	Nombre completo del destinatario.
$PROTOCOL$	Protocolo de las URL incluidas en el mensaje de correo electrónico.
$SECURE_PROTOCOL$	Protocolo seguro de las URL incluidas en el mensaje de correo electrónico.
$HOST$	El host del servidor de aplicación JBoss que ejecuta la aplicación de usuario del Gestor de identidades.
$PORT$	Puerto de la aplicación de usuario del Gestor de identidades.
$SECURE_PORT$	Puerto seguro de la aplicación de usuario del Gestor de identidades.
$TASKLIST_CONTEXT$	Página que muestra la lista de todas las peticiones que el receptor tiene pendientes.
$TASK_DETAILS$	Página que muestra información de la petición para la que se ha generado el mensaje de correo electrónico.

7 Cuando haya acabado, haga clic en *Aceptar*.

23.4.3 Modificación de los valores por defecto de la plantilla

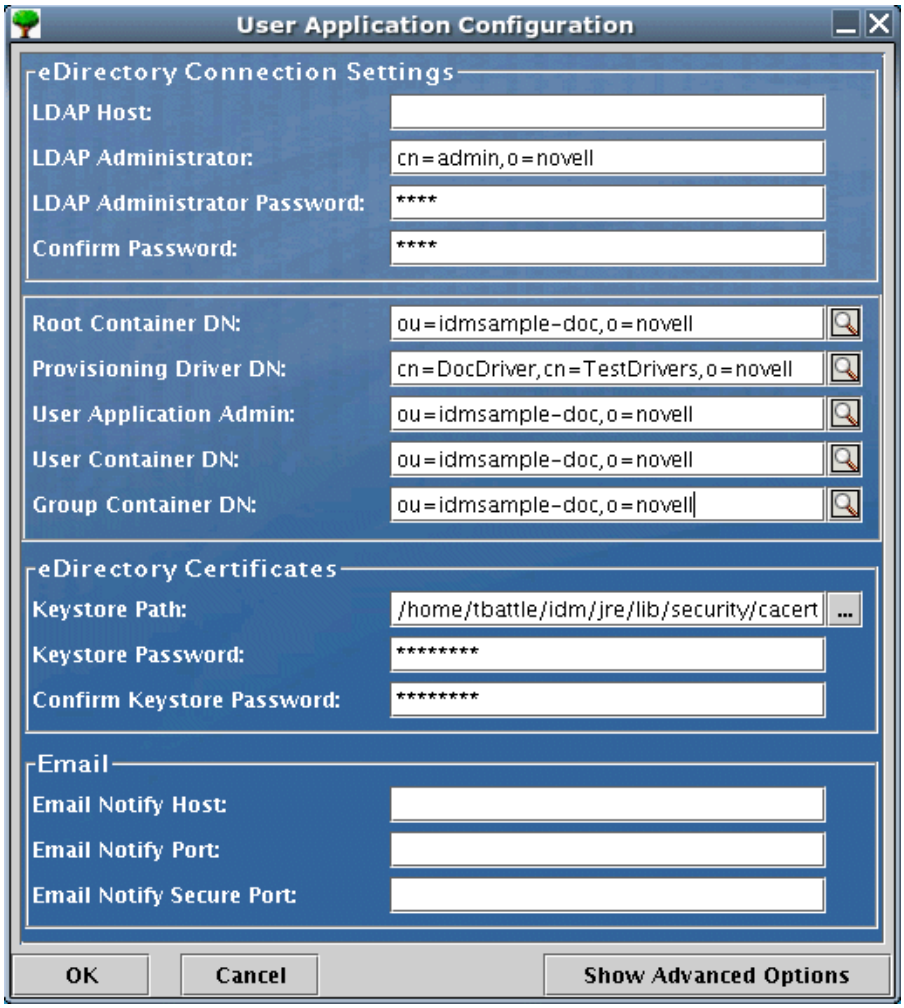
En el momento de realizar la instalación, puede definir los valores por defecto de varias etiquetas de sustitución utilizadas en las plantillas de correo electrónico. Cuando haya acabado la instalación, también podrá modificar dichos valores utilizando la herramienta de configuración de la aplicación de usuario.

Para modificar los valores de instalación:

1 Ejecute el guión ldapconfig.sh en la carpeta idm.

```
./configupdate.sh
```

Nota: En Windows, el archivo que debe ejecutarse es `configupdate.bat`.



2 Introduzca los cambios necesarios en cualquiera de los campos siguientes:

Campo	Descripción
Host de notificación por correo electrónico	Este campo se utiliza para sustituir el testigo $HOST$ en las plantillas de correo electrónico utilizadas en los flujos de aprobación. Si se deja en blanco, el servidor lo calculará. (Es el host de JBoss).
Puerto de notificación por correo electrónico	Este campo se utiliza para sustituir el testigo $PORT$ en las plantillas de correo electrónico utilizadas en los flujos de aprobación.
Puerto seguro de notificación por correo electrónico	Este campo se utiliza para sustituir el testigo $SECURE_PORT$ en las plantillas de correo electrónico utilizadas en los flujos de aprobación.

