Guía del administrador de negocio de Sun Identity Manager 8.1

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Referencia: 821–0062
Julio de 2009

090805@22510

Contenido

Prefacio

En esta guía se explica cómo utilizar el software de Sun™Identity Manager (Identity Manager) para proporcionar acceso seguro a los sistemas de información y las aplicaciones de su empresa. Aquí encontrará procedimientos y escenarios que le ayudarán a realizar las tareas habituales y de administración con el sistema Identity Manager.

Quiénes deben usar esta guía

Esta *Guía del administrador de negocio de Sun Identity Manager 8.1* está destinada a los administradores, desarrolladores de software y proveedores de servicios informáticos que implementan una plataforma integrada de gestión de identidades y acceso web utilizando el software y los servidores de Identity Manager.

Si conoce las tecnologías siguientes le resultará más fácil aplicar la información que contiene este manual:

- Protocolo ligero de acceso a directorios (LDAP)
- Java
- JavaServer Pages™ (JSP™)
- Protocolo de transferencia de hipertexto (HTTP)
- Lenguaje de marcado de hipertexto (HTML)
- Lenguaje de marcado extensible (XML)

Antes de leer este manual

Identity Manager es un componente de Sun Java Enterprise System, una infraestructura de software para aplicaciones empresariales distribuidas en un entorno de red o de Internet. Le conviene conocer la documentación suministrada con Sun Java Enterprise System, a la que puede acceder online en `http://docs.sun.com/coll/entsys_04q4`.

Dado que Identity Manager Directory Server se utiliza como almacén de datos en las implementaciones de Identity Manager, también debe familiarizarse con la documentación suministrada con dicho producto. Puede acceder online a la documentación de Directory Server en `http://docs.sun.com/coll/DirectoryServer_04q2`.

Organización de esta guía

Esta guía se divide en los capítulos y apéndices siguientes:

Capítulo 1, “Introducción a Identity Manager ”, donde se explica cómo Identity Manager y los distintos objetos de Identity Manager le ayudan a superar los retos administrativos en un entorno de trabajo dinámico.

Capítulo 2, “Introducción a la interfaz de usuario de Identity Manager ”, donde se explica cómo utilizar la interfaz gráfica de usuario de Identity Manager.

Capítulo 3, “Administración de usuarios y de cuentas”, que trata sobre la creación y administración de usuarios con la interfaz de administración.

Capítulo 5, “Roles y recursos”, que contiene información útil para comprender los roles y recursos de Identity Manager.

Capítulo 4, “Configuración de objetos de administración de negocio”, con información y procedimientos para configurar y mantener los objetos de administración de Identity Manager, como directivas, plantillas de correo electrónico, eventos y grupos de auditoría, entre otros.

Capítulo 6, “Administración”, que explica la utilización de la interfaz de administración para realizar diversas tareas del nivel de administrador. En este capítulo también encontrará información sobre el uso de roles, roles administrativos y capacidades.

Capítulo 7, “Carga y sincronización de datos”, dedicado al uso de las funciones de carga y sincronización de datos de Identity Manager para mantener la información al día.

Capítulo 8, “Informes”, que constituye una introducción a los tipos de informes de Identity Manager y explica cómo crear y administrar informes.

Capítulo 9, “Plantillas de tarea”, que presenta las plantillas de tarea de Identity Manager y su uso para configurar comportamientos de flujo de trabajo.

Capítulo 10, “Registro de auditoría”, donde se describe el sistema de auditoría de Identity Manager.

Capítulo 11, “PasswordSync”, que cubre la instalación, configuración y utilización de la función PasswordSync para detectar y sincronizar los cambios de contraseña.

Capítulo 12, “Seguridad”, donde se explica cómo usar Identity Manager para gestionar la seguridad del sistema.

Capítulo 13, “Auditoría de identidades: Conceptos básicos”, con los conceptos fundamentales de la auditoría de identidades y los controles de identidades.

Capítulo 14, “Auditoría: Directivas de auditoría”, donde se explica la creación y administración de directivas de auditoría mediante el Asistente de directiva de auditoría.

Capítulo 15, "Auditoría: Cumplimiento de supervisión", que explica cómo realizar revisiones de auditoría y administrar el cumplimiento de las normativas vigentes.

Capítulo 16, "Exportador de datos", donde conocerá el Exportador de datos y aprenderá a utilizar esta funcionalidad para escribir información sobre usuarios, roles y otros tipos de objetos en un almacén de datos externo.

Capítulo 17, "Administración de Service Provider", que trata sobre la configuración y administración de Service Provider.

Apéndice A, "Referencia de `lh`", que aborda el funcionamiento de la línea de comandos de Identity Manager.

Apéndice B, "Esquema de base de datos de registros de auditoría", con información sobre los valores de esquema de datos de auditoría para los tipos de base de datos compatibles y las asignaciones de registros de auditoría.

Apéndice C, "Referencia rápida de la interfaz de usuario", donde encontrará enseguida cómo se realiza cualquier tarea habitual en Identity Manager.

Apéndice D, "Definiciones de capacidades", una referencia rápida de las capacidades funcionales y basadas en tareas que puede asignar a los usuarios.

Guías relacionadas

Sun ofrece más documentación e información para ayudarle a instalar, utilizar y configurar Identity Manager. La biblioteca de Sun Identity Manager 8.1 está formada por las publicaciones indicadas a continuación.

Destinatarios principales	Título	Descripción
Todos	*Introducción a Sun Identity Manager*	Proporciona una descripción general de las características y la funcionalidad de Identity Manager. Incluye información sobre la arquitectura del producto y la integración de Identity Manager con otros productos de Sun, como Sun Open SSO Enterprise y Sun Role Manager.
	Notas de la versión de Sun Identity Manager 8.1	Incluye problemas específicos, problemas resueltos e información de última hora que no aparece en la documentación principal de Identity Manager.

Destinatarios principales	Título	Descripción
Administradores del sistema	*Sun Identity Manager 8.1 Installation*	Instrucciones para instalar Identity Manager y los componentes opcionales, como la Puerta de enlace de Sun Identity Manager y PasswordSync.
	Sun Identity Manager 8.1 Upgrade	Contiene instrucciones para actualizar desde una versión anterior de Identity Manager a una más reciente.
	Sun Identity Manager 8.1 System Administrator's Guide	Contiene información e instrucciones que ayudan a los administradores del sistema a gestionar, mejorar y solucionar los problemas de la instalación de Identity Manager.
Administradores de negocio	*Guía del administrador de negocio de Sun Identity Manager 8.1*	Explica cómo usar las funciones de abastecimiento y auditoría de Identity Manager. Incluye información sobre las interfaces de usuario, la administración de usuarios y cuentas, la generación de informes y más.
Integradores de sistemas	*Sun Identity Manager Deployment Guide*	Explica cómo implementar Identity Manager en los entornos de TI complejos. Incluye temas que abarcan el uso de atributos de identidad, la carga y sincronización de datos, la configuración de acciones de usuario, la aplicación de marcas de identidad personalizadas, etc.
	Sun Identity Manager Deployment Reference	Contiene información sobre flujos de trabajo, formularios, vistas, reglas y el lenguaje XPRESS.
	Sun Identity Manager 8.1 Resources Reference	Información para instalar, configurar y utilizar los adaptadores de recursos.
	Sun Identity Manager Service Provider 8.1 Deployment	Explica cómo implementar Sun Identity Manager Service Provider y en qué se diferencian las vistas, los formularios y los recursos respecto al producto Identity Manager estándar.
	Sun Identity Manager 8.1 Web Services	Explica cómo configurar la compatibilidad SPML, qué funciones SPML se admiten (y por qué) y cómo ampliar la compatibilidad en el campo.

Además, el sitio web `http://docs.sun.com` le proporciona acceso online a la documentación técnica de Sun. Puede examinar nuestro material de archivo o buscar un tema o manual específico.

Actualizaciones de la documentación

Las correcciones y actualizaciones para ésta y otras publicaciones sobre Identity Manager se colocan en la web de actualizaciones a la documentación de Identity Manager :

`http://blogs.sun.com/idmdocupdates/`

Es posible utilizar un canal RSS para comprobar periódicamente este sitio y recibir notificaciones cuando haya actualizaciones disponibles. Para suscribirse, descargue un lector de RSS y haga clic bajo Feeds en el lado derecho de la página. Desde la versión 8.0, existen diferentes canales para cada versión principal.

Referencias a sitios web de terceros relacionados

En este documento se proporcionan direcciones de Internet de terceros e información adicional relacionada.

Nota – Sun no se responsabiliza de la disponibilidad de los sitios Web de terceros que se mencionan en este documento. Sun no avala ni se hace responsable del contenido, la publicidad, los productos ni otros materiales disponibles en dichos sitios o recursos, o a través de ellos. Sun declina toda responsabilidad sobre los posibles daños o pérdidas, reales o presuntos, causados o presuntamente causados directa o indirectamente por los contenidos, bienes o servicios citados u otros accesibles en o a través de esas páginas o recursos.

Documentación, asistencia y formación

El sitio web de Sun proporciona información sobre estas otras fuentes de recursos:

- Documentación (`http://www.sun.com/documentation/`)
- Asistencia técnica (`http://www.sun.com/support/`)
- Formación (`http://www.sun.com/training/`)

Sun valora sus comentarios

En Sun estamos interesados en mejorar nuestra documentación y, por tanto, agradecemos sus comentarios y sugerencias. Para enviarnos sus comentarios, entre en `http://docs.sun.com`

Convenciones tipográficas

En la tabla siguiente se describen las convenciones tipográficas utilizadas en este documento.

TABLA P–1 Convenciones tipográficas

Tipo de letra	Significado	Ejemplo
`AaBbCc123`	Nombres de comandos, archivos y directorios; mensajes del sistema que aparecen en la pantalla.	Edite el archivo `.login`. Utilice el comando `ls- a` para ver la lista de archivos. `nombre_máquina% ha recibido correo.`
`AaBbCc123`	Lo que escribe el usuario, frente a los mensajes del propio sistema.	`nombre_máquina%` **`su`** `Contraseña:`
aabbcc123	Elemento variable: se sustituye por un nombre o un valor real.	El comando para eliminar un archivo es `rm` *nombrearchivo*.
AaBbCc123	Títulos de libros, palabras o términos nuevos y palabras que deben enfatizarse.	Lea el Capítulo 6 de la *Guía de usuario*. Una copia en *caché* es aquella que se almacena localmente. *No* guarde el archivo. **Nota:** Algunos términos enfatizados aparecen en negrita en los documentos en línea.

Indicadores de shell en los ejemplos de comandos

La tabla siguiente muestra el indicador predeterminado y el indicador de superusuario de los sistemas UNIX® para los shells de C, Bourne y Korn.

TABLA P–2 Indicadores del shell

Shell	Mensaje de petición
C	`nombre-máquina%`
Shell de superusuario de C	`nombre_máquina#`
Shells de Bourne y Korn	`$`
Shells de Bourne y Korn para superusuario	`#`

◆ ◆ ◆ CAPÍTULO 1

1 Introducción a Identity Manager

El sistema Sun Identity Manager le permite administrar y auditar el acceso a las cuentas y los recursos. Como le proporciona capacidades y herramientas para gestionar ágilmente las tareas periódicas y diarias de auditoría y abastecimiento de usuarios, Identity Manager le ayuda a prestar un servicio excepcional tanto a los clientes internos como externos.

Este capítulo contiene los temas siguientes:

Visión global

Las empresas actuales exigen más flexibilidad y prestaciones a sus servicios de TI. La administración del acceso a la información y los sistemas de empresa ha exigido tradicionalmente una interacción directa con un número restringido de cuentas. En la actualidad, administrar el acceso significa gestionar no sólo muchos más clientes internos, sino también colaboradores y clientes fuera de la empresa.

Esta mayor necesidad de acceso puede generar una carga adicional indirecta considerable. Como administrador, debe posibilitar de una manera efectiva y segura que los usuarios hagan su trabajo fuera y dentro de la empresa. Tras darles el acceso inicial, se enfrenta a constantes dificultades, como olvido de contraseñas o cambios de funciones y relaciones empresariales.

Además, las compañías actuales deben cumplir normativas estrictas que rigen la seguridad y la integridad de la información crítica de la empresa. En un entorno dictaminado por la legislación relativa al cumplimiento –como las leyes Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA) y Gramm-Leach-Bliley (GLB) en EE.UU.–, las actividades de supervisión y producción de informes engendran una carga adicional indirecta cuantiosa y muy cara. Usted necesita capacidad para poder responder rápidamente a los cambios del control de acceso y para satisfacer las demandas de recopilación de datos y generación de informes que contribuyen a mantener segura a su empresa.

Identity Manager está específicamente desarrollado para ayudarle a superar estas dificultades administrativas en un entorno dinámico. Al utilizar Identity Manager para distribuir la carga adicional indirecta que supone administrar el acceso y para acometer los retos del cumplimiento, aporta una solución a sus problemas primordiales: ¿cómo definir el acceso? Una vez definido, ¿cómo mantener la flexibilidad y el control?

Por su diseño seguro y flexible a la vez, puede configurar Identity Manager adaptándolo a la estructura de su empresa para solucionar estos problemas. La asignación de los objetos de Identity Manager a las entidades que usted administra (usuarios y recursos) le permite elevar drásticamente su eficiencia operativa.

En un entorno de proveedor de servicios, Identity Manager amplía estas capacidades para administrar también los usuarios de extranet.

Objetivos del sistema Identity Manager

La solución Identity Manager le permite cumplir los siguientes objetivos:

- Administrar el acceso a las cuentas para una enorme variedad de sistemas y recursos.
- Administrar de forma segura la información de cuenta dinámica para cada matriz de cuentas de usuario.
- Configurar derechos delegados para crear y administrar datos de cuentas de usuario.
- Gestionar grandes volúmenes de recursos empresariales y un número cada vez mayor de clientes y colaboradores de extranet.
- Autorizar el acceso seguro de los usuarios a los sistemas de información de la empresa. Identity Manager le proporciona funcionalidad completamente integrada para conceder, administrar y revocar privilegios de acceso en la totalidad de las organizaciones internas y externas.
- Mantener sincronizados los datos *sin* conservar los datos. La solución Identity Manager sustenta dos principios claves que deberían respetar las mejores herramientas de administración de sistemas:
  - El producto apenas debe causar impacto en el sistema que administra.
  - El producto no debe aumentar la complejidad de la empresa incorporando otro recurso que administrar.

  Definir directivas de auditoría para gestionar el cumplimiento con privilegios de acceso de usuario y administrar las infracciones automatizando las acciones de remediación y las alertas de correo electrónico.
- Efectuar revisiones de acceso periódicas y definir procedimientos de aprobación y de revisión de autenticación para automatizar el proceso de certificación de privilegios de usuario.

- Supervisar la información clave y auditar y revisar las estadísticas mediante el panel de control.

Definición del acceso de los usuarios a los recursos

Pueden ser *usuarios* de su empresa extendida todas las personas relacionadas con ella, incluidos empleados, clientes, colaboradores, proveedores o adquisiciones. En el sistema Identity Manager, los usuarios se representan con *cuentas de usuario*.

Según las relaciones que tengan con su empresa y otras entidades, los usuarios necesitarán acceso a distintas cosas, como sistemas informáticos, datos almacenados en bases de datos o aplicaciones informáticas concretas. En la terminología de Identity Manager, esas cosas se denominan *recursos*.

Como los usuarios suelen tener una o más identidades en cada recurso al que acceden, Identity Manager crea una única *identidad virtual* que se asigna a distintos recursos. Ello le permite administrar los usuarios como una única entidad. Consulte la Figura 1–1.

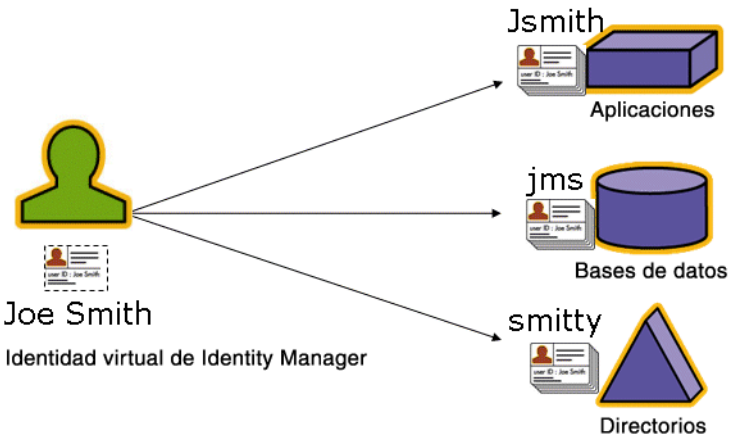


FIGURA 1–1 Relación entre los recursos de cuenta de usuario en Identity Manager

Para administrar eficazmente muchos usuarios, hay que agruparlos de una manera lógica. En la mayoría de las empresas, los usuarios se agrupan por departamentos funcionales o divisiones geográficas. Normalmente, cada uno de estos departamentos necesita acceso a diferentes recursos. En la terminología de Identity Manager, este tipo de grupo de denomina *organización*.

Otra manera de agrupar los usuarios es por características similares, como las relaciones con la empresa o las funciones del cargo. Estos agrupamientos se consideran *roles* en Identity Manager.

Dentro del sistema Identity Manager, se asignan roles a las cuentas de usuario para facilitar la habilitación e inhabilitación eficientes del acceso a los recursos. Asignar las cuentas a organizaciones permite una delegación eficiente de las responsabilidades administrativas.

Los usuarios de Identity Manager también se administran de forma directa o indirecta aplicando *directivas*, que determinan reglas, contraseñas y opciones de autenticación de los usuarios.

Tipos de usuario

Identity Manager ofrece dos tipos de usuario: *usuarios de Identity Manager* y *usuarios de Service Provider*, en caso de que configure el sistema Identity Manager para una implementación de proveedor de servicios. Estos tipos le permiten diferenciar usuarios que pueden tener distintos requisitos de abastecimiento según su relación con la empresa, por ejemplo, usuarios de extranet frente a usuarios de intranet.

Un escenario típico para una implementación de proveedor de servicios es una empresa proveedora de servicios que tiene usuarios internos y externos (clientes) que desea administrar mediante Identity Manager. Encontrará información para configurar una implementación de proveedor de servicios en la guía *Sun Identity Manager Service Provider 8.1 Deployment* .

El tipo de usuario de Identity Manager se especifica al configurar una cuenta de usuario. Para obtener más información sobre los usuarios de proveedor de servicios, consulte el Capítulo 17, “Administración de Service Provider”.

Delegación de la administración

Para distribuir satisfactoriamente la responsabilidad de administrar identidades de usuario, necesita el equilibrio adecuado de flexibilidad y control. Si concede determinados privilegios de administración de usuarios y delega tareas administrativas en Identity Manager, reducirá la carga adicional indirecta y aumentará la eficiencia al depositar la responsabilidad de administrar las identidades en aquellas personas que mejor conocen las necesidades de los usuarios, por ejemplo, un gerente de contratación. Los usuarios que poseen estos privilegios ampliados se denominan *administradores* de Identity Manager.

Sin embargo, la delegación sigue un patrón de seguridad. Para conservar un control adecuado, Identity Manager le permite asignar distintos niveles de *capacidades* a los administradores. Las capacidades autorizan niveles variables de acceso y acciones dentro del sistema.

El modelo de flujo de trabajo de Identity Manager incluye además un método para garantizar que se exija aprobación a determinadas acciones. El flujo de trabajo permite a los administradores de Identity Manager ejercer control sobre las tareas y llevar un seguimiento de su evolución. Para obtener más información sobre el flujo de trabajo, consulte el Capítulo 1, “Workflow” de *Sun Identity Manager Deployment Reference*.

Objetos de Identity Manager

Para administrar e implementar satisfactoriamente el sistema, es fundamental tener una visión nítida de los objetos de Identity Manager y cómo interactúan. Estos objetos son:

Nota – Al asignar nombre a los objetos de Identity Manager, no utilice los caracteres siguientes:

' (apóstrofo), . . (punto), | (línea), [(corchete izquierdo),] (corchete derecho), , (coma), : (dos puntos), $ (símbolo de dólar), " (comillas), \ (barra inclinada inversa) y = (signo de igual).

También deben evitarse los caracteres siguientes: _ (subrayado), % (porcentaje), ^ (acento circunflejo) y * (almohadilla).

Cuentas de usuario de Identity Manager

Un usuario es cualquiera que detente una cuenta del sistema Identity Manager. Identity Manager almacena diversos datos para cada usuario. En conjunto, esta información constituye una identidad de Identity Manager de un usuario.

Cuentas de usuario de Identity Manager

- Proporcionan a los usuarios acceso a uno o varios recursos, y administran los datos de las cuentas de usuario en esos recursos.
- Se les asignan roles, que condicionan el acceso de cada usuario a los distintos recursos.
- Forman parte de una organización, que determina cómo y quién administra las cuentas de usuario.

Configurar una cuenta de usuario es un proceso dinámico. Según los roles que seleccione al configurar la cuenta, podrá suministrar información de recurso más o menos específica para crear la cuenta. El número y el tipo de recursos asociados al rol asignado determinan la cantidad de información necesaria para crear la cuenta.

Los administradores son usuarios que poseen privilegios adicionales para administrar cuentas de usuario, recursos y otros objetos y tareas del sistema Identity Manager. Los administradores de Identity Manager gestionan las organizaciones y se les asigna una gama de capacidades que se aplican a los objetos en cada organización administrada.

Para obtener más información sobre las cuentas de usuario, consulte el Capítulo 3, "Administración de usuarios y de cuentas". Para obtener más información sobre las cuentas de administrador, consulte el Capítulo 6, "Administración".

Roles de Identity Manager

Un rol es un objeto de Identity Manager que permite agrupar los derechos de acceso a los recursos y asignarlos eficazmente a los usuarios. Los roles se organizan en cuatro tipos:

- Roles de negocio
- Roles de TI
- Aplicaciones
- Activos

Los *roles de negocio* sirven para organizar en grupos los derechos de acceso que necesitan las personas que realizan tareas similares en una organización. Los roles de negocio suelen representar funciones de tareas de usuario.

Los *roles de TI, las aplicaciones* y los *activos* organizan los derechos de recursos (o *derechos de acceso*) en grupos. Para proporcionar a los usuarios acceso a los recursos, los roles de negocio se asignan a roles de TI, aplicaciones y activos, lo que permite a los usuarios acceder a los recursos que necesitan para realizar sus tareas.

Los roles de TI, las aplicaciones y los activos pueden ser *requeridos, condicionales* u *opcionales.*

- **Los roles requeridos** se asignan siempre al usuario.
- **Los roles condicionales** tienen condiciones que deben evaluarse como verdaderas para poder ser asignados.
- **Los roles opcionales** se pueden solicitar por separado y, una vez aprobados, asignar al usuario.

Como los roles pueden ser condicionales u opcionales, los usuarios que tienen la misma descripción general de tareas pueden tener el mismo rol de negocio y, sin embargo, poseer derechos de acceso diferentes. Ello permite a un diseñador de roles de negocio definir un acceso genérico a los roles para cumplir las normativas, dejando flexibilidad al administrador para definir con precisión los derechos de acceso del usuario. Así no hace falta definir un nuevo rol de negocio cada vez que cambian las necesidades de acceso en la empresa, problema que se conoce como *explosión de roles*.

A un usuario se le puede asignar un rol, varios o ninguno.

Nota – Para obtener más información sobre los roles, consulte "Conceptos y administración de roles" en la página 121.

Recursos y grupos de recursos

Identity Manager almacena información sobre cómo conectarse a un recurso o un sistema. Los recursos a los que Identity Manager proporciona acceso incluyen:

- Recursos digitales, como:
  - Administradores de seguridad de sistemas centrales (mainframe)
  - Bases de datos
  - Servicios de directorio (como LDAP)
  - Aplicaciones
  - Sistemas operativos
  - Sistemas ERP (como SAP™)
- Recursos no digitales o `externos` a Identity Manager, por ejemplo:
  - Teléfonos móviles
  - Equipos de sobremesa
  - Equipos portátiles
  - Identificadores de seguridad

Cada recurso de Identity Manager almacena los siguientes tipos de información:

- Parámetros de recurso
- Parámetros de Identity Manager
- Información de cuenta (incluidos los atributos de cuenta y la plantilla de identidad)

Hay dos formas de asignar recursos a los usuarios: directamente (asignación individual o directa) o bien asignando el recurso a un rol, que a su vez se asigna a un recurso (asignación basada en roles o indirecta).

- **Asignación individual**. Los distintos recursos se asignan directamente a las cuentas de usuario.
- **Asignación basada en roles**. Uno o más recursos se asignan a un rol (aplicación, activo o rol de TI). A continuación, la aplicación, el activo o el rol de TI se asigna a un rol de negocio. Por último, se asignan uno o más roles de negocio a una cuenta de usuario.

Un objeto relacionado de Identity Manager, el *grupo de recursos*, se puede asignar a las cuentas de usuario del mismo modo que los recursos. Los grupos de recursos correlacionan los recursos para que pueda crear cuentas por un orden concreto en los recursos. También simplifican el proceso de asignación de múltiples recursos a las cuentas de usuario.

Para obtener más información sobre los grupos de recursos, consulte "Grupos de recursos" en la página 170.

Organizaciones y organizaciones virtuales

Las organizaciones son contenedores de Identity Manager que sirven para habilitar la delegación administrativa. Definen el ámbito de las entidades que administra o controla un administrador de Identity Manager.

Las organizaciones también pueden representar vínculos a recursos basados en directorios. En tal caso, se denominan *organizaciones virtuales*. Las organizaciones virtuales permiten administrar directamente los datos de los recursos sin cargar información en el depósito de Identity Manager. Con una organización virtual, Identity Manager refleja la estructura de directorios existente y la afiliación de usuarios y, en consecuencia, elimina las tareas de configuración repetidas y lentas.

Las organizaciones que a su vez contienen a otras organizaciones se denominan *organizaciones principales*. Las organizaciones se pueden crear con estructura plana o jerárquica. La jerarquía puede representar departamentos, áreas geográficas u otras divisiones lógicas por las que se administran las cuentas de usuario.

Para obtener más información sobre las organizaciones, consulte "Qué son las organizaciones en Identity Manager" en la página 209.

Uniones de directorios

Una *unión de directorios* es un conjunto de organizaciones relacionadas jerárquicamente que refleja el conjunto real de contenedores jerárquicos de recursos de directorio. Un *recurso de directorio* es aquél que utiliza un espacio de nombre jerárquico mediante contenedores jerárquicos. Entre los ejemplos de recursos de directorio tenemos los servidores LDAP y los recursos de Windows Active Directory.

Cada organización de una unión de directorios constituye una *organización virtual*. La organización virtual que ocupa la cima de una unión de directorios refleja el contenedor que representa el contexto base definido en el recurso. Las demás organizaciones virtuales de una unión de directorios son organizaciones secundarias *directas* o *indirectas* de la organización virtual principal y también reflejan uno de los contenedores de recurso de directorio que son secundarios respecto al contenedor del contexto base del recurso definido.

Puede afiliar los usuarios de Identity Manager a una organización virtual y ponerlos a su disposición igual que si fuera una organización física.

Para obtener más información sobre las uniones de directorios, consulte "Uniones de directorios y organizaciones virtuales" en la página 213.

Capacidades de Identity Manager

A cada usuario se le pueden asignar capacidades, o grupos de derechos, para permitirle realizar acciones administrativas en Identity Manager. Las capacidades permiten a los usuarios administrativos efectuar determinadas tareas en el sistema y actuar sobre los objetos de Identity Manager.

Las capacidades se asignan normalmente según responsabilidades de tareas específicas, como reinicialización de contraseñas o aprobación de cuentas. Al asignar capacidades y derechos a usuarios individuales, crea una estructura administrativa jerárquica que proporciona acceso y privilegios focalizados sin riesgo para la seguridad de los datos.

Identity Manager ofrece un conjunto de capacidades predeterminadas para funciones administrativas habituales. También puede crear y asignar capacidades que respondan a sus necesidades concretas.

Para obtener más información sobre las capacidades, consulte "Conceptos y administración de capacidades" en la página 216.

Roles de administrador

Los roles de administrador de Identity Manager le permiten definir un conjunto único de capacidades para cada conjunto de organizaciones gestionadas por un usuario administrativo. A un rol de administrador se le asignan capacidades y organizaciones controladas, que a su vez pueden asignarse a un usuario administrativo.

Las capacidades y organizaciones controladas pueden asignarse directamente a un rol de administrador. También se pueden asignar indirectamente (dinámicamente) cada vez que el usuario administrativo inicia una sesión en Identity Manager. Las reglas de Identity Manager controlan la asignación dinámica.

Para obtener más información sobre los roles de administrador, consulte "Conceptos y administración de roles de admin" en la página 220.

Directivas de Identity Manager

Las *directivas* establecen limitaciones para los usuarios de Identity Manager mediante la definición de restricciones sobre las características de ID de cuenta, inicio de sesión y contraseña. Las *directivas de cuentas del sistema Identity* definen opciones y restricciones de directivas de usuario, contraseña y autenticación. Las *directivas de contraseñas de recurso y de ID de cuenta* definen las reglas de longitud y de tipo de caracteres, además de las palabras permitidas y los valores de atributo. Una *directiva de diccionario* permite a Identity Auditor comparar las contraseñas con una base de datos de palabras para asegurarse de que estén protegidas frente a posibles ataques simples de diccionario.

Para obtener más información sobre las directivas, consulte "¿Qué son las directivas?" en la página 102.

Directivas de auditoría

A diferencia de otras directivas del sistema, una *directiva de auditoría* define una infracción de directiva para un grupo de usuarios de un recurso determinado. Las directivas de auditoría establecen una o varias reglas con las que se evalúa a los usuarios para detectar infracciones de cumplimiento. Estas reglas dependen de condiciones basadas en uno o varios atributos definidos por un recurso. Cuando el sistema analiza un usuario, aplica los criterios definidos en las directivas de auditoría asignadas a dicho usuario para averiguar si se han producido infracciones de cumplimiento.

Para obtener más información sobre las directivas de auditoría, consulte "Qué son las directivas de auditoría" en la página 440.

Relaciones entre objetos

En la tabla siguiente se resumen los objetos de Identity Manager y sus relaciones.

TABLA 1–1 Relaciones entre objetos de Identity Manager

Objeto de Identity Manager	¿Qué es?	¿Dónde se usa?
Cuenta de usuario	Una cuenta en Identity Manager y en uno o más recursos. Los datos de usuario se pueden cargar en Identity Manager desde los recursos. Una clase especial de usuarios, los administradores de Identity Manager, tienen privilegios extendidos.	**Rol**. En general, a cada cuenta de usuario se le asigna uno o varios roles. **Organización**. Las cuentas de usuario se estructuran jerárquicamente dentro de una organización. Los administradores de Identity Manager además gestionan las organizaciones. **Recurso**. Los distintos recursos se pueden asignar a cuentas de usuario. **Capacidad**. A los administradores se le asignan capacidades para las organizaciones que gestionan.

TABLA 1–1 Relaciones entre objetos de Identity Manager *(Continuación)*

Objeto de Identity Manager	¿Qué es?	¿Dónde se usa?
Rol	Los roles de negocio sirven para organizar en grupos los derechos de acceso que necesitan las personas que realizan tareas similares en una organización. Los roles de aplicaciones y de TI agrupan los recursos para poder asignarlos a los usuarios mediante roles de negocio. Las asignaciones de recursos basadas en roles simplifican la administración de recursos en las organizaciones grandes.	**Recursos y grupos de recursos**. Los recursos y grupos de recursos se asignan a roles de activos, aplicaciones y TI. **Cuenta de usuario**. Las cuentas de usuario con características similares se asignan a roles de negocio. **Roles de activos, de aplicaciones y de TI**, Los roles de activos, de aplicaciones y de TI se asignan a roles de negocio.
Recurso	Almacena información sobre un sistema, aplicación u otro recurso donde se administran cuentas.	**Rol**. Los recursos se asignan a aplicaciones y roles de TI, que a su vez se asignan a roles de negocio. Una cuenta de usuario hereda libremente el acceso a los recursos de sus asignaciones de roles de negocio. **Cuenta de usuario**. Los recursos se pueden asignar individualmente a cuentas de usuario.
Grupo de recursos	Grupo ordenado de recursos.	**Rol**. Los grupos de recursos se asignan a roles; una cuenta de usuario hereda libremente el acceso a los recursos de sus asignaciones de roles de negocio. **Cuenta de usuario**. Los grupos de recursos se pueden asignar directamente a cuentas de usuario.

TABLA 1–1 Relaciones entre objetos de Identity Manager *(Continuación)*

Objeto de Identity Manager	¿Qué es?	¿Dónde se usa?
Organización	Define el ámbito de las entidades que gestiona un administrador; es jerárquica.	**Recurso**. Los administradores de una organización pueden tener acceso a algunos o todos los recursos. **Administrador**. Las organizaciones están gestionadas (controladas) por los usuarios que poseen privilegios administrativos. Los administradores pueden gestionar una o varias organizaciones. Los privilegios administrativos de una organización se transmiten a sus organizaciones secundarias. **Cuenta de usuario**. Cada cuenta de usuario se puede asignar a una organización de Identity Manager y a una o varias organizaciones de directorios.
Unión de directorios	Conjunto de organizaciones relacionadas jerárquicamente que refleja el conjunto real de contenedores jerárquicos de recursos de directorio.	**Organización**. Cada organización de una unión de directorios constituye una organización virtual.
Rol de administrador (Admin)	Define un conjunto único de capacidades para cada conjunto de organizaciones asignadas a un administrador.	**Administrador**. Los roles de administrador se asignan a administradores. **Capacidades y organizaciones**. Las capacidades y organizaciones se asignan directa o indirectamente (dinámicamente) a roles de administrador.
Capacidad	Define un grupo de derechos del sistema.	**Administrador**. Las capacidades se asignan a administradores.
Directiva	Define límites de contraseña y autenticación.	**Cuenta de usuario**. Las directivas se asignan a cuentas de usuario. **Organización**. Las directivas se asignan o transmiten por herencia a las organizaciones.

TABLA 1–1 Relaciones entre objetos de Identity Manager *(Continuación)*

Objeto de Identity Manager	¿Qué es?	¿Dónde se usa?
Directiva de auditoría	Establece reglas con las que se evalúa a los usuarios para detectar infracciones de cumplimiento.	**Cuenta de usuario**. Las directivas de auditoría se asignan a cuentas de usuario. **Organización**. Las directivas de auditoría se asignan a organizaciones.

◆ ◆ ◆ CAPÍTULO 2

Introducción a la interfaz de usuario de Identity Manager

En este capítulo conocerá las interfaces gráficas de usuario (UI) de Identity Manager y cómo empezar a utilizar este producto enseguida.

Se tratan los siguientes temas:

Interfaz de administración de Identity Manager

El sistema Identity Manager tiene dos interfaces gráficas principales con las que se efectúan las tareas. Son la interfaz de usuario final y la interfaz de administración. La interfaz de usuario final (también denominada interfaz de usuario) se describe más adelante en la sección "Interfaz de usuario final de Identity Manager" en la página 40 de este capítulo. La interfaz de administración se describe a continuación.

La interfaz de administración de Identity Manager constituye la principal vista administrativa del producto. Los administradores de Identity Manager utilizan esta interfaz para administrar usuarios, configurar y asignar recursos, definir derechos y niveles de acceso, y auditar el cumplimiento en el sistema Identity Manager.

La interfaz está organizada mediante los elementos siguientes:

- **Fichas de la barra de navegación** Situadas en la parte superior de cada página de la interfaz, estas fichas sirven para recorrer las principales áreas funcionales.
- **Fichas secundarias o menús**. En función de la implementación que se esté utilizando, es posible que aparezcan fichas o menús secundarios debajo de cada ficha de la barra de navegación. Estos menús o fichas secundarias permiten acceder a tareas incluidas en cada área funcional.

En algunas áreas, como Cuentas, *los formularios con fichas* dividen los formularios extensos en una o varias páginas para facilitar su uso. Ello se ilustra en la Figura 2–1.

Nota – El Apéndice C, "Referencia rápida de la interfaz de usuario", contiene una sinopsis para efectuar tareas administrativas en la UI.

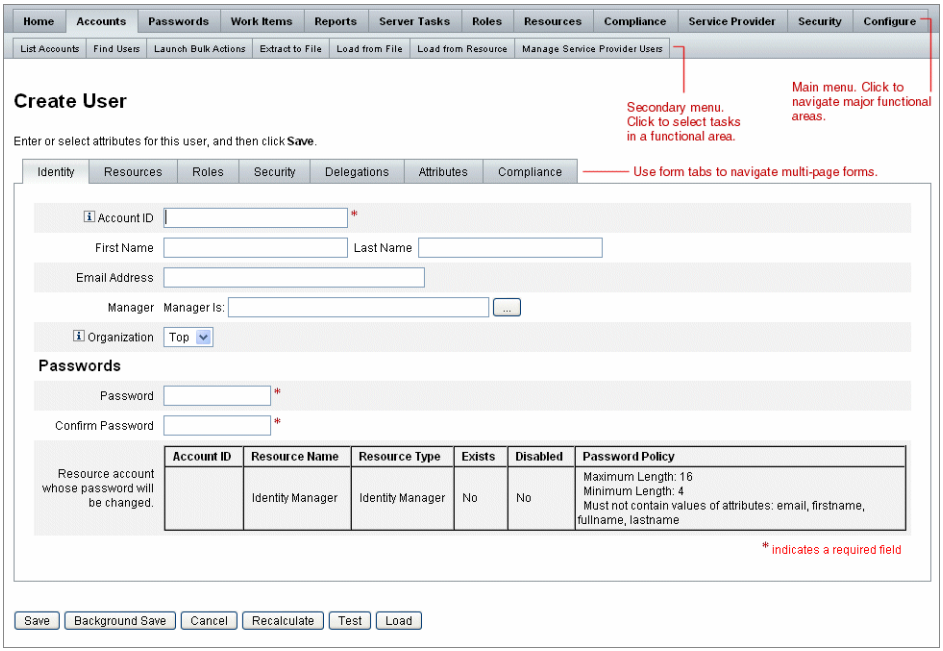


FIGURA 2–1 Interfaz de administración de Identity Manager

Inicio de sesión en la interfaz de administración de Identity Manager

▼ Para abrir la interfaz de administración

1 **Abra un navegador web y escriba la URL siguiente en la barra de dirección:**

`http://<AppServerHost>:<Port>/idm/login.jsp`

2 **Introduzca su ID de usuario y su contraseña y haga clic en Inicio de sesión.**

La interfaz de administración se abre si su ID de usuario tiene asignadas capacidades y una organización contralada.