3 Haga clic en *Aceptar* para confirmar los cambios.

Apéndices

VI

En los apéndices siguientes se proporciona información de consulta adicional y temas avanzados de la aplicación de usuario del Gestor de identidades

Extensiones del esquema

A

A.1 Extensiones del esquema de atributo

NOMBRE DEL ATRIBUTO	DESCRIPCIÓN
srvprvAOLIMAddress	**Dirección IM de AOL**
srvprvActiveDelegatees	Delegados activos de un usuario
srvprvActiveDelegators	Delegadores activos de un usuario
srvprvAssetRef	Representación de las propiedades del activo agregado para un activo nombrado asociado a un usuario mediante la clase srvprvAssetRecipientAux
srvprvAssignExpiration	Tiempo en el que caduca una asignación de apoderado (proxy) o delegado.
srvprvAssignFromContainer	Contenedores sujetos de una asignación de apoderado (proxy) o delegado
srvprvAssignFromGroup	Grupos sujetos de una asignación de apoderado (proxy) o delegado
srvprvAssignFromUser	Usuarios sujetos de una asignación de apoderado (proxy) o delegado
srvprvAssignToRelationship	Relación de destino de una asignación de delegado
srvprvAssignToUser	Los usuarios destino de una asignación de apoderado (proxy) o delegado
srvprvCategoryKey	Asocia una definición de petición de provisión determinada a un conjunto de categorías de provisión. Los valores son claves para una instancia srvprvChoice
srvprvDefaultTheme	El tema por defecto
srvprvEntitlementRef	Referencia a un derecho de DirXML (DirXML-Entitlement)
srvprvEntityType	Especifica el tipo de definición de la entidad del nivel de abstracción del directorio
srvprvFlowStrategy	Especifica la estrategia de invocación de flujo que se utilizará para la definición de la petición de provisión
srvprvGrant	Indicador que si está definido en true, especifica que la definición de petición de provisión admite una operación de otorgación
srvprvGroupwiseIMAddress	Dirección IM de Groupwise
srvprvHeaderFillerFile	Nombre del archivo de relleno del encabezado

NOMBRE DEL ATRIBUTO	DESCRIPCIÓN
srvprvAOLIMAddress	**Dirección IM de AOL**
srvprvHeaderFillerImage	Imagen de relleno del encabezado
srvprvHeaderFillerLastMod	Última modificación del relleno del encabezado
srvprvHeaderLogo2File	Nombre del archivo de la imagen secundaria del logotipo del encabezado
srvprvHeaderLogo2Image	Imagen secundaria del logotipo del encabezado
srvprvHeaderLogo2LastMod	Última modificación de la imagen secundaria del logotipo del encabezado
srvprvHeaderLogoFile	Nombre del archivo de la imagen principal del logotipo del encabezado
srvprvHeaderLogoImage	Imagen principal del logotipo del encabezado
srvprvHeaderLogoLastMod	Última modificación de la imagen principal del logotipo del encabezado
srvprvHeaderTextureFile	Nombre del archivo de texturas del encabezado
srvprvHeaderTextureImage	Imagen de la textura del encabezado
srvprvHeaderTextureLastMod	Última modificación de la textura del encabezado
srvprvIsTaskManager	Indica si el usuario es un supervisor de grupos de tareas
srvprvLocalizedDescrs	Proporciona un conjunto de cadenas de descripción localizadas para las aplicaciones Web de provisión, Diseñadores e iManager
srvprvLocalizedNames	Proporciona un conjunto de cadenas de nombres de visualización localizadas para las aplicaciones Web de provisión, Diseñadores e iManager
srvprvLoginFile	Nombre del archivo de entrada
srvprvLoginImage	Imagen de entrada
srvprvLoginLastMod	Última modificación de la entrada
srvprvLoginSmallFile	Nombre de archivo de la imagen pequeña de entrada
srvprvLoginSmallImage	Imagen pequeña de entrada
srvprvLoginSmallLastMod	Última modificación de la imagen pequeña de entrada
srvprvModified	Indicador utilizado para indicar cambios en las definiciones de instancias de objetos en el contenedor de modelos de directorio
srvprvNavBckgrColor	Color de fondo de la navegación
srvprvNavBckgrColorLastMod	Última modificación del color de fondo de la navegación
srvprvNavColor	Color de la navegación
srvprvNavColorLastMod	Última modificación del color de la navegación
srvprvPreferredLocale	Lista de criterios de búsqueda y consulta guardados

NOMBRE DEL ATRIBUTO	DESCRIPCIÓN
srvprvAOLIMAddress	**Dirección IM de AOL**
srvprvProcessXML	Documento XML que representa la definición de un proceso de provisión que incluye una acción de flujo de trabajo y provisión
srvprvRequestDefName	El nombre de definición de petición de provisión asociado a una definición de delegado.
srvprvRequestXML	Documento XML que representa el formulario de petición inicial y sus enlaces de datos
srvprvRevoke	Indicador que si está definido en true, especifica que la definición de petición de provisión admite una operación de revocación
srvprvStatus	Especifica el estado de los valores admitidos
srvprvTaskGroups	Grupos para los que el usuario es un supervisor de tareas
srvprvUUID	Identificador exclusivo de portlet.
srvprvTaskManager	Supervisor de tareas del grupo de tareas
srvprvYahooIMAddress	Dirección IM de Yahoo