Límites de sesión y cookies

Si están habilitadas las cookies en el navegador web del administrador, éste permanecerá conectado a la interfaz de administración durante el tiempo permitido por el límite de sesión configurado. Si las cookies están inhabilitadas en el navegador, al realizar determinadas acciones el sistema pedirá al administrador que vuelva a iniciar la sesión.

Dichas acciones incluyen:

- Cancelación del cambio de nombre de administrador, rol y organización
- Cancelación de eliminación de organización
- Creación de módulo de inicio de sesión de usuario y de módulo de inicio de sesión de administrador

Las cookies deben estar habilitadas para evitar sucesivas peticiones de reinicio de sesión.

Olvido del ID de usuario

Identity Manager permite al administrador recuperar su ID de usuario olvidado. Cuando un administrador hace clic en ¿Olvidó su ID de usuario? en la página de inicio de sesión, aparece una página de búsqueda donde se le pide información sobre los atributos de identidad asociados a la cuenta, como nombre y apellidos, dirección de correo electrónico o número de teléfono.

A continuación, Identity Manager elabora una consulta para buscar un único usuario que coincida con los valores introducidos. Si encuentra varias o ninguna coincidencia, muestra un mensaje de error en la página de búsqueda del ID de usuario.

La función de búsqueda está habilitada de manera predeterminada, pero es posible realizar una de las acciones siguientes para inhabilitarla:

- Configurar `forgotUserIdMode` en un valor falso (false) dentro de `login.jsp`.
- Editar el objeto de configuración del sistema y definir el atributo `disableForgotUserId` en un valor verdadero (true) para el atributo `admin` y/o el atributo `user`.

  Encontrará instrucciones para editar el objeto de configuración del sistema en "Edición de objetos de configuración de Identity Manager" en la página 118.

Nota – Si actualiza desde una versión anterior de Identity Manager a la versión 8.1, la función ¿Olvidó su ID de usuario? estará *inhabilitada* de manera predeterminada.

Para habilitar esta función, debe modificar los atributos siguientes en el objeto de configuración del sistema ("Edición de objetos de configuración de Identity Manager" en la página 118):

```
ui.web.user.disableForgotUserId = false
ui.web.admin.disableForgotUserId = false
```

El conjunto de nombres de atributo de usuario que aparecen se configura mediante los atributos de configuración del sistema `security.authn.lookupUserIdAttributes.<Interfaz de administración | Interfaz de usuario>`. Se pueden especificar los atributos que están definidos como consultables en el objeto de configuración `IDM Schema Configuration`.

Si se recupera el ID de usuario, Identity Manager lo notifica a la dirección de correo electrónico del usuario recuperado mediante la plantilla de correo Recuperar ID de usuario.

Interfaz de usuario final de Identity Manager

La interfaz de usuario final de Identity Manager (también llamada "interfaz de usuario de Identity Manager") presenta una vista limitada del sistema Identity Manager. Se trata de una vista adaptada específicamente a los usuarios que carecen de capacidades administrativas.

Nota – En "Inicio de sesión en la interfaz de usuario final de Identity Manager" en la página 43 se explica cómo iniciar la sesión en la interfaz de usuario final.

En la interfaz de usuario se pueden realizar diversas actividades, como cambiar la contraseña, efectuar tareas de autoabastecimiento, o administrar elementos de trabajo y delegaciones.

Identity Manager se puede configurar para que los usuarios puedan solicitar una cuenta haciendo clic en un vínculo dentro de la página de inicio de sesión de la interfaz de usuario final. Encontrará más información en "Registro anónimo" en la página 96.

Las cinco fichas de la interfaz de usuario final

La interfaz de usuario final está organizada en cinco secciones:

Ficha Página de inicio

Cuando un usuario inicia la sesión en la interfaz de usuario de Identity Manager, todos los elementos de trabajo pendientes y delegaciones del usuario aparecen en la ficha Página de inicio, como ilustra la figura siguiente.

FIGURA 2–2 Interfaz de usuario (ficha Página de inicio)

La ficha Página de inicio ofrece acceso rápido a todos los elementos pendientes. Los usuarios pueden hacer clic en un elemento de la lista para responder a una solicitud de elemento de trabajo o realizar otras acciones disponibles.

Ficha Elementos de trabajo

La ficha Elementos de trabajo se divide a su vez en las fichas Aprobaciones, Autenticaciones, Remediaciones y Otros. En esta área de la interfaz de usuario, los usuarios pueden aprobar o rechazar cualquier elemento de trabajo que les pertenezca o sobre el que tengan autorización.

Ficha Solicitudes

La ficha Solicitudes consta de dos fichas secundarias: Iniciar solicitudes y Ver.

La ficha Iniciar solicitudes ofrece dos opciones a los usuarios: Actualizar mis roles y Actualizar mis recursos.

- La página Actualizar mis roles permite a los usuarios solicitar en una lista los roles disponibles que pueden interesarles. Cuando el usuario final envía una solicitud de rol, se genera un elemento de trabajo y se envía una notificación de aprobación a los aprobadores designados para dicho rol. Los usuarios finales también pueden solicitar que se les suprima o *anule la asignación* de uno o más roles.

  En el Capítulo 5, "Roles y recursos", encontrará información para crear roles opcionales cuyo acceso pueden solicitar los usuarios finales.
- La página Actualizar mis recursos permite a los usuarios solicitar en una lista los recursos individuales que pueden interesarles. Al igual que las solicitudes de roles, las solicitudes de recursos generan elementos de trabajo que requieren aprobación para poder procesarse.

La ficha secundaria Ver muestra detalles del estado de las solicitudes enviadas por el usuario. En este área los usuarios pueden ver el estado del proceso y los resultados de las tareas para las solicitudes que envían.

Ficha Delegaciones

En la ficha Delegaciones, los usuarios pueden delegar elementos de trabajo a otros usuarios de Identity Manager. Por ejemplo, un usuario asignado como aprobador de uno o más roles puede establecer que los futuros elementos de trabajo de aprobación se envíen a un compañero mientras él está de vacaciones. En la página Delegaciones, los usuarios pueden crear y administrar delegaciones sin ayuda del administrador.

Ficha Perfil

En la ficha Perfil, los usuarios finales pueden administrar sus valores de configuración de contraseñas y cuentas de Identity Manager. Esta ficha se divide en cuatro fichas secundarias:

- **Cambiar contraseña**. Los usuarios finales pueden cambiar sus contraseñas en un recurso específico o en todos.
- **Atributos de cuenta**. Los usuarios finales pueden cambiar determinados atributos, como la dirección de correo electrónico a la que Identity Manager envía las notificaciones de las cuentas.
- **Preguntas de autenticación**. Sirve para administrar las preguntas y respuestas de autenticación de la cuenta del usuario.
- **Privilegios de acceso**. Muestra las asignaciones actuales de roles y recursos del usuario.

Inicio de sesión en la interfaz de usuario final de Identity Manager

Para iniciar la sesión en la interfaz de usuario final de Identity Manager, siga las instrucciones indicadas a continuación.

▼ Para abrir la interfaz de usuario final

1 **Abra un navegador web y escriba la URL siguiente en la barra de dirección:**

`http://<AppServerHost>:<Port>/idm/user/login.jsp`

2 **Introduzca un ID de usuario y una contraseña y haga clic en Inicio de sesión.**

Aparece la interfaz de usuario final.

Recuperación de ID de usuario olvidados

Identity Manager permite a los usuarios finales recuperar sus ID de usuario olvidados. Para obtener más información, consulte "Olvido del ID de usuario" en la página 39 dentro de la sección "Inicio de sesión en la interfaz de administración de Identity Manager" en la página 39.

Ayuda y Guía

Para realizar algunas tareas correctamente, quizá necesite consultar la Ayuda y la *Guía* (información e instrucciones del nivel de campos) de Identity Manager. La Ayuda y la Guía están disponibles en las interfaces de administración y de usuario final de Identity Manager.

Ayuda de Identity Manager

Para obtener ayuda e información sobre las tareas, haga clic en el botón Ayuda, que se encuentra en la parte superior de cada página de las interfaces de administración y de usuario final, como ilustra la figura siguiente.

FIGURA 2–3 Botón Ayuda en la interfaz de Identity Manager

En la parte inferior de cada ventana de Ayuda hay un vínculo Contenido, con el que se accede a otros temas de Ayuda y al glosario de terminología de Identity Manager.

Guía de Identity Manager

La Guía de Identity Manager es una breve ayuda focalizada que aparece junto a muchos campos. Sirve para introducir información o efectuar selecciones conforme se avanza por una página para realizar una tarea.

Junto a los campos que disponen de guía aparece un símbolo marcado con la letra “i”. Haga clic en dicho símbolo para abrir una ventana y ver la información correspondiente.

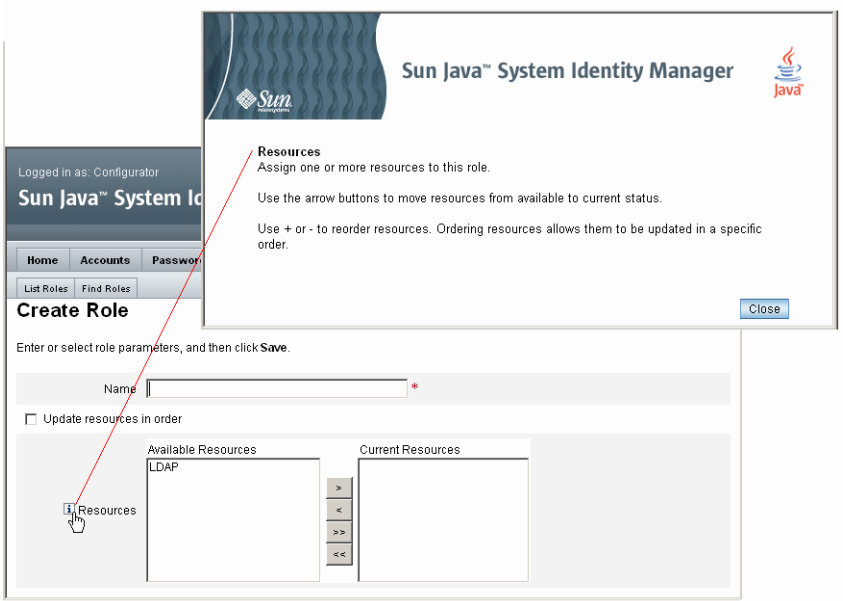


FIGURA 2–4 Guía de Identity Manager

Página de depuración de Identity Manager

La interfaz de administración incluye prácticas páginas para optimizar Identity Manager o solucionar problemas. Para acceder a estas páginas, abra la página de depuración de Identity Manager, también denominada página de configuración del sistema.

Para abrir la página de depuración de Identity Manager, escriba la URL siguiente en el navegador. (En las URL se puede diferenciar mayúsculas de minúsculas según la plataforma y la configuración.)

`http://<AppServerHost>:<Port>/idm/debug/session.jsp`

Para ver las páginas `/idm/debug/` se necesita capacidad de depuración. Para obtener información sobre las capacidades, consulte "Asignación de capacidades a usuarios" en la página 219.

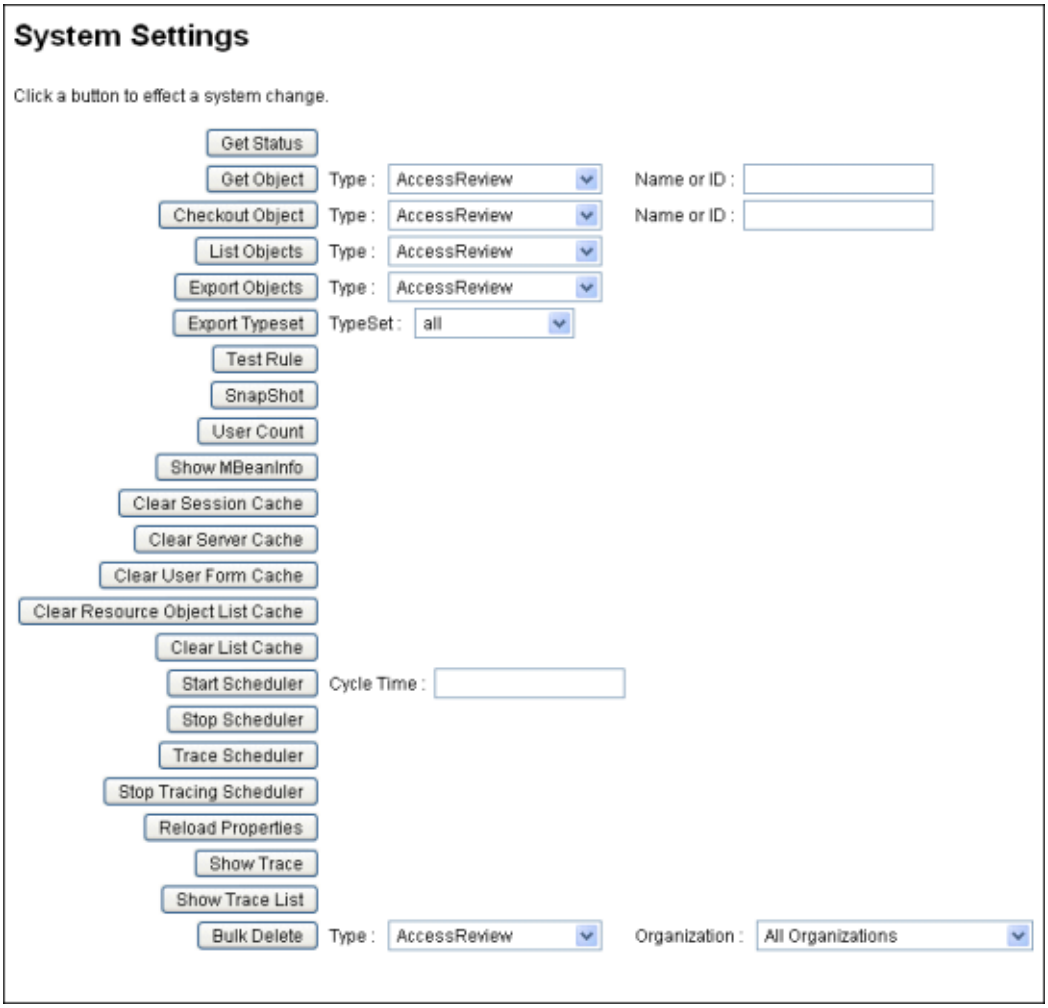


FIGURA 2–5 Página de depuración (configuración del sistema) de Identity Manager

Encontrará información sobre la solución de problemas en Identity Manager dentro del Capítulo 5, "Tracing and Troubleshooting" de *Sun Identity Manager 8.1 System Administrator's Guide*.

Identity Manager IDE

Sun Identity Manager Integrated Development Environment (Identity Manager IDE) ofrece una vista gráfica de los formularios, reglas y flujos de trabajo de Identity Manager. Es un complemento NetBeans totalmente integrado que se incluye en el paquete de distribución de Identity Manager.

Con Identity Manager IDE se crean y editan formularios que establecen las características disponibles en cada página de Identity Manager. También es posible modificar los *flujos de trabajo* de Identity Manager, que determinan la secuencia de las acciones o tareas realizadas al trabajar con cuentas de usuario de Identity Manager. Se pueden modificar además las reglas definidas en Identity Manager que condicionan los comportamientos de flujo de trabajo.

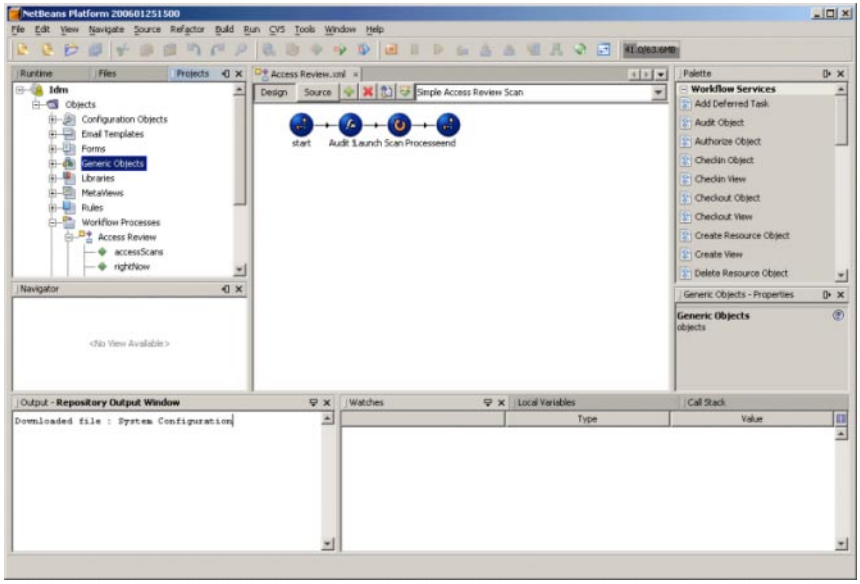


FIGURA 2–6 Interfaz de Identity Manager IDE

Para descargar Identity Manager IDE, visite este sitio web:

`https://identitymanageride.dev.java.net/`

También puede utilizar el (BPE) para realizar personalizaciones si lo tiene instalado con versiones anteriores de Identity Manager.

Dónde continuar

Una vez que se familiarice con las interfaces de Identity Manager y los medios para encontrar información, utilice la referencia siguiente para consultar los temas que le interesen:

Capítulo, Tema	Descripción
Capítulo 3, "Administración de usuarios y de cuentas"	Se describen el área Cuentas de la interfaz y procedimientos para administrar las cuentas de usuario.
Capítulo 5, "Roles y recursos"	Se explica cómo trabajar con roles y recursos en Identity Manager.
Capítulo 4, "Configuración de objetos de administración de negocio"	Se explican las tareas de configuración y cómo configurar los objetos de Identity Manager.
Capítulo 6, "Administración"	Se explica cómo crear y gestionar administradores y organizaciones en Identity Manager.
Capítulo 7, "Carga y sincronización de datos"	Le guía por las funciones y herramientas que puede usar para mantener los datos actuales en Identity Manager.
Capítulo 8, "Informes"	Se describen los informes y cómo se generan.
Capítulo 9, "Plantillas de tarea"	Se tratan las plantillas de tareas que sirven para configurar algunos comportamientos de flujo de trabajo.
Capítulo 10, "Registro de auditoría"	Se explican los registros de auditoría y el funcionamiento del sistema de auditoría.
Capítulo 11, "PasswordSync"	Se explica cómo configurar la utilidad PasswordSync para sincronizar los cambios de contraseñas en los dominios de Windows Active Directory con los cambios en Identity Manager.
Capítulo 12, "Seguridad"	Se describen las funciones de seguridad y su utilización.
Capítulo 13, "Auditoría de identidades: Conceptos básicos"	Se explican los conceptos básicos de la auditoría de identidades.
Capítulo 14, "Auditoría: Directivas de auditoría"	Se explica la creación de directivas de auditoría.
Capítulo 15, "Auditoría: Cumplimiento de supervisión"	Se explica cómo realizar revisiones de auditoría e implementar prácticas que ayudan a gestionar el cumplimiento de las normativas vigentes.
Capítulo 16, "Exportador de datos"	El Exportador de datos le permite escribir información sobre usuarios, roles y otros tipos de objetos en un almacén de datos externo.
Capítulo 17, "Administración de Service Provider"	Describe las funciones que sirven para administrar usuarios de proveedores de servicios.