A.2 Extensiones del esquema de la clase de objeto

NOMBRE DE LA CLASE DE OBJETO	DESCRIPCIÓN
srvprvAppConfig	**Contenedor de objetos de configuración de la aplicación del sistema de provisión al que se conecta su controlador DirXML padre**
srvprvAppDefs	Contenedor de objetos de configuración utilizado para inicializar el entorno de tiempo de ejecución de provisión como, por ejemplo, temas para el portal de identidad.
srvprvAssetRecipientAux	Registra la provisión de activos que no son de TI en un usuario
srvprvChoice	Enumeración de valores que se pueden asignar a un atributo concreto, utilizar en una consulta, etc. para utilizarlos en los portlets de identidades y otros componentes de la aplicación Web
srvprvChoiceDefs	Contenedor de definiciones de opciones del nivel de abstracción del directorio que los portlets de identidad y las aplicaciones Web expondrán
srvprvDelegateeAssignment	Definición de una asignación de delegado
srvprvDelegateeDefs	Contenedor de definiciones de delegados
srvprvDirectoryModel	Contenedor de objetos de metanivel del nivel de abstracción del directorio, contenido seleccionado del directorio, que los portlets de identidad y las aplicaciones Web expondrán

NOMBRE DE LA CLASE DE OBJETO	DESCRIPCIÓN
srvprvAppConfig	**Contenedor de objetos de configuración de la aplicación del sistema de provisión al que se conecta su controlador DirXML padre**
srvprvDirectoryModelConfig	Parámetros de configuración del nivel de abstracción del directorio de tiempo de ejecución
srvprvEntity	Define una vista de los atributos seleccionados para las clases definidas en el directorio, utilizada por los portlets de identidad y otros componentes de la aplicación Web
srvprvEntityAux	Clase de objeto estándar
srvprvEntityDefs	Contenedor de definiciones de entidades del nivel de abstracción del directorio que los portlets de identidad y las aplicaciones Web expondrán
srvprvProxyAssignment	Definición de una asignación de apoderado (proxy)
srvprvProxyDefs	Contenedor de definiciones de apoderados (proxy).
srvprvRelationship	Define las relaciones entre objetos del directorio, para utilizarlas en los portlets de identidad y otros componentes de la aplicación Web
srvprvRelationshipDefs	Contenedor de definiciones de relaciones del nivel de abstracción del directorio que los portlets de identidad y las aplicaciones Web expondrán
srvprvRequest	Expone un elemento provisionable que se va a otorgar o revocar, incluido el proceso de flujo de trabajo que define aspectos de tiempo de ejecución del flujo de trabajo y del destino de provisión
srvprvRequestDefs	Contenedor de definiciones de petición de provisión, el conjunto de elementos provisionables para el tiempo de ejecución de la aplicación Web
srvprvResource	Define el conjunto de asignaciones de directorio que se ejecutará para una operación de cumplimiento de provisión (ya sea Otorgar o Revocar)
srvprvResourceDefs	Contenedor de definiciones de destinos de provisión, incluidas descripciones de tiempo de diseño, así como cualquier plantilla o destino no utilizado
srvprvService	Describe cómo invocar un servicio Web específico desde un flujo de trabajo. Esto incluye la especificación de valores de entrada y de retorno
srvprvServiceDefs	Contenedor de objetos de definición de servicios, que empaquetan los servicios Web llamados por los flujos de trabajo.
srvprvTaskGroupAux	Grupo de tareas de provisión de servicio
srvprvTheme	Objeto Tema
srvprvUserAux	Entidad de usuario de provisión de servicio
srvprvWebAppConfig	Objeto de configuración de la aplicación Web

NOMBRE DE LA CLASE DE OBJETO	DESCRIPCIÓN
srvprvAppConfig	**Contenedor de objetos de configuración de la aplicación del sistema de provisión al que se conecta su controlador DirXML padre**
srvprvWorkflow	Define la red de actividades, incluidas las condiciones transversales que se ejecutarán, para obtener una aprobación para una acción de provisión
srvprvWorkflowDefs	Contenedor de objetos de flujo de trabajo, incluidos descripciones de tiempo de diseño y cualquier flujo de plantillas o flujo no utilizado
srvprvServiceDefs	Contenedor de objetos de definición de servicios, que empaquetan los servicios Web llamados por los flujos de trabajo.
srvprvStatus	Especifica el estado de los valores admitidos del objeto de provisión que se incluirán
srvprvTaskGroupAux	Grupo de tareas de provisión de servicio
srvprvTaskGroups	Grupos para los que el usuario es un supervisor de tareas
srvprvTaskManager	Supervisor de tareas del grupo de tareas
srvprvTheme	Objeto Tema
srvprvUserAux	Entidad de usuario de provisión de servicio
srvprvWebAppConfig	Objeto de configuración de la aplicación Web
srvprvWorkflow	Define la red de actividades, incluidas las condiciones transversales que se ejecutarán para obtener una aprobación para una acción de provisión
srvprvWorkflowDefs	Contenedor de objetos de flujo de trabajo, incluidos descripciones de tiempo de diseño y cualquier flujo de plantillas o flujo no utilizado
srvprvYahooIMAddress	Dirección IM de Yahoo