Capítulo, Tema	Descripción
Apéndice A, “Referencia de `lh`”	Describe los comandos disponibles en la línea de comandos de Identity Manager.
Apéndice B, “Esquema de base de datos de registros de auditoría”	Información sobre los valores de esquema de datos de auditoría para los tipos de base de datos compatibles y las asignaciones de base de datos de registro de auditoría.
Apéndice C, “Referencia rápida de la interfaz de usuario”	Una referencia rápida para efectuar tareas administrativas en la UI. Muestra la ubicación principal donde debe situarse para comenzar cada tarea, junto con ubicaciones alternativas o métodos (en su caso) que puede usar para realizar la misma tarea.
Apéndice D, “Definiciones de capacidades”	Una lista de las capacidades funcionales (con definiciones) y basadas en tareas predeterminadas de Identity Manager. En este apéndice también se indican las fichas y fichas secundarias accesibles con cada capacidad basada en tareas.

◆ ◆ ◆ CAPÍTULO 3

Administración de usuarios y de cuentas

Este capítulo contiene información y procedimientos para crear y administrar usuarios mediante la interfaz de administración de Identity Manager.

Esta información se ha dividido como sigue:

El área Cuentas de la interfaz

Un usuario es cualquiera que detente una cuenta del sistema Identity Manager. Identity Manager almacena diversos datos para cada usuario. En conjunto, esta información constituye una identidad de Identity Manager de un usuario.

En la página Cuentas / Lista de usuarios de Identity Manager puede administrar usuarios de Identity Manager. Para acceder a esta área, haga clic en **Cuentas** dentro de la barra de menús de la interfaz de administración.

La lista de cuentas muestra todas las cuentas de usuario de Identity Manager. Las cuentas se agrupan en organizaciones y organizaciones virtuales, representadas jerárquicamente en carpetas.

Puede ordenar la lista de cuentas por el nombre completo, los apellidos o el nombre del usuario. Haga clic en la barra de encabezado para ordenar por columna. Al hacer clic en la misma barra de encabezado, el orden cambia entre ascendente y descendente. al ordenar por nombre completo (columna Nombre), todos los elementos de la jerarquía, en todos los niveles, se ordenan alfabéticamente.

Para expandir la vista jerárquica y ver todas las cuentas de una organización, haga clic en el indicador triangular existente junto a la carpeta. Haga clic de nuevo en el indicador para contraer la vista.

Listas de acciones en el área Cuentas

Las listas de acciones situadas en la parte superior e inferior del área de cuentas (ilustradas en "Listas de acciones en el área Cuentas" en la página 52) sirven para realizar diversas acciones.

Las listas de acciones están estructuradas así:

- **Nuevas acciones**. Para crear usuarios, organizaciones y uniones de directorios.
- **Acciones de usuario**. Para editar, ver y cambiar el estado de los usuarios; cambiar y reinicializar contraseñas; eliminar, habilitar, inhabilitar, desbloquear, mover, actualizar y renombrar usuarios; y ejecutar informes de auditoría de usuarios.
- **Acciones de organización**. Para efectuar diversas acciones de organización y de usuario.

Búsqueda en las listas del área Cuentas

Utilice la función de búsqueda del área de cuentas para encontrar usuarios y organizaciones. Basta con seleccionar Organizaciones o Usuarios en la lista, introducir uno o varios caracteres iniciales del nombre de la organización o el usuario en el área de búsqueda y después hacer clic en **Buscar**. Para obtener más información sobre las búsquedas en el área de cuentas, consulte "Búsqueda y visualización de cuentas de usuario" en la página 62.

Estado de cuenta de usuario

Los iconos que aparecen junto a cada cuenta de usuario indican el estado actual asignado a la cuenta. En la Tabla 3–1 se explica el significado de cada icono.

TABLA 3–1 Descripciones de los iconos de estado de cuenta de usuario

Indicador	Estado
	La cuenta de Identity Manager del usuario está bloqueada. Recuerde que este icono sólo refleja el estado bloqueado de la cuenta de Identity Manager, no de ninguna de las cuentas de recursos del usuario. Los usuarios quedan bloqueados cuando superan el máximo número de intentos fallidos de inicio de sesión con la cuenta de Identity Manager según se especifica en la directiva de cuenta de Identity Manager. Para este número máximo sólo se cuentan los inicios de sesión con contraseña o pregunta en cuentas de Identity Manager que han fallado. Por tanto, si una aplicación de inicio de sesión en Identity Manager (o sea, la interfaz de administración, la interfaz de usuario final, etc.) no incluye el módulo de inicio de sesión de Identity Manager en su grupo de módulos de inicio de sesión, no se aplicará la directiva de fallo de contraseña de Identity Manager. No obstante, con independencia de los módulos de inicio de sesión que haya configurados para una determinada aplicación de inicio de sesión en Identity Manager, los inicios de sesión con pregunta fallidos que superen el máximo configurado en la directiva de cuenta de Identity Manager pueden provocar el bloqueo de un usuario y la aparición de este icono. Encontrará información para desbloquear las cuentas de usuario en "Desbloqueo de cuentas de usuario" en la página 78.
	La cuenta de Identity Manager del administrador está bloqueada. Recuerde que este icono sólo refleja el estado bloqueado de la cuenta de Identity Manager, no de ninguna de las cuentas de recursos del administrador. Para obtener más información, consulte la descripción anterior correspondiente al icono de bloqueo de usuario.
	La cuenta está inhabilitada en todos los recursos asignados y en Identity Manager. (Cuando la cuenta está habilitada, no aparece ningún icono.). Encontrará información para habilitar las cuentas de usuario inhabilitadas en "Inhabilitación, habilitación y desbloqueo de cuentas de usuario" en la página 76.
	La cuenta está parcialmente inhabilitada, lo que significa que está inhabilitada en uno o más recursos asignados.
	El sistema ha intentado crear o actualizar la cuenta de usuario de Identity Manager en uno o varios recursos, pero no ha podido. (Cuando se actualiza una cuenta en todos los recursos asignados, no aparece ningún icono.).

Nota – En la columna Administrador aparece entre paréntesis un nombre de usuario de administrador si Identity Manager no encuentra una cuenta de Identity Manager que coincida con el nombre mostrado.

Páginas de usuario (Crear/Editar/Ver)

En esta sección se describen las páginas Crear usuario, Editar usuario y Ver usuario que están disponibles en la interfaz de administración. Más adelante en este capítulo se incluyen instrucciones para utilizar estas páginas.

Nota – En esta documentación se describe el conjunto predeterminado de las páginas Crear usuario, Editar usuario y Ver usuario que se incluye con Identity Manager. Para plasmar mejor sus procesos de negocio o capacidades de administración concretas, le conviene crear formularios de usuario personalizados específicos para su entorno. Para obtener más información sobre la personalización de formularios de usuario, consulte el Capítulo 2, "Identity Manager Forms" de *Sun Identity Manager Deployment Reference*.

Las páginas de usuario predeterminadas de Identity Manager están organizadas en las siguientes fichas o secciones:

- Identidad
- Asignaciones
- Seguridad
- Delegaciones
- Atributos
- Cumplimiento

Ficha Identidad

En el área Identidad se define el ID de cuenta de un usuario, su nombre, información de contacto, administrador, la organización pertinente y la contraseña de cuenta de Identity Manager. También identifica los recursos a que tiene acceso el usuario y la directiva de contraseñas que rige cada cuenta de recursos.

Nota – Encontrará información sobre la configuración de directivas de contraseñas de cuenta en la sección "Administración de la seguridad de las cuentas y los privilegios" en la página 87 de este capítulo.

En la figura siguiente se ilustra el área Identidad de la página Crear usuario.

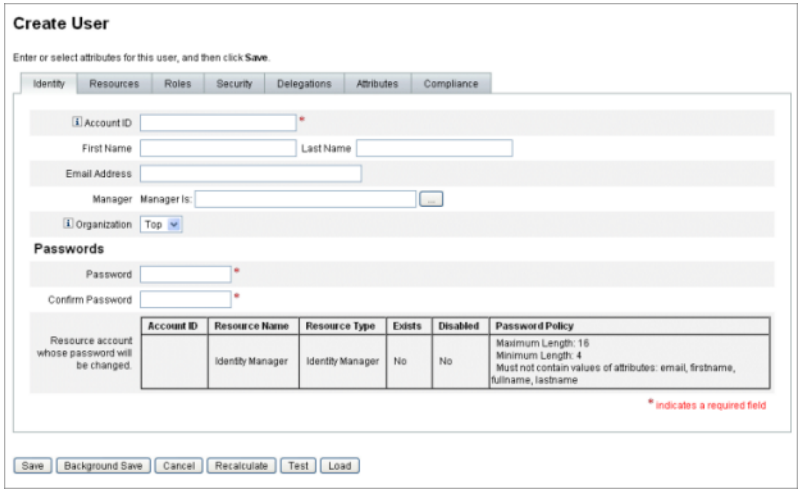


FIGURA 3–1 Crear usuario - Identidad

Ficha Recursos

El área Recursos permite la asignación directa de recursos y grupos de recursos a un usuario. También se pueden asignar exclusiones de recursos.

Los recursos asignados directamente complementan a los asignados indirectamente al usuario mediante la *asignación de roles*. La asignación de roles caracteriza a una clase de usuarios. Los roles determinan el acceso de los usuarios a los recursos mediante la asignación indirecta.

Ficha Roles

La ficha Roles sirve para asignar uno o más roles a un usuario y para gestionar dichas asignaciones.

Encontrará información sobre esta ficha dentro de "Para asignar roles a un usuario" en la página 146.

Ficha Seguridad

En la terminología de Identity Manager, un usuario que tiene asignadas capacidades extendidas es un *administrador* de Identity Manager. La ficha Seguridad sirve para asignar privilegios de administrador a un usuario.

Encontrará más información sobre el uso de la ficha Seguridad para crear administradores en "Creación y gestión de administradores" en la página 203.

La ficha **Seguridad** consta de las secciones siguientes:

- **Roles de administrador (Admin)**. Asigna uno o más roles administrativos al usuario. Un rol es una combinación específica de capacidades y organizaciones controladas que facilita la asignación de tareas administrativas a los usuarios de una manera coordinada.
- **Capacidades**. Habilita derechos en el sistema Identity Manager. A cada administrador de Identity Manager se le asignan una o más capacidades, normalmente asociadas a responsabilidades de tareas.

  Las capacidades se explican en "Conceptos y administración de capacidades" en la página 216. El Apéndice D, "Definiciones de capacidades",Apéndice D, "Definiciones de capacidades" contiene una lista de capacidades basadas en tareas junto con sus definiciones. En este apéndice también se indican las fichas y fichas secundarias accesibles con cada capacidad.
- **Organizaciones controladas**. Asigna organizaciones que este usuario tiene derecho a gestionar como administrador. El administrador puede administrar objetos en la organización asignada y en cualquier organización que pertenezca a ella en la jerarquía.

Nota – Para tener capacidades de administrador, el usuario debe tener asignado al menos un rol de administrador, o una o varias capacidades Y ADEMÁS una o varias organizaciones controladas. Para obtener más información sobre los administradores en Identity Manager, consulte "Conceptos de administración de Identity Manager " en la página 201.

- **Formulario de usuario**. Especifica el formulario de usuario que el administrador debe utilizar al crear y editar usuarios. Si se selecciona **Ninguno**, el administrador heredará el formulario de usuario asignado a su organización.
- **Formulario de vista de usuarios**. Especifica el formulario de usuario que el administrador debe utilizar al ver usuarios. Si se selecciona **Ninguno**, el administrador heredará el formulario de vista de usuarios asignado a su organización.
- **Directiva de cuenta**. Define límites de contraseña y autenticación.

Ficha Delegaciones

La ficha Delegaciones de la página Crear usuario sirve para delegar elementos de trabajo a otros usuarios durante un periodo de tiempo específico. Para obtener más información sobre la delegación de elementos de trabajo, consulte "Delegación de elementos de trabajo" en la página 234.

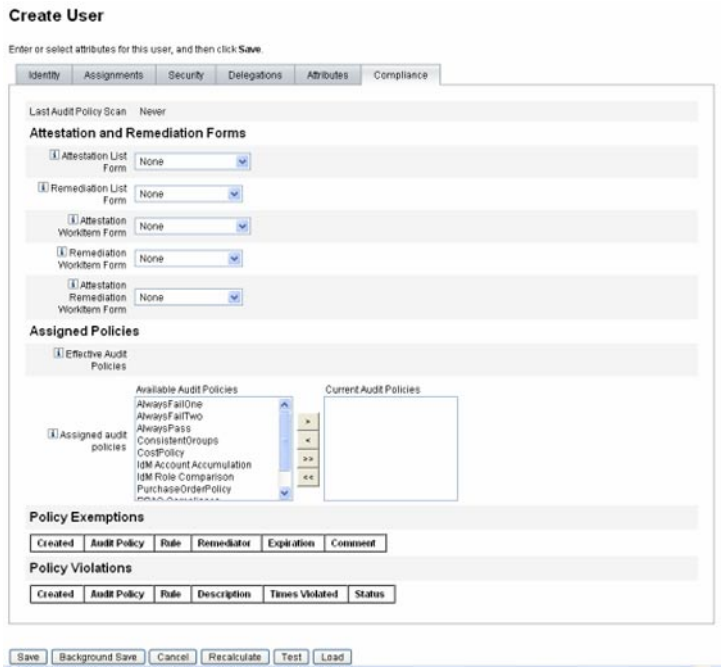
Ficha Atributos

En la ficha Atributos de la página Crear usuario se definen los atributos de cuenta asociados a los recursos asignados. Los atributos aparecen clasificados por recurso asignado y varían según los recursos que estén asignados.

Ficha Cumplimiento

En la ficha Cumplimiento:

- Se eligen los formularios de autenticación y remediación para una cuenta de usuario.
- Se especifican las directivas de auditoría asignadas a la cuenta de usuario, incluidas las que se aplican al asignar la organización del usuario. Estas asignaciones de directivas sólo se pueden cambiar editando la organización actual del usuario o trasladando éste a otra organización.
- Se indica el estado actual de los análisis, las infracciones y las exenciones de directivas (como ilustra la figura siguiente), si es aplicable a la cuenta de usuario. La información incluye la fecha y hora del último análisis de directivas de auditoría para el usuario seleccionado.



Para asignar directivas de auditoría, traslade las directivas seleccionadas desde la lista **Directivas de auditoría disponibles** a la lista **Directivas de auditoría actuales**.

Nota – Si desea ver las infracciones de cumplimiento registradas para un usuario durante un periodo de tiempo concreto, seleccione **Ver registro de infracciones de cumplimiento** en la lista **Acciones de usuario** y especifique el rango de entradas que quiere ver.

Creación de usuarios y trabajo con cuentas de usuario

En la página Cuentas/Lista de usuarios de la interfaz de administración se pueden efectuar diversas acciones con los siguientes objetos del sistema:

- **Administradores y usuarios**. Ver, crear, editar, mover, renombrar, desabastecer, habilitar, inhabilitar, actualizar, desbloquear, eliminar, anular asignación, desvincular y auditar.

  Para obtener más información sobre la creación y edición de cuentas de administrador, consulte "Conceptos de administración de Identity Manager " en la página 201.
- **Organizaciones**. Crear, editar, actualizar y realizar acciones de usuario con afiliados a una organización.

  Para obtener más información sobre las organizaciones, consulte "Qué son las organizaciones en Identity Manager" en la página 209.
- **Uniones de directorios**. Crear un conjunto de organizaciones relacionadas jerárquicamente para reflejar un conjunto real de contenedores jerárquicos de recursos de directorio.

  Para obtener más información sobre las uniones de directorios, consulte "Uniones de directorios y organizaciones virtuales" en la página 213.

Habilitación de diagramas de proceso

Los diagramas de proceso representan el flujo de trabajo que sigue Identity Manager al crear o actuar de cualquier otra forma en una cuenta de usuario. Cuando están habilitados, los diagramas de proceso aparecen en la página de resultados o de resumen de tareas que se crea una vez que Identity Manager completa la tarea.

En Identity Manager versión 8.0, los diagramas de proceso se inhabilitaron tanto para las instalaciones nuevas como de actualización.

▼ Para habilitar el uso de diagramas de proceso en Identity Manager

1. **Abra el objeto de configuración del sistema para editarlo mediante el procedimiento que se explica en "Edición de objetos de configuración de Identity Manager" en la página 118.**

2. **Busque el siguiente elemento XML:**

```
<Attribute name='disableProcessDiagrams'>
  <Boolean>true</Boolean>
</Attribute>
```

3. **Cambie el valor `true` a `false`.**

4. **Pulse Guardar.**

5 **Reinicie el servidor o servidores para que el cambio surta efecto.**

Los diagramas de proceso también pueden habilitarse en la interfaz de usuario final, pero sólo si antes se han habilitado en la interfaz de administración siguiendo los pasos antes descritos. Encontrará más información en el apartado "Para habilitar los diagramas de proceso en la interfaz de usuario final" en la página 114.

▼ Para crear un usuario en Identity Manager

Puede crear y administrar usuarios en la ficha Cuentas de la barra de menús de la interfaz de administración.

1 **En la interfaz de administración, seleccione Cuentas.**

2 **Para crear un usuario en una organización determinada, seleccione la organización y después elija Nuevo usuario en la lista Nuevas acciones.**

Para crear una cuenta de usuario en la organización principal, elija Nuevo usuario en la lista Nuevas acciones.

3 **Rellene la información de las fichas o secciones siguientes.**

- **Identidad 36**. Nombre, organización, contraseña y otros detalles. (Consulte "Ficha Identidad" en la página 54.)
- **Recursos**. Asignaciones de recursos individuales y de grupos de recursos, así como exclusiones de recursos. (Consulte "Ficha Recursos" en la página 55.)
- **Roles**. Asignaciones de roles. Para obtener más información sobre los roles, consulte "Conceptos y administración de roles" en la página 121. Encontrará instrucciones para rellenar la ficha Roles dentro de "Para asignar roles a un usuario" en la página 146.
- **Seguridad**. Roles de administrador, organizaciones controladas y capacidades. También, valores de configuración de formularios de usuario y directiva de cuentas. (Consulte "Ficha Seguridad" en la página 55.)
- **Delegaciones 110**. Delegaciones de elementos de trabajo. (Consulte "Ficha Delegaciones" en la página 56.)
- **Atributos**. Atributos específicos para los recursos asignados. (Consulte "Ficha Atributos" en la página 56.)
- **Cumplimiento**. Seleccione los formularios de autenticación y remediación para la cuenta de usuario. El área de cumplimiento también sirve para especificar las directivas de auditoría asignadas a la cuenta de usuario, incluidas las que se aplican al asignar la organización del usuario. Muestra el estado actual de los análisis, las infracciones y las exenciones de directivas, e incluye información sobre el último análisis de directivas de auditoría del usuario. (Consulte "Ficha Atributos" en la página 56.)

Tenga en cuenta que las opciones disponibles en un área pueden depender de las selecciones efectuadas en otra.

Para plasmar mejor sus procesos de negocio o capacidades de administración concretas, le conviene personalizar el formulario de usuario específicamente para su entorno. Para obtener más información sobre la personalización de formularios de usuario, consulte "Customizing Forms" de *Sun Identity Manager Deployment Reference*.

4 Cuando termine, guarde la cuenta.

Hay dos opciones para guardar una cuenta de usuario:

- **Guardar**. Guarda la cuenta de usuario. Si asigna muchos recursos a la cuenta, este proceso puede alargarse.
- **Guardar en segundo plano**. Este proceso guarda una cuenta de usuario mediante una tarea en segundo plano, lo que le permite seguir trabajando en Identity Manager. Para cada proceso de guardar que se está realizando, aparece un indicador de estado de la tarea en las páginas Cuentas, Buscar usuario, Resultados e Inicio.

  En la tabla siguiente se describen los indicadores de estado, que le ayudan a supervisar el progreso del proceso de guardar.

Indicador de estado	Estado
	El proceso de guardar se está realizando.
	El proceso de guardar está suspendido. A menudo, esto significa que el proceso está esperando su aprobación.
	El proceso se ha completado satisfactoriamente. Esto no significa que el usuario se haya guardado con éxito, sino que el proceso se ha completado sin errores.
	El proceso aún no ha comenzado.
	El proceso se ha completado con uno o varios errores.

Si coloca el ratón sobre el icono de usuario que aparece en el indicador de estado, verá información sobre el proceso de guardar en segundo plano.

Nota – Si se ha configurado la creación, al crear un usuario se creará un elemento de trabajo que puede verse en la ficha Aprobaciones. Al aprobar dicho elemento se anulará la fecha de creación y se creará la cuenta. Si se rechaza el elemento, se cancelará la creación de la cuenta. Para obtener más información sobre la configuración de la creación, consulte "Configuración de la ficha Creación y eliminación" en la página 331.

Creación de varias cuentas de recursos para un usuario

Identity Manager permite asignar varias cuentas de recursos a un mismo usuario. Para ello, ofrece la posibilidad de definir varios tipos de cuentas de recursos o *tipos de cuentas* para cada recurso. Deben crearse los tipos de cuentas de recursos necesarios en consonancia con cada tipo de cuenta funcional del recurso. Por ejemplo, superusuario de AIX o administrador de negocio de AIX.

¿Por qué asignar varias cuentas por usuario y recurso?

A veces, un usuario de Identity Manager puede necesitar más de una cuenta en un recurso. Un usuario puede tener diversas funciones de trabajo relacionadas con el recurso. Por ejemplo, puede ser a la vez usuario y administrador del recurso. La experiencia aconseja utilizar cuentas distintas para cada función. De esta manera, si una cuenta entraña riesgo, aún sigue siendo seguro el acceso a las otras cuentas.

Configuración de tipos de cuentas

Para que un recurso admita varias cuentas para un mismo usuario, primero hay que definir los tipos de cuentas de recursos en Identity Manager. Use el Asistente de recursos para definir tipos de cuentas de recursos para un recurso. Encontrará información al respecto en "Administración de la lista de recursos" en la página 161.

Debe habilitar y configurar los tipos de cuentas de recursos antes de asignarlos a los usuarios.

Asignación de tipos de cuentas

Una vez definidos los tipos de cuentas, es posible asignarlos a un recurso. Identity Manager trata cada asignación de un tipo de cuenta como una cuenta distinta. En consecuencia, cada asignación concreta en un rol puede tener un conjunto de atributos diferente.

Como en el caso de una sola cuenta por recurso, todas las asignaciones de un tipo específico generan una única cuenta, con independencia del número de asignaciones.

Aunque es posible asignar usuarios a un número indeterminado de tipos distintos de cuentas en un recurso, a cada usuario se le puede asignar una sola cuenta de un tipo específico en un recurso. La excepción a esta regla es el tipo predefinido predeterminado. Los usuarios pueden tener cualquier número de cuentas del tipo predeterminado en un recurso. Sin embargo, ello no es recomendable, porque causa ambigüedad al referenciar las cuentas en los formularios y las revisiones.

Búsqueda y visualización de cuentas de usuario

Con la función de búsqueda de Identity Manager puede buscar cuentas de usuario. Una vez que ha introducido y seleccionado los parámetros de búsqueda, Identity Manager busca todas las cuentas que coincidan con sus criterios de selección.

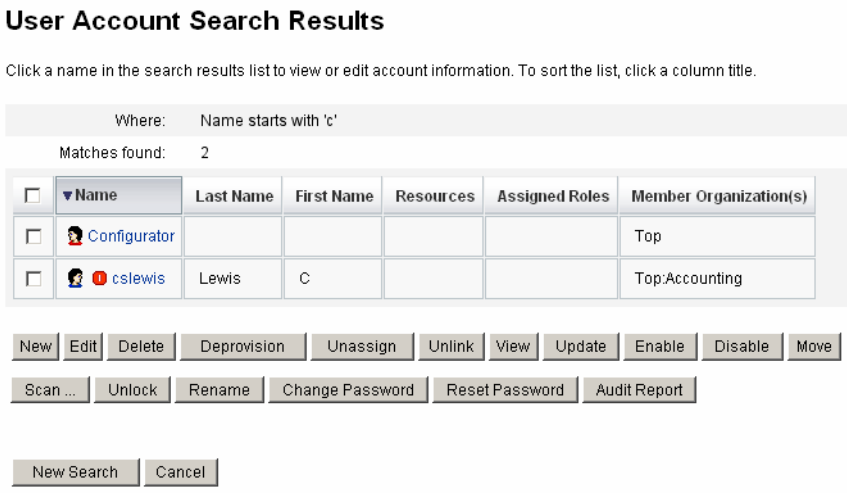
Para buscar cuentas, elija Cuentas → Buscar usuarios en la barar de menús. Puede buscar cuentas con uno o varios de estos tipos de búsqueda:

- **Información de cuenta** (como nombre de usuario, dirección de correo electrónico, nombre o apellidos). Estas opciones dependen de la implementación específica de Identity Manager en su empresa.
- **Administrador del usuario**. El nombre de usuario del administrador aparece entre paréntesis si no coincide con una cuenta existente en Identity Manager.
- **Estado de cuenta de recursos**. Las opciones incluyen:
  - **Inhabilitado**. El usuario no puede acceder a ninguna cuenta de recursos asignada o de Identity Manager.
  - **Parcialmente inhabilitado**. El usuario no puede acceder a una o más cuentas de recursos asignadas.
  - **Habilitado**. El usuario tiene acceso a todas las cuentas de recursos asignadas.
- **Recurso asignado**. Las opciones incluyen:
  - **Rol** (consulte "Para buscar usuarios asignados a un rol específico" en la página 153)
  - **Organización**
  - **Control organizativo**
  - **Capacidades**
  - **Rol de administrador**
- **Estado de cuenta de usuario**. Las opciones incluyen:
  - **Bloqueado**. La cuenta de usuario está bloqueada porque se ha superado el máximo número permitido de intentos fallidos de iniciar de sesión con contraseña o pregunta.
  - **No bloqueado**. El acceso a la cuenta de usuario no está restringido.
- **Estado de actualización**. Las opciones incluyen:
  - **no**. Cuentas de usuario que se no han actualizado en ningún recurso.
  - **alguno**. Cuentas de usuario que se han actualizado al menos en un recurso asignado, pero no en todos.
  - **todos**. Cuentas de usuario que se han actualizado en todos los recursos asignados.

La lista de resultados de la búsqueda muestra todas las cuentas que coinciden con los criterios de búsqueda.

En la página de resultados puede:

- Seleccionar cuentas de usuario para editarlas. Para editar una cuenta, haga clic en la lista de resultados de la búsqueda o selecciónela en la lista y después elija Editar.
- Realizar acciones con una o más cuentas (como habilitar, inhabilitar, desbloquear, eliminar, actualizar o cambiar/reinicializar contraseñas). Para efectuar una acción, seleccione una o varias cuentas en la lista de resultados de la búsqueda y después haga clic en la acción adecuada.
- Crear cuentas de usuario.



Edición de usuarios

En esta sección se explica cómo ver, editar, reasignar y cambiar de nombre las cuentas de usuario.

▼ Para ver cuentas de usuario

Utilice la página Ver usuario y proceda como sigue para ver información de cuentas.

1 **En la interfaz de administración, seleccione Cuentas en el menú.**

Aparece la página Lista de usuarios.

2 **Marque la casilla adjunta al usuario cuya cuenta desea ver.**

3 **En el menú desplegable Acciones de usuario, seleccione Ver.**

Aparece la página Ver usuario con un subconjunto de información sobre la identidad del usuario, asignaciones, seguridad, delegaciones, atributos y cumplimiento. La información de la página Ver usuario es de sólo lectura, no puede editarse.

4 **Haga clic en Cancelar para regresar a la lista de cuentas.**

▼ Para editar cuentas de usuario

Utilice la página Editar usuario y proceda como sigue para editar información de cuentas.

1 **En la interfaz de administración, seleccione Cuentas en el menú.**

2 **Marque la casilla adjunta al usuario cuya cuenta desea editar.**

3 **En el menú desplegable Acciones de usuario, seleccione Editar.**

4 **Realice las modificaciones y guárdelas.**

Identity Manager muestra la página de actualización de cuentas de recursos. En ella aparecen las cuentas de recursos asignadas al usuario y los cambios que se aplicarán a la cuenta.

5 **Seleccione Actualizar todas las cuentas de recursos para aplicar las modificaciones a todos los recursos asignados, o bien seleccione una, ninguna o varias cuentas de recursos asociadas al usuario para actualizarlas.**

6 **Vuelva a pulsar Guardar para terminar de editar o haga clic en Regresar a Edición para efectuar más cambios.**

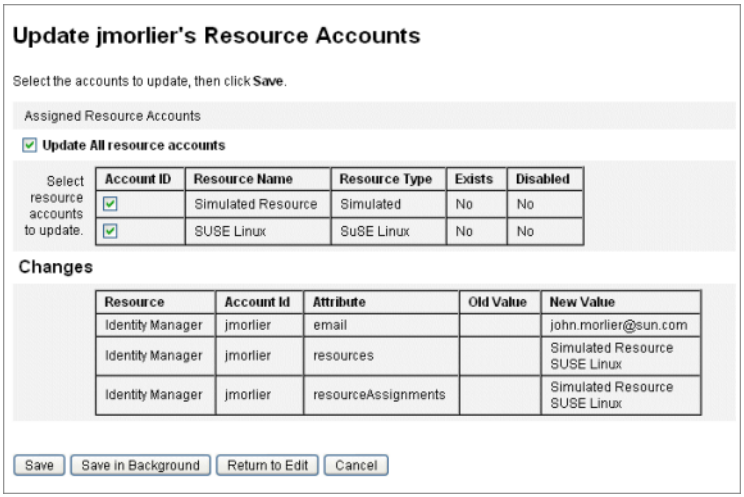


FIGURA 3–2 Editar usuario (actualización de cuentas de recursos)

Reasignación de usuarios a otra organización

La acción de mover permite suprimir uno o varios usuarios de una organización y reasignarlos, o moverlos, a otra.

▼ Para mover un usuario

1. **En la interfaz de administración, seleccione Cuentas en el menú.**
   Aparece la página Lista de usuarios.
2. **Marque la casilla adjunta al usuario o usuarios que desea mover.**
3. **En el menú desplegable Acciones de usuario, seleccione Mover.**
   Aparece la página de tareas Cambiar organización de usuarios.
4. **Seleccione la organización a la que desea reasignar el usuario y haga clic en Iniciar.**

Cambio de nombre de usuarios

Cambiar el nombre de una cuenta en un recurso suele ser complicado. Por este motivo, Identity Manager ofrece una función específica para renombrar una cuenta de usuario de Identity Manager o una o varias cuentas de recursos asociadas al usuario.

Para utilizar la función de cambio de nombre, seleccione una cuenta de usuario en la lista y, a continuación, elija la opción Cambiar nombre en la lista Acciones de usuario.

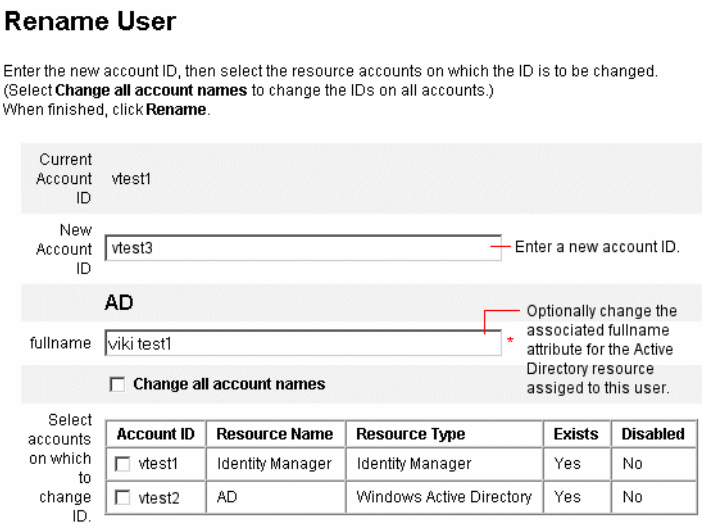
En la página Cambiar nombre de usuario puede cambiar el nombre de la cuenta de usuario, nombres de cuentas de recursos asociadas y atributos de cuentas de recursos asociadas a la cuenta del usuario en Identity Manager.

Nota – Algunos tipos de recursos no se pueden renombrar.

Como muestra la figura siguiente, el usuario tiene asignado un recurso de Active Directory.

Durante el proceso de cambio de nombre puede modificar:

- El nombre de la cuenta de usuario de Identity Manager
- El nombre de la cuenta de recurso de Active Directory
- El atributo de recurso de Active Directory (nombre completo)



Actualización de recursos asociados a una cuenta

En una acción de actualización, Identity Manager actualiza los recursos asociados a una cuenta de usuario. Las actualizaciones efectuadas desde el área de cuentas envían a los recursos seleccionados todos los cambios pendientes que se habían realizado previamente para un usuario.

Esta situación puede producirse cuando:

- Un recurso no estaba disponible cuando se efectuaron actualizaciones.
- En un rol o grupo de recursos se ha realizado un cambio que debe propagarse a todos los usuarios asignados a dicho grupo. En tal caso, debe utilizar la página Buscar usuario para encontrar los usuarios y después seleccionar los usuarios a los que desea aplicar la acción de actualización.

Hay las siguientes opciones al actualizar la cuenta de usuario:

- Elegir si las cuentas de recursos asignadas deben recibir la información actualizada.
- Actualizar todas las cuentas de recursos o seleccionar cuentas individuales en una lista.

Actualización de recursos en una sola cuenta de usuario

Para actualizar una cuenta de usuario, selecciónela en la lista y, a continuación, elija Actualizar en la lista Acciones de usuario.

En la página de actualización de cuentas de recursos, elija uno o varios recursos para actualizarlos, o bien seleccione Actualizar todas las cuentas de recursos para actualizar todas las cuentas de recursos asignadas. Cuando termine, pulse Aceptar para comenzar el proceso de actualización. Otra posibilidad es seleccionar Guardar en segundo plano para realizar la acción como un proceso en segundo plano.

Una página de confirmación corrobora los datos enviados a cada recurso.

La Figura 3–3 muestra la página de actualización de cuentas de recursos.

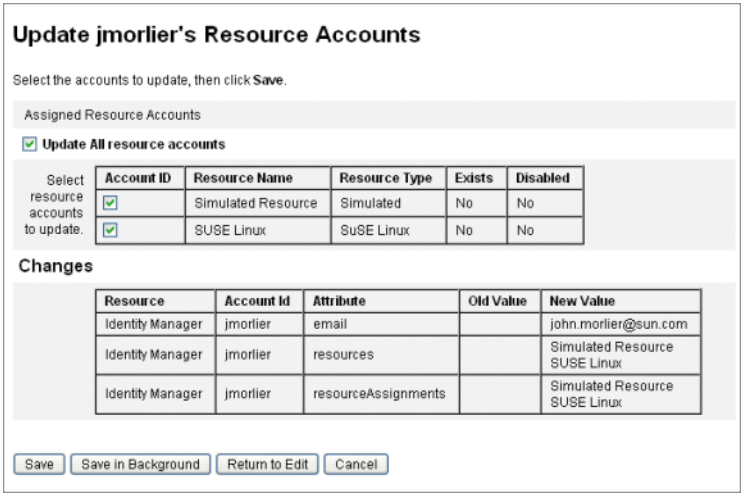


FIGURA 3–3 Actualizar cuentas de recurso

Actualización de recursos en varias cuentas de usuario

Es posible actualizar dos o más cuentas de usuario de Identity Manager simultáneamente. Seleccione varias cuentas de usuario en la lista y, a continuación, elija Actualizar en la lista Acciones de usuario.

Nota – Al actualizar varias cuentas de usuario no es posible seleccionar cuentas de recursos asignadas individualmente en cada cuenta de usuario. En vez de ello, este proceso actualiza todos los recursos en todas las cuentas de usuario seleccionadas.

Eliminación de cuentas de usuario de Identity Manager

En Identity Manager, una cuenta de usuario de Identity Manager se elimina igual que una cuenta de recursos remota. Siga los pasos para eliminar una cuenta de recursos, pero seleccionando la cuenta de Identity Manager en lugar de una cuenta de recursos remota.

Nota – Si un usuario tiene elementos de trabajo pendientes propios o delegados a otro usuario, Identity Manager no dejará que se elimine la cuenta del usuario de Identity Manager. Los elementos de trabajo delegados se deben resolver o reenviar a otro usuario para poder eliminar la cuenta del usuario en Identity Manager.

Para obtener más información, consulte "Eliminación de recursos de una sola cuenta de usuario" en la página 70 y "Eliminación de recursos de varias cuentas de usuario" en la página 71.

Eliminación de recursos de cuentas de usuario

Identity Manager ofrece diversas operaciones de eliminación que sirven para eliminar el acceso a una cuenta de usuario de Identity Manager de un recurso:

- **Eliminar**. Para cada recurso seleccionado, Identity Manager elimina la cuenta del usuario en el recurso remoto. (Para eliminar un usuario de Identity Manager, seleccione Identity Manager como recurso.)
  - Las cuentas de recursos eliminadas se *desvinculan* automáticamente del usuario de Identity Manager.
  - En el caso de las cuentas de recursos eliminadas, no se *anula la asignación* del usuario. El recurso permanece asignado al usuario salvo que se seleccione también la acción de anulación de asignación.
- **Anular asignación**. Identity Manager suprime cada recurso seleccionado de la lista de recursos asignados del usuario.
  - Las cuentas de recursos no asignadas se *desvinculan* automáticamente del usuario de Identity Manager.
  - La cuenta de usuario en el recurso remoto *no* se elimina. La cuenta permanece intacta salvo que se seleccione también la acción de eliminación.
- **Desvincular**. Para cada recurso seleccionado, la información de cuenta de recursos del usuario se suprime de Identity Manager.
  - La cuenta del usuario en el recurso remoto permanece intacta salvo que se seleccione también la acción de eliminación.
  - El recurso permanece en la lista de recursos asignados del usuario salvo que se seleccione también la acción de anulación de asignación.
  - si desvincula una cuenta asignada indirectamente al usuario mediante un rol o un grupo de recursos, el vínculo puede restaurarse al actualizar el usuario.

Aunque el desabastecimiento se incluye como una acción de usuario en los menús de la página Lista de usuarios, en realidad sólo existen tres acciones de eliminación en Identity Manager: eliminar, anular asignación y desvincular.

Para desabastecer un recurso remoto, aplique las acciones de eliminación y anulación de asignación al recurso.

Eliminación de recursos de una sola cuenta de usuario

Siga el procedimiento indicado a continuación para realizar una operación de eliminación con un único usuario de Identity Manager. Si trabaja con una única cuenta de usuario a la vez, puede especificar distintas operaciones de eliminación, anulación de asignación y/o desvinculación para diferentes cuentas de recursos.