A.3 Representación LDIF

A continuación, proporcionamos información completa (en formato LDIF) del esquema, incluidas la sintaxis, las reglas de contención y más información, que no se muestra en las tablas de resumen anteriores. Esta información está sujeta a cambios.

```
versión: 1 # Copyright (c) 2004-2005 Trabajo no publicado de Novell,
Inc. Reservados todos los derechos. # # ESTE TRABAJO ES UN TRABAJO NO
PUBLICADO Y CONTIENE INFORMACIÓN CONFIDENCIAL Y DE PROPIEDAD, ASÍ COMO
SECRETOS COMERCIALES DE NOVELL, INC. EL ACCESO A ESTE TRABAJO ESTÁ
RESTRINGIDO A (I) LOS EMPLEADOS DE NOVELL, INC. QUE NECESITEN SABER
COMO REALIZAR TAREAS DENTRO DEL ÁMBITO DE SUS ASIGNACIONES Y (II)
ENTIDADES QUE NO SEAN NOVELL, INC. QUE POSEEN LOS ACUERDOS DE LICENCIA
ADECUADOS. NINGUNA PARTE DE ESTE TRABAJO PODRÁ UTILIZARSE, PONERSE EN
PRÁCTICA, COPIARSE, DISTRIBUIRSE, REVISARSE, MODIFICARSE, TRADUCIRSE,
```

```
RESUMIRSE, CONDENSARSE, EXPANDIRSE, RECOPILARSE, COMPILARSE,
ENLAZARSE, REFUNDIRSE, TRANSFORMARSE O ADAPTARSE SIN LA AUTORIZACIÓN
PREVIA POR ESCRITO DE NOVELL, INC. EL USO O EXPLOTACIÓN DE ESTE TRABAJO
SIN AUTORIZACIÓN PUEDE ESTAR SUJETO A RESPONSABILIDAD CRIMINAL Y
CIVIL. # # Base schema extensions for SpitFire # # Last Modified: 6/27/
05 (ek) # # See rfc2252 for information on attribute syntax definitions
#   String = 1.3.6.1.4.1.1466.115.121.1.15 #   Boolean =
1.3.6.1.4.1.1466.115.121.1.7 #   Octet String =
1.3.6.1.4.1.1466.115.121.1.40 #  DN = 1.3.6.1.4.1.1466.115.121.1.12 #
Case Exact String = 1.3.6.1.4.1.1466.115.121.1.26 #   Case Ignore List
= 2.16.840.1.113719.1.1.5.1.6 #   Case Ignore String =
1.3.6.1.4.1.1466.115.121.1.15 #   Stream =
1.3.6.1.4.1.1466.115.121.1.5 #   Time = 1.3.6.1.4.1.1466.115.121.1.24
# # OID registered for EPM: #   subarc "450" registered at: https://
wiki.innerweb.novell.com/wiki.phtml?title=OID_Registration #
attribute prefix: 2.16.840.1.113719.1.450.4.{3 digit unique per
attribute} #   object class prefix: 2.16.840.1.113719.1.450.6.{3 digit
unique number per class} #-----------------------------------------
-------------------------------------------------------------------
---------- #-- Framework Attributes #-------------------------------
-------------------------------------------------------------------
--------------------- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.127 NAME
'srvprvUUID' DESC 'Standard Attribute' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26{64512} SINGLE-VALUE X-NDS_PUBLIC_READ
'1' X-NDS_NOT_SCHED_SYNC_IMMEDIATE '1' ) dn: cn=schema changetype:
modify add: objectClasses objectClasses: (
2.16.840.1.113719.1.450.6.127 NAME 'srvprvEntityAux' DESC 'Standard
ObjectClass' AUXILIARY MAY srvprvUUID X-NDS_NOT_CONTAINER '1' ) #-----
-------------------------------------------------------------------
------------------------------------------------ #-- User Attributes
#-----------------------------------------------------------------
---------------------------------------------------- dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.60 NAME 'srvprvHideUser' DESC 'Indicates if
a user is hidden during searches' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.61 NAME
'srvprvHideAttributes' DESC 'List of attributes a user is hiding from
other users' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.62 NAME 'srvprvQueryList' DESC 'List of
saved query/search criteria' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.63 NAME
'srvprvCapabilities1' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.64 NAME 'srvprvCapabilities2' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.65 NAME
```

```
'srvprvCapabilities3' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.66 NAME 'srvprvCapabilities4' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.67 NAME
'srvprvCapabilities5' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.68 NAME 'srvprvIMAddress' DESC 'Key-value
pair of Instant messenger Addresses i.e. groupwise~jsmith' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) # This is temporary until we convert
the application to use the multi-value IM address (srvprvIMAddress)
above dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.69 NAME
'srvprvGroupwiseIMAddress' DESC 'Groupwise IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.70 NAME
'srvprvYahooIMAddress' DESC 'Yahoo IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.71 NAME
'srvprvAOLIMAddress' DESC 'AOL IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.72 NAME 'srvprvActiveDelegatees' DESC 'The
active delegatees of a user' SYNTAX  2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.73 NAME 'srvprvActiveDelegators' DESC 'The
active delegators of a user' SYNTAX  2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.74 NAME 'srvprvIsTaskManager' DESC
'Indicates if user is a task group manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.75 NAME 'srvprvTaskGroups' DESC 'Groups for
which the user is a task manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.77 NAME
'srvprvPreferredLocale' DESC 'List of saved query/search criteria'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.128 NAME 'srvprvUserAux' DESC 'Service
provisioning user entity' AUXILIARY MAY ( srvprvHideUser $
srvprvHideAttributes $ srvprvQueryList $ srvprvCapabilities1 $
srvprvCapabilities2 $ srvprvCapabilities3 $ srvprvCapabilities4 $
srvprvCapabilities5 $ srvprvIMAddress $ srvprvGroupwiseIMAddress $
```

```
srvprvYahooIMAddress $  srvprvAOLIMAddress $ srvprvIsTaskManager $
srvprvTaskGroups $ srvprvActiveDelegatees $ srvprvActiveDelegators $
srvprvPreferredLocale) X-NDS_NOT_CONTAINER '1' ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.129 NAME 'srvprvTaskManager' DESC 'Task
manager of the task group' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.130 NAME 'srvprvTaskGroupAux' DESC 'Service
provisioning task group' AUXILIARY MAY ( srvprvTaskManager ) X-
NDS_NOT_CONTAINER '1' ) #-----------------------------------------
-----------------------------------------------------------------
--------- #-- Provisioning Attributes #-----------------------------
-----------------------------------------------------------------
---------------------- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.100 NAME
'srvprvCategoryKey' DESC 'Associates a given Provisioning Request
Definition to a set of provisioning categories. Values are keys to a
srvprvChoice instance.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.101 NAME 'srvprvGrant' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Grant operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.102 NAME 'srvprvRevoke' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Revoke operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.103 NAME 'srvprvFlowStrategy' DESC
'Specifies the flow invocation strategy to be used for the Provisioning
Request Definition.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
) dn: cn=schema changetype: modify add: attributeTypes attributeTypes:
( 2.16.840.1.113719.1.450.4.104 NAME 'srvprvLocalizedNames' DESC
'Provides set of localized display name strings for the provisioning
web applications, Designers and iManager.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.105 NAME
'srvprvLocalizedDescrs' DESC 'Provides set of localized description