▼ Para empezar una acción de eliminación, anulación de asignación o desvinculación en una sola cuenta de usuario

1. **En la interfaz de administración, seleccione Cuentas en el menú principal.**

   Aparece la página Lista de usuarios en la ficha Listar cuentas.

2. **Seleccione un usuario y haga clic en el menú desplegable Acciones de usuario.**

3. **Elija en la lista cualquiera de las acciones de eliminación (Eliminar, Anular asignación o Desvincular).**

   Identity Manager muestra la página de eliminación de cuentas de recursos (Figura 3–4).

4. **Rellene el formulario. Encontrará más información sobre las acciones Eliminar, Anular asignación y Desvincular en "Eliminación de recursos de cuentas de usuario" en la página 69.**

5. **Haga clic en Aceptar.**

   La Figura 3–4 muestra la página de eliminación de cuentas de recursos. En la captura de pantalla, el usuario jrenfro tiene una sola cuenta activa en un recurso remoto (Simulated Resource). Se ha seleccionado la acción Eliminar, lo que significa que, una vez enviado el formulario, se eliminará la cuenta de jrenfro en el recurso. Como las cuentas eliminadas se desvinculan automáticamente, la información de cuentas de este recurso desaparecerá de Identity Manager. El recurso "Simulated Resource" permanecerá asignado al usuario jrenfro, porque no se ha seleccionado la acción de anulación de asignación.

   Para eliminar la cuenta de Identity Manager de jrenfro, es preciso seleccionar la acción Eliminar en Identity Manager.

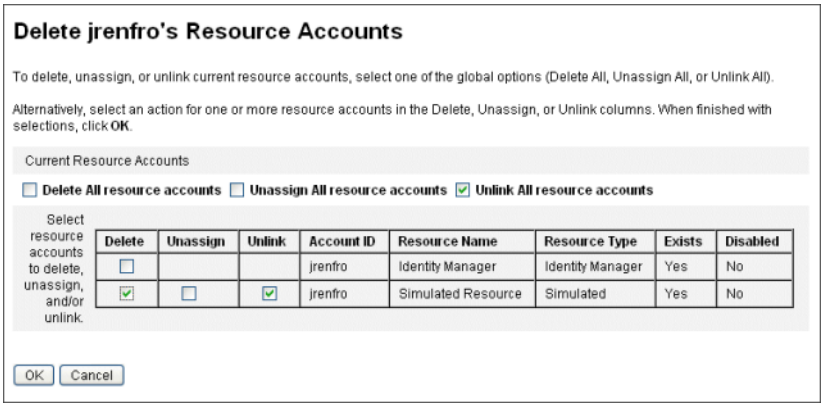


FIGURA 3–4 Página de eliminación de cuentas de recursos

Eliminación de recursos de varias cuentas de usuario

Es posible realizar una operación de eliminación con más de una cuenta de usuario de Identity Manager simultáneamente, pero la operación de eliminación seleccionada sólo puede aplicarse a *todas* las cuentas de recursos del usuario.

Las operaciones de eliminación también pueden efectuarse mediante la función Acciones masivas de cuenta de Identity Manager. Consulte "Comandos Delete, DeleteAndUnlink, Disable, Enable, Unassign y Unlink" en la página 82.

▼ Para empezar una acción de eliminación, anulación de asignación o desvinculación en varias cuentas de usuario

1. **En la interfaz de administración, seleccione Cuentas en el menú principal.**

   Aparece la página Lista de usuarios en la ficha Listar cuentas.

2. **Seleccione uno o más usuarios y haga clic en el menú desplegable Acciones de usuario.**

3. **Elija en la lista cualquiera de las acciones de eliminación (Eliminar, Anular asignación o Desvincular).**

   Identity Manager muestra la página Confirmar si Eliminar, Anular asignación o Desvincular (Figura 3–5).

4. **Especifique la acción que desea realizar.**

Las opciones incluyen:

- **Eliminar sólo el usuario**. Elimina las cuentas de Identity Manager de los usuarios. Esta opción no elimina ni anula la asignación de las cuentas de recursos de los usuarios.
- **Eliminar el usuario y las cuentas de recursos**. Elimina las cuentas de Identity Manager de los usuarios y todas las cuentas de recursos de los usuarios.
- **Eliminar sólo las cuentas de recursos**. Elimina todas las cuentas de recursos de los usuarios. Esta opción no anula la asignación de las cuentas de recursos ni elimina las cuentas de Identity Manager de los usuarios.
- **Eliminar las cuentas de recursos y anular la asignación de los recursos asignados directamente desde el usuario**. Elimina y anula la asignación de todas las cuentas de recursos de los usuarios, pero no elimina las cuentas de Identity Manager de los usuarios.
- **Anular asignación de las cuentas de recursos asignadas directamente desde el usuario**. Anula la asignación de las cuentas de recursos asignadas directamente. Esta opción no elimina las cuentas de los usuarios en los recursos remotos. Las cuentas de recursos asignadas a través de un rol o un grupo de recursos no resultan afectadas.
- **Desvincular las cuentas de recursos del usuario**. La información de cuenta de recursos del usuario se suprime de Identity Manager. No se eliminan ni se anula la asignación de las cuentas de los usuarios en los recursos remotos. Las cuentas asignadas indirectamente a los usuarios mediante un rol o un grupo de recursos pueden restaurarse al actualizar los usuarios.

5 Haga clic en Aceptar.

La Figura 3–5 muestra la página Confirmar si Eliminar, Anular asignación o Desvincular. En la parte superior de la página aparecen las seis acciones disponibles que pueden realizarse para varios usuarios. En la parte inferior de la página aparecen los usuarios que resultarán afectados por la acción seleccionada.

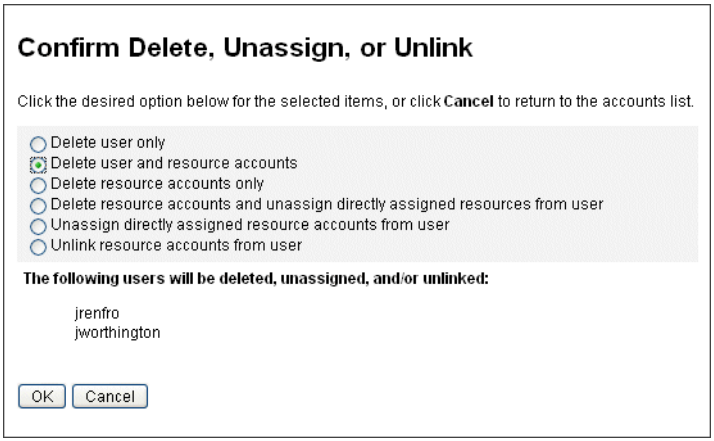


FIGURA 3–5 Página Confirmar si Eliminar, Anular asignación o Desvincular

Cambio de contraseñas de usuario

A todos los usuarios de Identity Manager se les asigna una contraseña. Una vez establecida, la contraseña de usuario de Identity Manager se utiliza para sincronizar las contraseñas de las cuentas de recursos del usuario. Si no es posible sincronizar una o varias contraseñas de cuentas de recursos (por ejemplo, para cumplir directivas de contraseñas obligatorias), puede definirlas individualmente.

Nota – Encontrará información sobre las directivas de contraseñas de cuenta y sobre la autenticación de usuarios en la sección "Administración de la seguridad de las cuentas y los privilegios" en la página 87.

▼ Cambio de contraseñas en la página Lista de usuarios

Puede cambiar la contraseña de una cuenta de usuario con la acción Modificar contraseña de usuario de la página Lista de usuarios (Cuentas → Listar cuentas). Siga estos pasos:

1. **En la interfaz de administración, seleccione Cuentas en el menú principal.**

   Aparece la página Lista de usuarios en la ficha Listar cuentas.

2. **Seleccione un usuario y haga clic en el menú desplegable Acciones de usuario.**

3. **Para cambiar la contraseña, seleccione Cambiar contraseña.**

   Aparece la página Modificar contraseña de usuario.

4. **Escriba la contraseña nueva y pulse el botón Cambiar contraseña.**

▼ Para cambiar contraseñas con el menú principal

Siga estos pasos para cambiar la contraseña de una cuenta de usuario desde el menú principal:

1 **En la interfaz de administración, seleccione Contraseñas en el menú principal.**

De manera predeterminada, aparece la página Modificar contraseña de usuario.

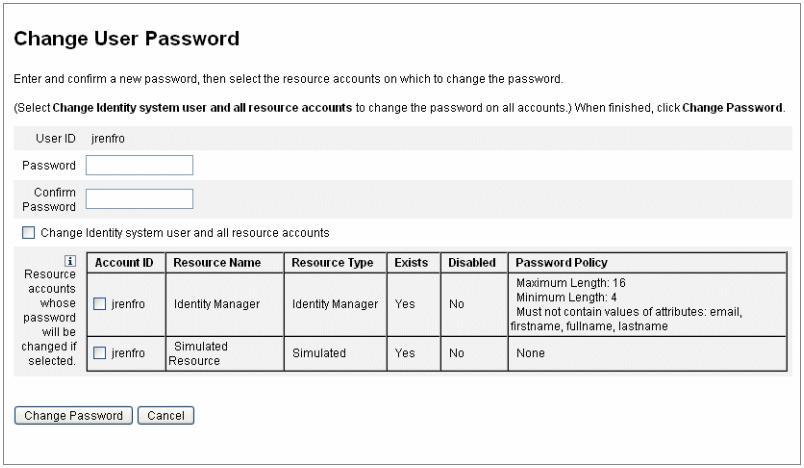


FIGURA 3–6 Modificar contraseña de usuario

2 **Seleccione un término de búsqueda (por ejemplo, nombre de cuenta, dirección de correo electrónico, apellidos o nombre) y un tipo de búsqueda (comienza con, termina con o es).**

3 **Introduzca uno o varios caracteres de un término de búsqueda en el campo de entrada y, a continuación, haga clic en Buscar. Identity Manager devuelve una lista de todos los usuarios cuyos ID contienen los caracteres especificados. Haga clic para seleccionar un usuario y volver a la página Modificar contraseña de usuario.**

4 **Introduzca y confirme la información de la nueva contraseña y después haga clic en Cambiar contraseña para modificar la contraseña de usuario en la lista de cuentas de recursos. Identity Manager muestra un diagrama de flujo de trabajo con la secuencia de las acciones realizadas para cambiar la contraseña.**

Reinicialización de contraseñas de usuario

Para reinicializar las contraseñas de las cuentas de usuario de Identity Manager se sigue un proceso similar al de cambio de contraseña. Lo que varía en el proceso de reinicialización es que no se especifica una contraseña nueva. En vez de ello, Identity Manager genera aleatoriamente

una contraseña nueva (según las directivas de selección y de contraseñas) para la cuenta de usuario, las cuentas de recursos o una combinación de éstas.

La directiva asignada al usuario (ya sea directamente o a través de su organización) controla diversas opciones de reinicialización, entre ellas:

- La frecuencia con que se puede reinicializar una contraseña sin que se inhabilite la reinicialización.
- Dónde aparece o a dónde se envía la nueva contraseña.

  Según la Opción de notificación de reinicialización seleccionada para el rol, Identity Manager enviará la nueva contraseña al usuario por correo electrónico o se la mostrará en la página Resultados al administrador de Identity Manager que ha solicitado la reinicialización.

▼ Reinicialización de contraseñas en la página Lista de usuarios

La acción de usuario Reinicializar contraseña está disponible en la página Lista de usuarios (Cuentas > Listar cuentas).

Siga estos pasos para reinicializar una contraseña en la página Lista de usuarios:

1. **En la interfaz de administración, seleccione Cuentas en el menú principal. Aparece la página Lista de usuarios en la ficha Listar cuentas.**
2. **Seleccione un usuario y haga clic en el menú desplegable Acciones de usuario.**
3. **Para reinicializar la contraseña, seleccione Reinicializar contraseña.**

   Aparece la página Reinicializar contraseña de usuario.
4. **Pulse el botón Reinicializar contraseña.**

▼ Para caducar contraseñas aplicando la directiva de cuentas de Identity Manager

Cuando se reinicializa una contraseña de usuario, la contraseña caduca inmediatamente de manera predeterminada. Por tanto, la primera vez que los usuarios inician una sesión tras reinicializar la contraseña, han de elegir una contraseña nueva para obtener acceso. Para anular este comportamiento predeterminado, puede editar el formulario de reinicialización de contraseña de usuario, de modo que la contraseña del usuario caducará cuando lo estipule la directiva de caducidad de contraseñas establecida en la directiva de cuentas de Identity Manager asociada a ese usuario.

Proceda como sigue para anular el requisito de cambio de contraseña predeterminado:

1 **Edite el formulario de reinicialización de contraseña de usuario y defina en `false` este valor:**

```
resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword
```

2 **Use la opción Reinicializar de la directiva de cuentas de Identity Manager para especificar cuándo debe caducar una contraseña.**

Los valores de configuración incluyen:

- **permanente**. Identity Manager aplica el periodo especificado en el atributo de directiva `passwordExpiry` para calcular a partir de la fecha actual en qué fecha debe reinicializarse la contraseña y después asigna la fecha resultante al usuario. Si no se especifica ningún valor, la contraseña cambiada o reinicializada no caduca nunca.
- **temporal**. Identity Manager aplica el periodo especificado en el atributo de directiva `tempPasswordExpiry` para calcular a partir de la fecha actual en qué fecha debe reinicializarse la contraseña y después asigna la fecha resultante al usuario. Si no se especifica ningún valor, la contraseña cambiada o reinicializada no caduca nunca. Si `tempPasswordExpiry` se define en el valor 0, la contraseña caduca inmediatamente.

  El atributo `tempPasswordExpiry` sólo se aplica cuando se reinicializan contraseñas (cambian aleatoriamente). No se aplica a las modificaciones de contraseñas.

Inhabilitación, habilitación y desbloqueo de cuentas de usuario

En esta sección se explica cómo inhabilitar y habilitar cuentas de usuario de Identity Manager. También se indica cómo ayudar a los usuarios cuyas cuentas de Identity Manager han quedado bloqueadas.

▼ Para inhabilitar cuentas de usuario

Al inhabilitar una cuenta de usuario, se modifica esa cuenta para que el usuario ya no pueda iniciar la sesión en Identity Manager ni en ninguna cuenta de recursos asignada.

Recuerde que los administradores pueden inhabilitar cuentas de usuario con la interfaz de administración, pero no pueden bloquearlas. Las cuentas sólo se bloquean cuando el usuario supera el número permitido de intentos fallidos de inicio de sesión especificados en la directiva de cuentas de Identity Manager.

Nota – Si un recurso asignado carece de soporte nativo para inhabilitar cuentas, pero sí permite cambiar contraseñas, es posible configurar Identity Manager para inhabilitar cuentas de usuario en dicho recurso asignando nuevas contraseñas generadas aleatoriamente.

Siga estos pasos para asegurarse de que esta funcionalidad actúa correctamente:

1. **Abra la página "Parámetros de Identity System" en el asistente de edición de recursos. (Dentro de "Administración de recursos" en la página 167 encontrará instrucciones para iniciar el asistente.)**

2. **En la tabla "Configuración de funciones de cuenta", compruebe si las funciones Contraseña e Inhabilitar no tienen marcada la columna ¿Inhabilitar? (Para mostrar la función Inhabilitar, seleccione Mostrar todas las funciones.)**

   Si la función Mostrar Inhabilitar tiene marcada la columna ¿Inhabilitar?, no será posible inhabilitar las cuentas del recurso.

Más información

Inhabilitación de cuentas de usuario individuales

Para inhabilitar una cuenta de usuario, selecciónela en la lista de usuarios y, a continuación, elija Inhabilitar en el menú desplegable Acciones de usuario.

En la página Inhabilitar que aparece, seleccione las cuentas de recursos que desea inhabilitar y pulse Aceptar. Identity Manager muestra los resultados de inhabilitar la cuenta de usuario de Identity Manager y todas las cuentas de recursos asociadas. La lista de cuentas indica que la cuenta de usuario está inhabilitada.

Inhabilitación de varias cuentas de usuario

Es posible inhabilitar dos o más cuentas de usuario de Identity Manager simultáneamente. Seleccione varias cuentas de usuario en la lista y, a continuación, elija Inhabilitar en la lista Acciones de usuario.

Nota – Al inhabilitar varias cuentas de usuario no es posible seleccionar cuentas de recursos asignadas individualmente en cada cuenta de usuario. En vez de ello, este proceso inhabilita todos los recursos en todas las cuentas de usuario seleccionadas.

▼ Para habilitar cuentas de usuario en un recurso mediante reinicializaciones de contraseña

Al habilitar una cuenta de usuario se invierte el proceso de inhabilitación.

Según las opciones de notificación seleccionadas, Identity Manager también muestra la contraseña en la página de resultados del administrador.

El usuario puede reinicializar a continuación la contraseña (mediante el proceso de autenticación), o puede restablecerla un usuario con privilegios de administrador.

Nota – Si un recurso asignado carece de soporte nativo para habilitar cuentas, pero sí permite cambiar contraseñas, es posible configurar Identity Manager para habilitar cuentas de usuario en dicho recurso reinicializando las contraseñas.

Siga estos pasos para asegurarse de que esta funcionalidad actúa correctamente:

1. **Abra la página "Parámetros de Identity System" en el asistente de edición de recursos. (Dentro de "Administración de recursos" en la página 167 encontrará instrucciones para iniciar el asistente.)**

2. **En la tabla "Configuración de funciones de cuenta", compruebe si las funciones Contraseña e Habilitar no tienen marcada ¿Inhabilitar?. columna ¿Inhabilitar? (Para mostrar la función Habilitar, seleccione Mostrar todas las funciones.)**

   Si la función Habilitar tiene marcada la columna ¿Inhabilitar?, no será posible habilitar las cuentas del recurso.

Más información

Habilitación de cuentas de usuario individuales

Para habilitar una cuenta de usuario, selecciónela en la lista y, a continuación, elija Habilitar en la lista Acciones de usuario.

En la página Habilitar que aparece, seleccione las cuentas de recursos que desea habilitar y pulse Aceptar. Identity Manager muestra los resultados de habilitar la cuenta de Identity Manager y todas las cuentas de recursos asociadas.

Habilitación de varias cuentas de usuario

Es posible habilitar dos o más cuentas de usuario de Identity Manager simultáneamente. Seleccione varias cuentas de usuario en la lista y, a continuación, elija Habilitar en la lista Acciones de usuario.

Nota – Al habilitar varias cuentas de usuario no es posible seleccionar cuentas de recursos asignadas individualmente en cada cuenta de usuario. En vez de ello, este proceso habilita todos los recursos en todas las cuentas de usuario seleccionadas.

Desbloqueo de cuentas de usuario

Los usuarios quedan bloqueados cuando fracasan sus intentos de iniciar una sesión en Identity Manager. Para quedar bloqueado, el usuario debe superar el número permitido de intentos fallidos de inicio de sesión especificados en la directiva de cuentas de Identity Manager.

Nota – En la cifra de bloqueo de Identity Manager sólo cuentan los intentos de iniciar la sesión en una interfaz de usuario de Identity Manager (es decir, las interfaces de administración, usuario final, línea de comandos o API SPML). No se cuentan los intentos fallidos de inicio de sesión en cuentas de recursos, que tampoco bloquean la cuenta de Identity Manager del usuario.

La directiva de cuentas de Identity Manager establece el máximo número de intentos fallidos de iniciar la sesión con contraseña o pregunta que se pueden realizar.

- Los usuarios que superan el número máximo de intentos fallidos de inicio de sesión con contraseña quedan bloqueados en todas las interfaces de aplicación de Identity Manager, incluida la de olvido de contraseña.
- Los usuarios que superan el número máximo de intentos fallidos de inicio de sesión con pregunta pueden autenticarse en todas las interfaces de aplicación de Identity Manager, excepto la de olvido de contraseña.

Tentativas de contraseña de inicio de sesión no satisfactorias

Los usuarios que tienen bloqueado el acceso a Identity Manager debido a un exceso de intentos fallidos de inicio de sesión con contraseña no pueden iniciar la sesión hasta que un administrador desbloquee la cuenta o hasta que caduque el bloqueo.

- Un administrador puede desbloquear una cuenta si tiene control administrativo sobre la organización a la que está afiliado el usuario y posee la capacidad `Desbloquear usuario`.
- Si se define un valor de `tiempo de espera de bloqueo` en la directiva de cuentas de Identity Manager, el bloqueo de una cuenta acabará caducando. El valor de `tiempo de espera de bloqueo` para los intentos fallidos de inicio de sesión con contraseña está determinado por el valor de "El bloqueo de cuenta debido a fallos de inicio de sesión con contraseña caduca en".

Tentativas de pregunta de inicio de sesión no satisfactorias

Los usuarios que tienen bloqueado el acceso a la interfaz de olvido de contraseña debido a un exceso de intentos fallidos de inicio de sesión con pregunta no pueden iniciar la sesión en dicha interfaz hasta que un administrador desbloquee la cuenta, o hasta que el usuario bloqueado (o un usuario con capacidades adecuadas) cambie o reinicialice la contraseña del usuario), o hasta que caduque el bloqueo.

- Un administrador puede desbloquear una cuenta si tiene control administrativo sobre la organización a la que está afiliado el usuario y posee la capacidad `Desbloquear usuario`.
- Si se define un valor de `tiempo de espera de bloqueo` en la directiva de cuentas de Identity Manager, el bloqueo de una cuenta acabará caducando. El valor de `tiempo de espera de bloqueo` para los intentos de inicio fallidos de sesión con pregunta está determinado por el valor de "El bloqueo de cuenta debido a fallos de inicio de sesión con pregunta caduca en".

Un administrador con capacidades adecuadas puede aplicar las operaciones siguientes al estado de bloqueo de un usuario.

- Actualizar (incluido el reabastecimiento de recursos).
- Cambiar o reinicializar la contraseña.
- Inhabilitar o habilitar.
- Renombrar
- Desbloquear

Para desbloquear cuentas, seleccione una o varias cuentas de usuario en la lista y, a continuación, elija Desbloquear usuarios en la lista Acciones de usuario o Acciones de organización.

Acciones masivas de cuenta

En las cuentas de Identity Manager se pueden realizar diversas acciones *masivas*, lo que permite actuar sobre múltiples cuentas a la vez.

Es posible efectuar las siguientes acciones masivas:

- **Delete**. Elimina, anula asignaciones y desvincula las cuentas de recursos seleccionadas. Seleccione la opción "Cuenta de Identity Manager de destino" para eliminar también la cuenta de Identity Manager de cada usuario.
- **Eliminar y desvincular**. Elimina todas las cuentas de recursos seleccionadas y desvincula las cuentas de los usuarios.
- **Inhabilitar**. Inhabilita las cuentas de recursos seleccionadas. Seleccione la opción "Cuenta de Identity Manager de destino" para inhabilitar también la cuenta de Identity Manager de cada usuario.
- **Habilitar**. Habilita las cuentas de recursos seleccionadas. Seleccione la opción "Cuenta de Identity Manager de destino" para habilitar la cuenta de Identity Manager de cada usuario.
- **Anular asignación, Desvincular**. Desvincula las cuentas de recursos seleccionadas y suprime las asignaciones de cuentas de usuario de Identity Manager a esos recursos. Al anular una asignación no se elimina la cuenta del recurso. No puede anular la asignación de una cuenta que ha sido asignada indirectamente al usuario de Identity Manager mediante un rol o un grupo de recursos.
- **Unlink**. Suprime la asociación (vínculo) de una cuenta de recursos con la cuenta de usuario de Identity Manager. Al desvincular no se elimina la cuenta del recurso. Si desvincula una cuenta que ha sido asignada indirectamente al usuario de Identity Manager mediante un rol o un grupo de recursos, el vínculo puede restaurarse al actualizar el usuario.

Las acciones masivas funcionan de forma más eficaz si dispone de una lista de usuarios en un archivo o una aplicación, por ejemplo, un cliente de correo electrónico o un programa de hoja de cálculo. Puede copiar y pegar la lista en un campo de esta página de la interfaz o bien cargar la lista de usuarios desde un archivo.

La mayoría de estas acciones pueden realizarse en los resultados de una búsqueda de usuarios. Utilice la página Buscar usuarios (Cuentas → Buscar usuarios) para buscar usuarios.

Puede guardar los resultados de una operación masiva de cuentas en un archivo CSV con sólo hacer clic en Descargar CSV cuando aparezcan los resultados de la tarea al terminarla.

Inicio de acciones masivas de cuenta

▼ Para iniciar acciones masivas de cuenta

1. **En la interfaz de administración, seleccione Cuentas en el menú principal.**
2. **Haga clic sobre Iniciar acciones masivas en el menú secundario.**
3. **Rellene el formulario y pulse Iniciar.**

   Identity Manager inicia una tarea en segundo plano para realizar las acciones masivas.

   Para supervisar el estado de la tarea de acciones masivas, elija Tareas del servidor en el menú principal y después Todas las tareas.

Uso de listas de acciones

Puede especificar una lista de acciones masivas con un formato de valores separados por comas (CSV). Esto le permite ofrecer una combinación de diferentes tipos de acciones en una única lista de acciones. Además, puede especificar acciones de creación y actualización más complejas.

El formato CSV está formado por dos o más líneas de entrada. Cada línea consta de una lista de valores separados por comas. La primera línea contiene los nombres de los campos. Cada una de las líneas restantes corresponde a una acción que se debe efectuar en un usuario de Identity Manager, en las cuentas de recursos del usuario o en ambos elementos. Cada línea debe contener el mismo número de valores. Los valores vacíos dejarán sin modificar el valor del campo correspondiente.

Cualquier entrada de acción masiva en formato CSV tiene dos campos obligatorios:

- **user**. Contiene el nombre del usuario de Identity Manager.
- **command**. Contiene la acción que se aplica al el usuario de Identity Manager. Los comandos válidos son:
  - **Delete**. Elimina, anula asignaciones y desvincula las cuentas de recursos, la cuenta de Identity Manager o ambas.
  - **DeleteAndUnlink**. Elimina y desvincula cuentas de recursos.
  - **Disable**. Inhabilita las cuentas de recursos, la cuenta de Identity Manager o ambas.

- **Enable**. Habilita las cuentas de recursos, la cuenta de Identity Manager o ambas.
- **Unassign**. Anula asignaciones y desvincula las cuentas de recursos.
- **Unlink**. Desvincula las cuentas de recursos.
- **Create**. Crea la cuenta de Identity Manager. También crea de forma opcional cuentas de recursos.
- **Update**. Actualiza la cuenta de Identity Manager. También crea, actualiza o elimina de forma opcional cuentas de recursos.
- **CreateOrUpdate**. Realiza una acción de creación si la cuenta de Identity Manager no existe aún. De lo contrario, realiza una acción de actualización.

Comandos Delete, DeleteAndUnlink, Disable, Enable, Unassign y Unlink

Para efectuar acciones con los comandos Delete, DeleteAndUnlink, Disable, Enable, Unassign o Unlink, el único campo adicional que hace falta especificar es "resources". En el campo "resources" debe indicar qué cuentas de qué recursos resultarán afectadas.

El campo "resources" admite los siguientes valores:

- **all**. Procesa todas las cuentas de recursos, incluida la de Identity Manager.
- **resonly**. Procesa todas las cuentas de recursos excepto la de Identity Manager.
- *nombre_recurso* `[ | ` *nombre_recurso ...* `]`. Procesa las cuentas de recursos especificadas. Especifique Identity Manager para procesar la cuenta de Identity Manager.

A continuación se muestra un ejemplo del formato CSV para varias de estas acciones:

```
command,user,resources
Delete,John Doe,all
Disable,Jane Doe,resonly
Enable,Henry Smith,Identity Manager
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Comandos Create, Update y CreateOrUpdate

Si va a realizar acciones con los comandos Create, Update o CreateOrUpdate, puede especificar campos de la vista de usuario además de los campos "user" y "command". Los nombres de campo utilizados son las expresiones de ruta de los atributos en las vistas. Encontrará información sobre los atributos disponibles en la vista de usuario dentro de "User View Attributes" de *Sun Identity Manager Deployment Reference*. Si está utilizando un formulario de usuario personalizado, los nombres de campo del formulario contienen algunas de las expresiones de ruta que puede utilizar.

Algunas de las expresiones de ruta más utilizadas en las acciones masivas son:

- **waveset.roles**. Una lista con uno o varios nombres de rol para asignarlos a la cuenta de Identity Manager.
- **waveset.resources**. Una lista con uno o varios nombres de recurso para asignarlos a la cuenta de Identity Manager.
- **waveset.applications**. Una lista con uno o varios nombres de rol para asignarlos a la cuenta de Identity Manager.
- **waveset.organization**. El nombre de la organización donde debe situarse la cuenta de Identity Manager.
- **accounts**[*nombre_recurso*].*nombre_atributo*. Un atributo de cuenta de recursos. Los nombres de los atributos aparecen enumerados en el esquema del recurso.

Éste es un ejemplo de uso del formato CSV para realizar acciones de creación y actualización:

```
command,user,waveset.resources,password.password,
password.confirmPassword,accounts[Windows Active Directory].description,
accounts[Corporate Directory].location Create,John Doe,
Windows Active Directory|Solaris Server,changeit,changeit,John Doe - 888-555-5555,
Create,Jane Smith,Corporate Directory,changeit,changeit,,New York
CreateOrUpdate,Bill Jones,,,,,California
```

El comando `CreateOrUpdate` permite especificar un determinado tipo de cuenta en un recurso que admite varios tipos de cuenta. Por tanto, si un usuario tiene varias cuentas en un determinado recurso, cada una de las cuales puede ser de un tipo de cuenta distinto, el ejemplo siguiente ilustra cómo actualizar el tipo de cuenta `admin` para el usuario `UserAye`:

```
command,user,accounts[Sim1|admin].emailAddress
CreateOrUpdate,userAye,bbye8@example.com
```

Nota –

Aunque el comando `CreateOrUpdate` permite configurar atributos específicos de cuenta para las cuentas de un usuario, no olvide que los siguientes valores de la sección global de la vista del usuario se aplicarán a *todas* las cuentas especificadas:

- `accountId`
- `email`
- `password`
- `disable`
- Todos los atributos extendidos

En consecuencia, un comando `BulkOps` con el formato siguiente *quizá* no actúe como se espera.

```
command,user,accounts[Sim1].email
CreateOrUpdate,userAye,bbye8@example.com
```

Si `userAye` ya tiene un valor para `email`, dicho valor se aplicará al atributo email en el recurso `Sim1`. No es posible anular este comportamiento.

Campos con varios valores

Algunos campos pueden tener múltiples valores. Se les conoce como campos de varios valores. Por ejemplo, el campo `waveset.resources` puede utilizarse para asignar varios recursos a un usuario. Puede emplear el carácter de barra vertical o línea (|) para separar varios valores en un campo. La sintaxis de varios valores puede especificarse de la siguiente forma:

```
value0 | value1 [ | value2 ... ]
```

Al actualizar campos de varios valores en usuarios existentes, no es recomendable sustituir los valores actuales del campo por uno o varios valores nuevos. Es posible que desee eliminar algunos valores o agregar nuevos valores a los actuales. Puede utilizar directivas de campo para especificar cómo desea que se utilicen los valores del campo. Las directivas de campo anteceden al valor de campo y suelen ir entre caracteres de barra vertical:

```
|directive [ ; directive ] | field values
```

Puede elegir las siguientes directivas:

- **Replace**. Sustituye los valores actuales por los especificados. Ésta es la directiva predeterminada si no se ha especificado ninguna (o sólo se ha especificado la directiva List, Enumerar).
- **Merge**. Añade los valores especificados a los valores actuales. Los valores duplicados se filtran.
- **Remove**. Suprime los valores especificados de los valores actuales.
- **List**. Impone el valor del campo para que se utilice como si tuviera varios valores, aunque sólo tenga uno. Este directiva no suele ser necesaria, ya que la mayoría de los campos se controlan de forma adecuada, independientemente del número de valores. Ésta es la única directiva que puede especificarse con otra.

Nota – En los valores de campo se diferencian mayúsculas de minúsculas. Debe tenerse en cuenta al especificar las directivas Merge (Fusionar) y Remove (Eliminar). Los valores deben coincidir de forma exacta parra eliminarlos correctamente o para impedir que haya varios valores similares al realizar una fusión.

Caracteres especiales en valores de campo

Si un valor de campo incluye una coma (`,`) o comillas (`"`), o si desea conservar los espacios iniciales o finales, deberá introducir el valor entre comillas (`"valor_campo"`). Deberá sustituir las comillas del valor de campo por dos caracteres de comillas (`"`). Por ejemplo, `"John ""Johnny"" Smith"` da como resultado el valor de campo `John "Johnny" Smith`.

Si un valor de campo contiene una barra vertical (|) o inclinada inversa (\), deberá preceder dicho carácter con una barra inclinada inversa (\| o \\).

Atributos de vista de acciones masivas

Cuando se realizan acciones con los comandos Create, Update o CreateOrUpdate, hay otros atributos de la vista de usuario que sólo están disponibles o utilizables al procesar acciones masivas. Se puede hacer referencia a estos atributos en el formulario de usuario para permitir un comportamiento específico en las acciones masivas.

Estos atributos son los siguientes:

- Los atributos `waveset.bulk.fields.`*nombre_campo* contienen los valores de los campos leídos en la entrada CSV, donde *nombre_campo* es el nombre del campo. Por ejemplo, los campos command y user se incluyen en los atributos con las expresiones de ruta `waveset.bulk.fields.command` y `waveset.bulk.fields.user`, respectivamente.
- Los atributos `waveset.bulk.fieldDirectives.nombre_campo` sólo se definen para los campos para los que se ha especificado una directiva. El valor es la cadena de la directiva.
- Configure el atributo booleano `waveset.bulk.abort` en el valor "true" para anular la acción actual.
- Configure el atributo `waveset.bulk.abortMessage` en una cadena de mensaje para que aparezca cuando `waveset.bulk.abort` se haya definido como "true". Si no se ha definido este atributo, se mostrará un mensaje de anulación genérico.

Reglas de correlación y confirmación

Utilice las reglas de correlación y confirmación cuando no disponga del nombre de usuario de Identity Manager para escribirlo en el campo usuario de sus acciones. Si no especifica un valor para el campo Usuario, deberá especificar una regla de correlación al iniciar la acción en masa. Si especifica un valor para el campo Usuario, las reglas de correlación y confirmación no se evaluarán para esa acción.

Una regla de correlación busca los usuarios de Identity Manager que coinciden con los campos de la acción. Una regla de confirmación prueba un usuario de Identity Manager con respecto a los campos de la acción para determinar si coincide o no. Este tratamiento bifásico permite a Identity Manager mejorar la correlación, ya que encuentra rápidamente a posibles usuarios (según el nombre o los atributos) y realiza comprobaciones costosas solamente en el caso de posibles usuarios.

Cree una regla de correlación o de confirmación creando un objeto de regla con un subtipo de `SUBTYPE_ACCOUNT_CORRELATION_RULE` o `SUBTYPE_ACCOUNT_CONFIRMATION_RULE`, respectivamente.

Para obtener más información sobre las reglas de correlación y de confirmación, consulte el Capítulo 3, “Data Loading and Synchronization” de *Sun Identity Manager Deployment Guide*.

Reglas de correlación

El valor de entrada de una regla de correlación es una asignación de los campos de acción. La salida debe ser uno de los siguientes:

- Cadena (con un nombre o ID de usuario)
- Lista de elementos de cadena (un ID o nombre de usuario cada uno)
- Lista de elementos de `WSAttribute`
- Lista de elementos de `AttributeCondition`

Una regla de correlación típica genera una lista de nombres de usuario según los valores de los campos de la acción. Una regla de correlación también puede generar una lista de condiciones de atributo (relacionadas con los atributos de solicitud de `Type.USER`) que se utilizarán para seleccionar usuarios.

Una regla de correlación debe ser relativamente económica pero lo más selectiva posible. Si es posible, deje el procesamiento costoso para una regla de confirmación.

Las condiciones de atributo deben hacer referencia a atributos de `Type.USER` que puedan solicitarse. Se configuran en el objeto de configuración de Identity Manager denominado `IDM Schema Configuration`.

Para realizar la correlación en un atributo extendido es necesario una configuración especial:

El atributo extendido debe especificarse como consultable.

▼ Para configurar como consultable un atributo extendido

1. **Abra** `IDM Schema Configuration`**. Necesita la capacidad de IDM Schema Configuration para ver o editar** `IDM Schema Configuration`**.**

2. **Busque el elemento** `<IDMObjectClassConfiguration name='Usuario'>`**.**

3. **Busque el elemento** `<IDMObjectClassAttributeConfiguration name=' xyz '>`**, donde** `xyz` **es el nombre del atributo que desea configurar como consultable.**

4. **Configure** `queryable='true'`

   En "Reglas de correlación" en la página 86, el atributo extendido `email` se define como consultable.

Ejemplo 3–1 Extracto de XML donde se define el atributo extendido email como consultable

```
<IDMSchemaConfiguration>
  <IDMAttributeConfigurations>
    <IDMAttributeConfiguration name='email' syntax='STRING'/>
    </IDMAttributeConfiguration>
```