strings for the provisioning web applications, Designers and
iManager.' SYNTAX  1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.106 NAME 'srvprvStatus' DESC 'Specifies the
status of the Provisioning Object. Supported values will include:
Inactive, Active, Template, and Retired.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.107 NAME 'srvprvProcessXML' DESC 'XML
document representing a Provisioning process definition including
Workflow and Provisioning Action.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.108 NAME 'srvprvEntityType' DESC 'Specifies
Directory Abstraction Layer Entity definition type: P-Public
definitions or S-System definitions.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
```

```
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.109 NAME 'srvprvRequestXML' DESC 'XML
document representing the initial request form and its data bindings'
SYNTAX  1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.110 NAME 'srvprvModified' DESC 'Flag to
indicate changes to definitions object instances in the directory
model container' SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.111 NAME 'srvprvEntitlementRef' DESC
'Reference to a DirXML-Entitlement' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE ) #------------------------
-------------------------------------------------------------------
----------------------------- #-- Provisioning Configuration
Containers #-----------------------------------------------------------
------------------------------------------------------------------ dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.100 NAME 'srvprvAppConfig' DESC 'Container
for application configuration objects of the Provisioning System to
which its DirXML-Driver parent connects.' SUP top STRUCTURAL MUST ( cn
$ version ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'DirXML-Driver' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.101 NAME
'srvprvRequestDefs' DESC 'Container for Provisioning Request
Definitions, the set of provisionable items to the Web Application run-
time.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.102 NAME 'srvprvWorkflowDefs' DESC
'Container for Workflow objects, including design-time descriptions
plus any template or unused flows.' SUP top STRUCTURAL MUST ( cn ) MAY
( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.103 NAME
'srvprvResourceDefs' DESC 'Container for Provisioning Target
definitions, including design-time descriptions plus any template or
unused targets.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.104 NAME 'srvprvServiceDefs' DESC 'Container
for Service Definition objects, which wrap Web Services called by
Workflows.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.105 NAME 'srvprvDirectoryModel' DESC
'Container for Directory Abstraction Layer meta-level objects,
selected contents of the directory to be exposed by the Identity
Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ srvprvModified ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.106 NAME
'srvprvAppDefs' DESC 'Container for configuration objects used to
initialise the Provisioning run-time environment, such as themes for
the Identity Portal.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
```

```
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.111 NAME 'srvprvEntityDefs' DESC 'Container
for Directory Abstraction Layer Entity defintions, to be exposed by the
Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn )
MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.112 NAME
'srvprvRelationshipDefs' DESC 'Container for Directory Abstraction
Layer Relationship definitions, to be exposed by the Identity Portlets
and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) )
dn: cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.113 NAME 'srvprvChoiceDefs' DESC 'Container
for Directory Abstraction Layer Choice definitions, to be exposed by
the Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST (
cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) #### Provisioning Configuration Object
Classes dn: cn=schema changetype: modify add: objectclasses
objectClasses: ( 2.16.840.1.113719.1.450.6.107 NAME 'srvprvRequest'
DESC 'Exposes one provisionable item to be granted or revoked,
including the workflow process which defines the run-time aspects of
the Workflow and Provisioning Target.' SUP top STRUCTURAL MUST ( cn $
srvprvStatus $ srvprvFlowStrategy $ srvprvGrant $ srvprvRevoke $
srvprvCategoryKey $ srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY
( description $ srvprvEntitlementRef $ XmlData $ srvprvRequestXML $
srvprvProcessXML ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvRequestDefs' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.108 NAME 'srvprvWorkflow' DESC 'Defines the
network of activites including traversal conditions to be executed in
order to obtain approval for a provisioning action.' SUP top STRUCTURAL
MUST ( cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs  ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvWorkflowDefs' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.109 NAME 'srvprvResource' DESC 'Defines the
set of directory assignments to execute for a provisioning fulfillment
operation (either Grant or Revoke).' SUP top STRUCTURAL MUST ( cn $
srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY ( description $
srvprvEntitlementRef $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvResourceDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.110 NAME 'srvprvService' DESC 'Describes how
to invoke a specific Web Service from an Workflow. This includes
specification of input and return values.' SUP top STRUCTURAL MUST ( cn
) MAY ( description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvServiceDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.114 NAME 'srvprvEntity' DESC 'Defines a view
of selected attributes for defined classes in the directory, used by
the Identity Portlets and other Web Application components.' SUP top
STRUCTURAL MUST ( cn $ srvprvEntityType ) MAY ( description $ XmlData )
X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
```

```
'srvprvEntityDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.115 NAME
'srvprvRelationship' DESC 'Defines relationships between objects in
the directory, for use in the Identity Portlets and other Web
Application components.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvRelationshipDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.116 NAME 'srvprvChoice' DESC 'Enumeration of
values which can be assigned to a particular attribute, used in a
query, etc. for use in the Identity Portlets and other Web Application
components.' SUP top STRUCTURAL MUST ( cn ) MAY ( description $ XmlData
) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvChoiceDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.113719.1.450.6.117 NAME
'srvprvDirectoryModelConfig' DESC 'Runtime Directory Abstraction Layer
configurarion parameters' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) ) #### User Aux Classes
and Attributes dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.80 NAME 'srvprvAssetRef'
DESC 'Representation of the aggregate asset properties for a named
asset associated to a user via the srvprvAssetRecipientAux class.'
SYNTAX 2.16.840.1.113719.1.1.5.1.6 ) dn: cn=schema changetype: modify
add: objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.80 NAME
'srvprvAssetRecipientAux' DESC 'Records the provisioning of non-IT
assets on a user' AUXILIARY MAY ( srvprvAssetRef ) ) #----------------
------------------------------------------------------------------------
------------------------------------ #-- Web Application Config
Class #-------------------------------------------------------------
------------------------------------------------------------ dn:
cn=schema changetype: modify add: attributeTypes attributeTypes:
(2.16.840.1.113719.1.450.4.20 NAME 'srvprvDefaultTheme' DESC 'The
default theme' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.21 NAME 'srvprvWebAppConfig' DESC 'Web
Application Config Object' SUP top STRUCTURAL MUST (cn) MAY
(description $ srvprvDefaultTheme $ XmlData ) X-NDS_NOT_CONTAINER '1'
X-NDS_NAMING 'cn' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) ) #-----------
------------------------------------------------------ ------------
---------------------------------------- #-- Theme Branding
Structural Class #--------------------------------------------------
------------------------------------------------------------------------
-- dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.21 NAME
'srvprvHeaderLogoImage' DESC 'Header Logo Primary Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.22 NAME 'srvprvHeaderLogoFile' DESC 'Header
Logo Primary Image File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.23 NAME
'srvprvHeaderLogoLastMod' DESC 'Header Logo Primary Last Modified'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
```

```
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.24 NAME 'srvprvHeaderLogo2Image' DESC
'Header Logo Secondary Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.25 NAME
'srvprvHeaderLogo2File' DESC 'Header Logo Secondary Image File Name'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 | SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.26 NAME 'srvprvHeaderLogo2LastMod' DESC
'Header Logo Secondary Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.27 NAME 'srvprvHeaderTextureImage' DESC
'Header Texture Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.28 NAME
'srvprvHeaderTextureFile' DESC 'Header Texture File Name' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.29 NAME 'srvprvHeaderTextureLastMod' DESC
'Header Texture Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.30 NAME
'srvprvHeaderFillerImage' DESC 'Header Filler Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.31 NAME 'srvprvHeaderFillerFile' DESC
'Header Filler File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.32 NAME
'srvprvHeaderFillerLastMod' DESC 'Header Filler Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.33 NAME 'srvprvLoginImage' DESC 'Login
Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.34 NAME 'srvprvLoginFile' DESC 'Login File
Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.35 NAME 'srvprvLoginLastMod' DESC 'Login
Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.36 NAME 'srvprvLoginSmallImage' DESC 'Login
Small Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.37 NAME 'srvprvLoginSmallFile' DESC 'Login
Small File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.38 NAME 'srvprvLoginSmallLastMod' DESC
'Login Small Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.39 NAME 'srvprvNavColor'
DESC 'Navigation Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
```

```
attributeTypes: ( 2.16.840.1.113719.1.450.4.40 NAME
'srvprvNavColorLastMod' DESC 'Navigation Color Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.41 NAME 'srvprvNavBckgrColor' DESC
'Navigation Background Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.42 NAME
'srvprvNavBckgrColorLastMod' DESC 'Navigation Background Color Last
Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.20 NAME 'srvprvTheme' DESC 'Theme Object'
SUP top STRUCTURAL MUST (cn) MAY (description $ srvprvHeaderLogoImage
$ srvprvHeaderLogoFile $ srvprvHeaderLogoLastMod $
srvprvHeaderLogo2Image $ srvprvHeaderLogo2File $
srvprvHeaderLogo2LastMod $ srvprvHeaderTextureImage $
srvprvHeaderTextureFile $ srvprvHeaderTextureLastMod $
srvprvHeaderFillerImage $ srvprvHeaderFillerFile $
srvprvHeaderFillerLastMod $ srvprvLoginImage $ srvprvLoginFile $
srvprvLoginLastMod $ srvprvLoginSmallImage $ srvprvLoginSmallFile $
srvprvLoginSmallLastMod $ srvprvNavColor $ srvprvNavColorLastMod $
srvprvNavBckgrColor $ srvprvNavBckgrColorLastMod ) X-NDS_NOT_CONTAINER
'1' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) X-NDS_NAMING 'cn' ) #-------
------------------------------------------------------------------
---------------------------------------------- #-- Attributes,
objects, and containers for Proxy, Delegatee and User availability, #-
------------------------------------------------------------------
------------------------------------------------------ dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.120 NAME 'srvprvAssignFromUser' DESC 'User
subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.121 NAME
'srvprvAssignFromGroup' DESC 'Group subjects of a proxy or delegatee
assignment' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.122 NAME 'srvprvAssignFromContainer' DESC
'Container subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.123 NAME
'srvprvAssignToUser' DESC 'The User targets of a proxy or delegatee
assignment' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.124 NAME 'srvprvAssignToRelationship' DESC
'A target relationship of a delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.125 NAME 'srvprvAssignExpiration' DESC 'Time
at which a proxy or delegatee assignment expires' SYNTAX
1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.126 NAME 'srvprvRequestDefName' DESC 'The
provisioning request definition name associated with a delegatee
definition.' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
```

```
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.120 NAME 'srvprvProxyDefs' DESC 'Container
for proxy definitions.' SUP top STRUCTURAL MUST ( cn ) MAY (
description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.121 NAME
'srvprvDelegateeDefs' DESC 'Container for delegatee definitions.' SUP
top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.122 NAME 'srvprvProxyAssignment' DESC 'Proxy
assignment definition' SUP top STRUCTURAL MUST ( cn $
srvprvAssignToUser ) MAY ( description $ srvprvAssignFromUser $
srvprvAssignFromGroup $ srvprvAssignFromContainer $
srvprvAssignExpiration ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvProxyDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.123 NAME
'srvprvDelegateeAssignment' DESC 'Delegatee assignment definition' SUP
top STRUCTURAL MUST cn MAY ( srvprvRequestDefName $ description $
srvprvAssignFromUser $ srvprvAssignFromGroup $
srvprvAssignFromContainer $ srvprvAssignToUser $
srvprvAssignToRelationship $ srvprvAssignExpiration ) X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvDelegateeDefs' ) ) ############### DO
NOT DELETE THIS LINE ###################
############################################################
```

Configuración del archivo de reserva de la aplicación

B

En este apéndice se describen los valores avanzados que se pueden configurar sólo editando el archivo WAR de la aplicación de usuario. Los temas son:

B.1 Acerca del archivo WAR de la aplicación de usuario

La aplicación de usuario del Gestor de identidades está empaquetada como un archivo de reserva WAR de la aplicación Web compatible con J2EE. El archivo WAR de la aplicación de usuario contiene un conjunto de clases Java y archivos XML que controlan el comportamiento en tiempo de ejecución de la aplicación. Por lo general, este archivo no debe modificarse, aunque en casos excepcionales, es posible que necesite abrirlo e introducir cambios menores para controlar el comportamiento de la aplicación.

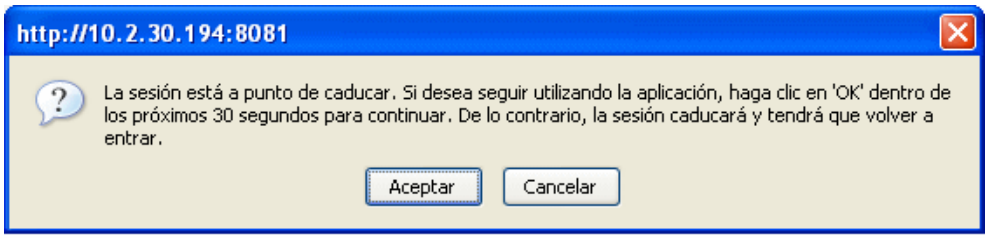
Nota: En la parte restante de este apéndice, se presupone que el lector está familiarizado con los procedimientos y conceptos de J2EE. Si no está seguro acerca de cómo realizar cambios dentro de un archivo WAR, consulte la documentación de J2EE.

B.2 Configuración del tiempo límite de la sesión

Para evitar que el servidor se sobrecargue con sesiones inactivas, la aplicación de usuario del Gestor de identidades agotará el tiempo límite de una sesión de usuario que permanezca inactiva durante un amplio período de tiempo. El intervalo de tiempo límite por defecto es de 10 minutos. Puede cambiar el valor por defecto editando el archivo *web.xml* en la carpeta WEB-INF del archivo WAR de la aplicación de usuario.

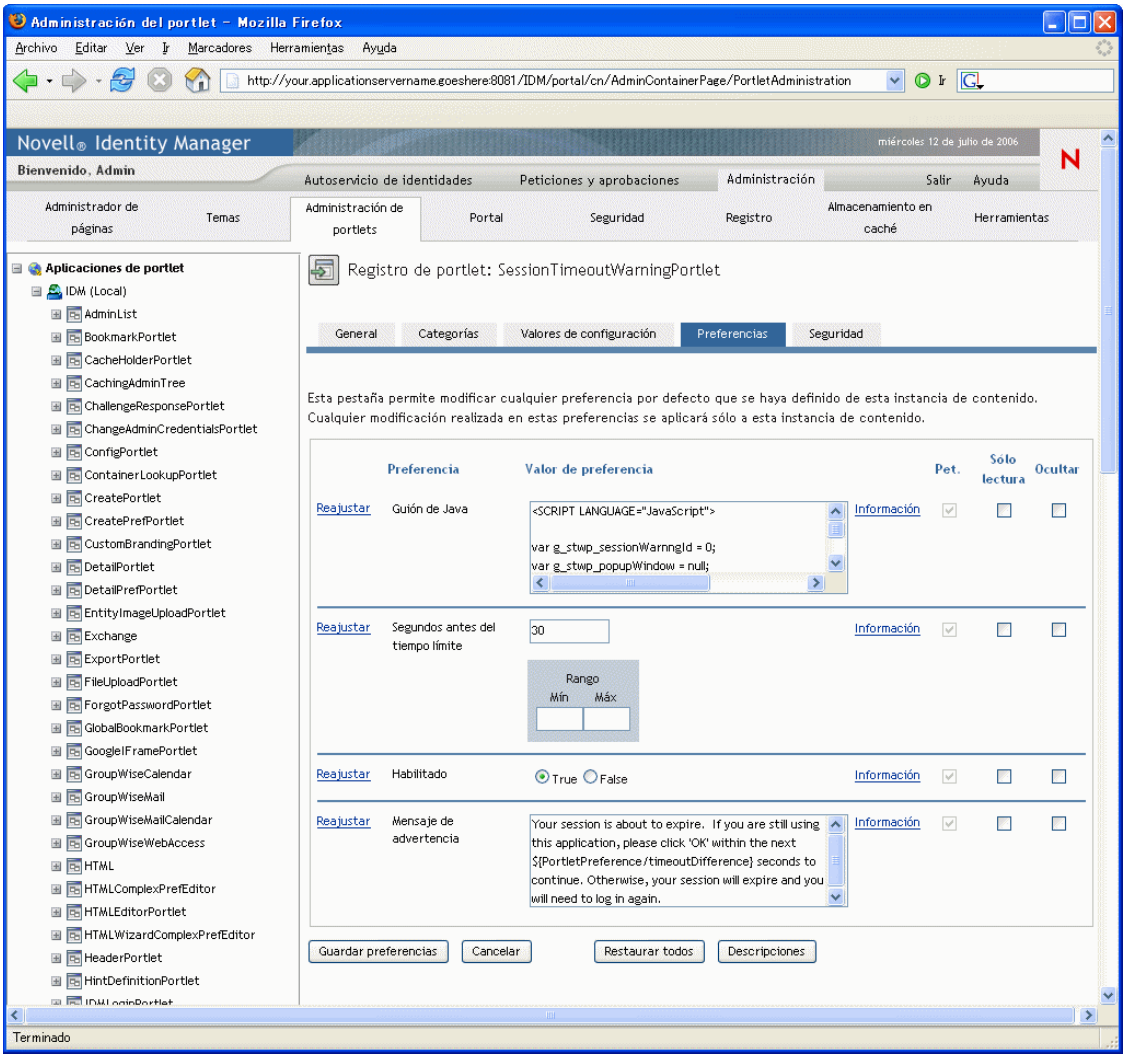
Edición del intervalo de tiempo límite de una sesión El archivo web.xml de WAR tiene un elemento denominado <*session-timeout*> (que se encuentra bajo el elemento <*session-config*>) que especifica durante cuánto tiempo puede permanecer inactiva una sesión antes de que alcance su tiempo límite. Para definir el intervalo de tiempo límite de una sesión, cambie el valor de este elemento. El valor debe especificarse en minutos.

Control del comportamiento del mensaje de alerta Por defecto, la aplicación de usuario del Gestor de identidades muestra un mensaje de alerta siempre que una sesión de usuario está a punto de alcanzar su tiempo límite.



Si el usuario no responde al mensaje haciendo clic en Aceptar, la sesión alcanzará su tiempo límite. El mensaje de alerta está habilitado por defecto. Si así lo desea, puede inhabilitarlo. Además, puede especificar durante cuánto tiempo el usuario puede responder al mensaje de alerta.

Para controlar el comportamiento del mensaje de alerta, deberá configurar *SessionTimeoutWarningPortlet*. Para ello, será preciso editar las preferencias del portlet en el registro de portlet, tal como se muestra a continuación:



Para especificar durante cuánto tiempo el usuario puede responder al mensaje de alerta, edite el valor *Segundos antes del tiempo límite*. Para inhabilitar el mensaje de alerta, haga clic en *False (Falso)* al lado de *Enabled (Habilitado)*. Cuando haya acabado de introducir los cambios, haga clic en *Guardar preferencias*.