```
  </IDMAttributeConfigurations>
  <IDMObjectClassConfigurations>
    <IDMObjectClassConfiguration name='User' extends='Principal' description='User description'>
      <IDMObjectClassAttributeConfiguration name='email' queryable='true'/>
    </IDMObjectClassConfiguration>
  </IDMObjectClassConfigurations>
</IDMSchemaConfiguration>
```

Para que el cambio de `IDM Schema Configuration` surta efecto, debe reiniciar la aplicación de Identity Manager (o el servidor de aplicaciones).

Reglas de confirmación

En cualquier regla de confirmación las entradas son así:

- Use `userview` para una vista completa de un usuario de Identity Manager.
- Use `account` para una asignación de campos de acción.

Una regla de confirmación devuelve un valor booleano en forma de cadena de "verdadero" si el usuario coincide con los campos de acción. Si no es así, el valor que devuelve es "falso".

Una regla de confirmación típica compara los valores internos de la vista del usuario con los valores de los campos de acción. Como segunda fase opcional en el procesamiento de correlación, la regla de confirmación realiza una comprobación que no se puede expresar en una regla de correlación (o que es demasiado costosa para evaluarla en una regla de correlación).

En general, sólo se necesita una regla de confirmación en los siguientes casos:

- La regla de correlación puede devolver más de un usuario coincidente.
- Los valores de usuario que deben compararse no son consultables.

Una regla de confirmación se ejecuta una vez para cada usuario coincidente devuelto por la regla de correlación.

Administración de la seguridad de las cuentas y los privilegios

En esta sección se tratan acciones que pueden realizarse para proporcionar acceso seguro a las cuentas de usuario y para administrar los privilegios de usuario en Identity Manager.

- "Definición de directivas de contraseñas" en la página 88
- "Autenticación de usuarios" en la página 91
- "Asignación de privilegios administrativos" en la página 95

Definición de directivas de contraseñas

Las directivas de contraseñas de recursos establecen las limitaciones de las contraseñas. Las directivas de contraseñas sólidas elevan la seguridad y contribuyen a proteger los recursos frente a los intentos de inicio de sesión no autorizados. Puede editar una directiva de contraseñas para definirla o seleccionar valores con una gama de características.

Para empezar a trabajar con directivas de contraseñas, elija Seguridad en el menú principal y después Directivas.

Para editar una directiva de contraseñas, selecciónela en la lista Directivas. Para crear una directiva de contraseñas, elija Directiva de calidad de cadena en la lista de opciones Nuevo.

Nota – Para obtener más información sobre las directivas, consulte "Configuración de directivas de Identity Manager" en la página 101.

Creación de directivas

Las directivas de contraseñas son el tipo predeterminado de directivas de calidad de cadena. Tras asignarle nombre y una descripción opcional a la nueva directiva, seleccione las opciones y los parámetros de las reglas que la definen.

Reglas sobre longitud

Las reglas sobre longitud determinan el número mínimo y máximo de caracteres que puede tener una contraseña. Seleccione esta opción para habilitar la regla y después introduzca un valor límite para la regla.

Tipo de directiva

Elija uno de los botones de tipo de directiva. Si elige la opción Otra, deberá introducir el tipo en el campo de texto suministrado.

Reglas de tipo de carácter

Las reglas de tipo de carácter determinan el número mínimo y máximo de caracteres de determinados tipos y cifras que pueden incluirse en una contraseña.

Ello incluye:

- El número mínimo y máximo de caracteres alfabéticos, numéricos, mayúsculas, minúsculas y caracteres especiales.
- El número mínimo y máximo de caracteres numéricos incrustados.
- El número máximo de caracteres repetidos y secuenciales.

- El número mínimo de caracteres alfabéticos y numéricos iniciales.

Introduzca una cifra límite para cada regla de tipo de carácter, o bien indique Todos para especificar que todos los caracteres deben ser de ese tipo.

Número mínimo de reglas de tipo de carácter.

También es posible definir el número mínimo de reglas de tipo de carácter que deben aprobar la validación, como ilustra la Figura 3–7. El número mínimo que se debe aprobar es uno. El máximo no puede superar el número de reglas de tipo de carácter que se han habilitado.

Nota – Para definir en el valor máximo el número mínimo que se debe aprobar, introduzca Todos.

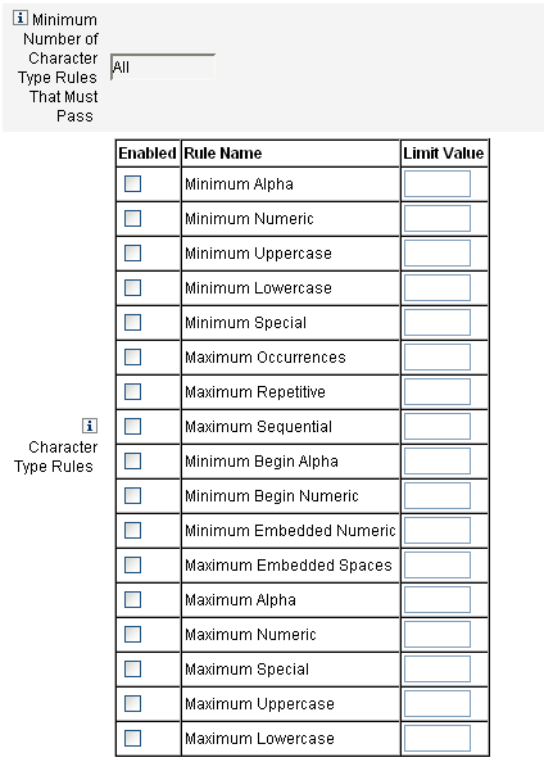


FIGURA 3–7 Reglas de directivas de contraseñas (Tipo de carácter)

Selección de directivas de diccionario

Existe la posibilidad de comprobar las contraseñas con las palabras de un diccionario para protegerse frente a los ataques de diccionario sencillos.

Para poder usar esta opción es preciso:

- Configurar el diccionario
- Cargar palabras del diccionario

El diccionario se configura en la página Directivas. Para obtener más información sobre la configuración del diccionario, consulte "¿Qué es una directiva de diccionario?" en la página 104.

Directiva de historial de contraseñas

Puede prohibir la reutilización de las contraseñas que se han usado justo antes de una contraseñas recién seleccionada.

En el campo Número de contraseñas anteriores que no pueden ser reutilizadas, introduzca un número mayor que 1 para prohibir la reutilización de las contraseñas actual y anterior. Por ejemplo, si introduce 3, la nueva contraseña no puede ser igual que la actual contraseña o las dos contraseñas utilizadas inmediatamente antes.

También se puede prohibir la reutilización de caracteres similares de contraseñas ya usadas. En el campo Número máximo de caracteres similares de contraseñas anteriores que no pueden volver a utilizarse, escriba el número de caracteres consecutivos de las contraseñas anteriores que no pueden repetirse en la nueva contraseña. Por ejemplo, si escribe un valor de 7 y la contraseña anterior era 'password1', la nueva contraseña no puede ser 'password2' o 'password3'.

Si escribe un valor 0, todos los caracteres deberán ser diferentes, sea cual sea la secuencia. Por ejemplo, si la contraseña anterior era abcd, la nueva contraseña no puede incluir los caracteres a, b, c ni d.

La regla puede aplicarse a una o varias contraseñas anteriores. El número de contraseñas anteriores comprobadas es el número especificado en el campo 'Número de contraseñas anteriores que no pueden volver a utilizarse'.

No debe contener palabras

Puede introducir una o más palabras que no puede contener la contraseña. Escriba una palabra en cada línea del cuadro de entrada.

También se pueden excluir palabras configurando e implementando la directiva de diccionario. Para obtener más información, consulte "¿Qué es una directiva de diccionario?" en la página 104.

No debe contener atributos

Puede introducir uno o más atributos que no puede contener la contraseña.

Puede especificar los siguientes atributos:

- `accountID`
- `email`
- `firstname`
- `fullname`
- `lastname`

Puede cambiar el conjunto de atributos “no debe contener" en el objeto de configuración `UserUIConfig`. Para obtener más información, consulte “No debe contener atributos en directivas” en la página 104.

Implementación de directivas de contraseñas

Las directivas de contraseñas se establecen para cada recurso. Para implementar una directiva de contraseñas para un recurso específico, selecciónelo en la lista de opciones Directiva de contraseñas, que se halla en el área Configuración de directivas de las páginas Parámetros del asistente de creación o edición de recursos: Identity Manager.

Autenticación de usuarios

Si un usuario olvida su contraseña o si ésta se reinicializa, puede responder a una o varias preguntas de autenticación para obtener acceso a Identity Manager. El administrador establece estas preguntas y las reglas por las que se rigen, dentro de la directiva de cuentas de Identity Manager. A diferencia de las directivas de contraseñas, las directivas de cuentas de Identity Manager se asignan directamente al usuario o a través de la organización que tiene asignada (en las páginas Crear y Editar usuario).

▼ Para configurar la autenticación en una directiva de cuentas

1. **Elija Seguridad en el menú principal y después Directivas.**

2. **Seleccione “Directiva de cuentas de Identity Manager” en la lista de directivas.**

   La selección se autenticación realiza en el área Opciones de directivas de autenticación secundarias de la página.

   Importante. Cuando se configura por primera vez, el usuario debe iniciar la sesión en la interfaz de usuario e introducir las respuestas iniciales a sus preguntas de autenticación. Si no se establecen estas respuestas, el usuario no podrá iniciar la sesión sin contraseña.

La directiva de preguntas de autenticación estipula lo que sucede cuando un usuario pulsa el botón '¿Olvidó su contraseña?' en la página de inicio de sesión o al acceder a la página Modificar mis respuestas. Cada opción se describe dentro de "Autenticación de usuarios" en la página 91.

Opción	Descripción
Todos	Exige que el usuario responda a todas las preguntas personalizadas y definidas en la directiva.
Cualquiera	Identity Manager muestra todas las preguntas personalizadas y definidas en la directiva. Debe indicar cuántas preguntas debe contestar el usuario.
Siguiente	Exige que el usuario responda a todas las posibles preguntas definidas en la directiva la primera vez que inicia una sesión. Si el usuario pulsa el botón '¿Olvidó su contraseña?' durante el inicio de sesión, Identity Manager muestra la primera pregunta. Si el usuario responde de forma incorrecta, Identity Manager presenta la siguiente pregunta, y así sucesivamente, hasta que obtiene la respuesta correcta y permite el inicio de sesión, o bien bloquea la cuenta si se supera el límite especificado de intentos fallidos. Esta directiva no admite preguntas generadas por los usuarios.
Aleatorio	Permite al administrador especificar cuántas preguntas debe responder el usuario. Identity Manager elige y muestra al azar el número especificado de preguntas definidas en la lista de la directiva, así como las definidas por el usuario. El usuario debe responder a todas las preguntas mostradas.
Operación por turnos	Identity Manager selecciona la siguiente pregunta en la lista de preguntas configuradas y asigna dicha pregunta al usuario. La primera pregunta de la lista de preguntas de autenticación se asigna al primer usuario, y la segunda se asigna al segundo usuario. Este patrón se sigue aplicando hasta que se supera el número de preguntas. A partir de entonces, las preguntas se asignan a los usuarios por orden consecutivo. Por ejemplo, si hay 10 preguntas, la primera pregunta se asigna al 11º y al 21º usuario. Sólo se muestra la pregunta seleccionada. Si prefiere que el usuario responda cada vez a una pregunta distinta, utilice la directiva Aleatorio y defina el número de preguntas en 1. Si prefiere que el usuario responda a una pregunta distinta cada vez, utilice la directiva Aleatorio y defina el número de preguntas en 1. Para obtener más información sobre esta función, consulte "Preguntas de autenticación personalizadas" en la página 93.

Si desea comprobar las opciones de autenticación, inicie la sesión en la interfaz de usuario de Identity Manager, pulse el botón '¿Olvidó su contraseña?' y responda a las preguntas que aparezcan.

La Figura 3–8 ilustra un ejemplo de la pantalla de autenticación de cuentas de usuario.

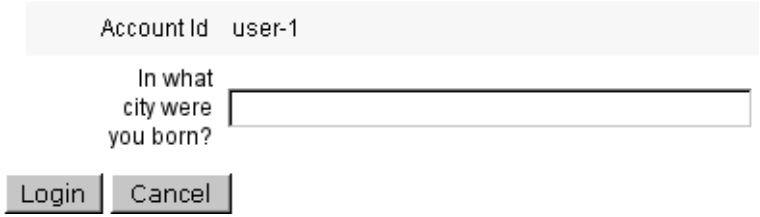


FIGURA 3–8 Autenticación de cuenta de usuario

Preguntas de autenticación personalizadas

En la directiva de cuentas de Identity Manager se puede seleccionar una opción que permite a los usuarios definir sus propias preguntas de autenticación en las interfaces de usuario o de administración. También es posible definir el número mínimo de preguntas que el usuario debe suministrar y contestar para iniciar la sesión usando preguntas de autenticación personalizadas.

De esta forma, los usuarios pueden añadir y cambiar respuestas en la página Cambiar las respuestas a las preguntas de autenticación. La Figura 3–9 muestra un ejemplo al respecto.

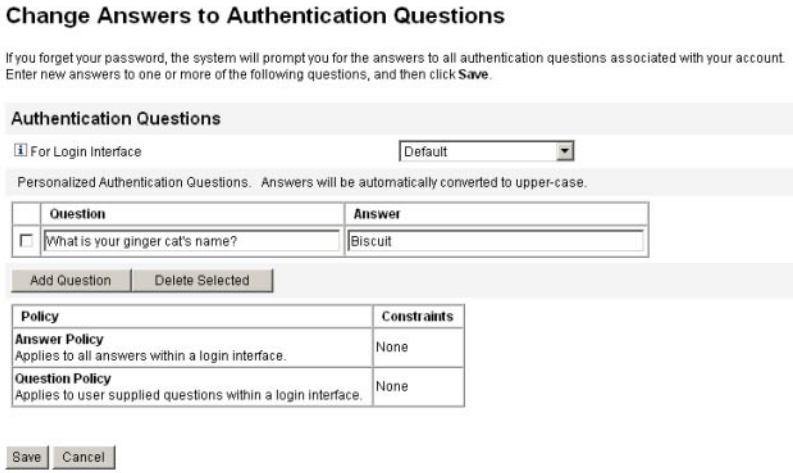


FIGURA 3–9 Cambiar las respuestas a preguntas de autenticación personalizadas

Elusión del desafío de cambio de contraseña tras autenticar

Cuando un usuario se autentica correctamente respondiendo a una o varias preguntas, el sistema le plantea un desafío predeterminado para que introduzca una contraseña nueva. No obstante, es posible configurar Identity Manager para eludir el desafío de cambio de contraseña definiendo la propiedad de configuración del sistema `bypassChangePassword` para una o más aplicaciones de Identity Manager.

Encontrará instrucciones para editar el objeto de configuración del sistema en "Edición de objetos de configuración de Identity Manager" en la página 118.

Para eludir el desafío de cambio de contraseña en todas las aplicaciones tras una autenticación correcta, defina la propiedad `bypassChangePassword` como se indica a continuación en el objeto de configuración del sistema.

EJEMPLO 3–2 Definición del atributo para eludir el desafío de cambio de contraseña

```
<Attribute name="ui"
 <Object>
   <Attribute name="web">
     <Object>
       <Attribute name='questionLogin'>
         <Object>
           <Attribute name='bypassChangePassword'>
             <Boolean>true</Boolean>
           </Attribute>
         </Object>
       </Attribute>
   ...
 </Object>
...
```

Para inhabilitar este desafío de contraseña en una aplicación concreta, configúrelo como sigue.

EJEMPLO 3–3 Definición del atributo para inhabilitar el desafío de cambio de contraseña

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='user'>
          <Object>
            <Attribute name='questionLogin'>
              <Object>
                <Attribute name='bypassChangePassword'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
         </Object>
       </Attribute>
     ...
  </Object>
...
```

Asignación de privilegios administrativos

Puede asignar privilegios administrativos o capacidades de Identity Manager a los usuarios así:

- Roles de administrador (Admin). Los usuarios que tienen asignado un rol de administrador heredan las capacidades y las organizaciones controladas definidas en el rol. De manera predeterminada, a todas las cuentas de usuario de Identity Manager se les asigna el `rol de administrador de usuarios` al crearlas. Encontrará información detallada sobre los roles de administrador y su creación dentro de "Conceptos y administración de recursos de Identity Manager" en la página 160 en el Capítulo 5, "Roles y recursos".
- Capacidades. Las capacidades están definidas por reglas. Identity Manager proporciona grupos de capacidades funcionales que se pueden seleccionar. La asignación de capacidades aumenta la granularidad al asignar privilegios administrativos. Para obtener más información sobre las capacidades y su creación, consulte "Conceptos y administración de capacidades" en la página 216 en el Capítulo 6, "Administración".
- Organizaciones controladas. Las organizaciones controladas conceden privilegios de control administrativos en las organizaciones especificadas. Para obtener más información, consulte "Qué son las organizaciones en Identity Manager" en la página 209 en el Capítulo 6, "Administración".

Para obtener más información sobre los administradores de Identity Manager y las tareas administrativas, consulte el Capítulo 6, "Administración".

Descubrimiento automático

La interfaz de usuario final de Identity Manager permite a los usuarios finales *descubrir* las cuentas de recursos. Esto significa que un usuario que tenga una identidad de Identity Manager puede asociarla a una cuenta de recursos existente pero no asociada.

Habilitación del descubrimiento automático

Para habilitar el descubrimiento automático, es preciso editar un objeto de configuración especial (EndUserResources) y agregarlo al nombre de cada recurso donde se desee que el usuario pueda descubrir cuentas.

▼ Para habilitar el descubrimiento automático

1 **Edite el objeto de configuración "EndUserResources".**

Encontrará instrucciones para editar objetos de configuración de Identity Manager en "Edición de objetos de configuración de Identity Manager" en la página 118.

2 **Añada <String>*Recurso* </String>, donde *Recurso* es el nombre de un objeto de recurso del depósito, como muestra la Figura 3–10.**

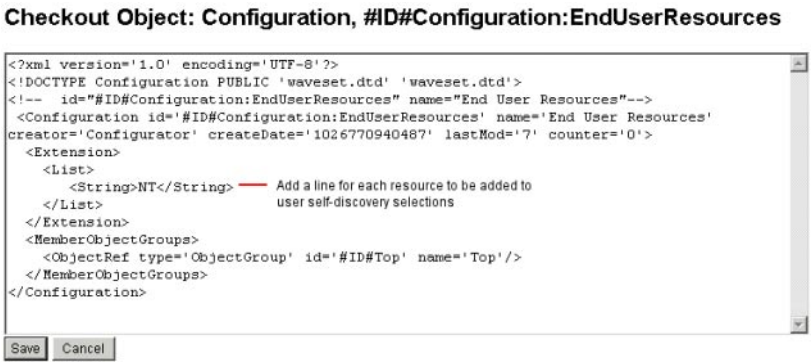


FIGURA 3–10 Objeto de configuración "EndUserResources"

3 **Pulse Guardar.**

Cuando el descubrimiento automático está habilitado, se muestra una nueva opción al usuario dentro de la ficha de menú Perfil en la interfaz de usuario de Identity Manager (Self Discovery). En este área, el usuario puede seleccionar un recurso en una lista y después introducir el ID de cuenta y una contraseña para vincular la cuenta a su identidad de Identity Manager.

Nota – Los administradores también pueden utilizar la organización de usuario final para proporcionar a los usuarios finales acceso a los objetos de configuración de Identity Manager. Encontrará más información en "La organización de usuario final" en la página 231.

Registro anónimo

La función de registro anónimo permite que un usuario que no tiene cuenta en Identity Manager la obtenga solicitándola.

Habilitación del registro anónimo

La función de registro anónimo está inhabilitada de manera predeterminada.

▼ Para habilitar la función de registro anónimo

1 **En la interfaz de administración, seleccione Configurar y después Interfaz de usuario.**

2 **En el área Registro anónimo, seleccione la opción Habilitar y pulse Guardar.**

Cuando un usuario inicie la sesión en la interfaz de usuario, la página de inicio de sesión mostrará el texto ¿Es la primera vez que es usuario? seguido de un vínculo Solicitar cuenta.

Nota – La solicitud de cuenta con ¿Es la primera vez que es usuario? es personalizable. Encontrará información detallada en *Sun Identity Manager Deployment Guide*.

FIGURA 3–11 Página de la interfaz de usuario con el vínculo "Solicitar cuenta" habilitado.

Configuración del registro anónimo

En el área Registro anónimo de la página de la interfaz de usuario, puede configurar las siguientes opciones para el proceso de registro anónimo:

- **Plantilla de notificación**. Especifique el ID de una plantilla de correo electrónico que servirá para enviar notificaciones al usuario solicitante de una cuenta.
- **Exigir normas de privacidad**. Si se selecciona, el usuario debe aceptar las normas de privacidad antes de solicitar una cuenta. Está activada de forma predeterminada.
- **Habilitar validación**. Si se selecciona, el usuario debe validar su cargo para poder solicitar una cuenta. Está activada de forma predeterminada.

- **URL de inicio de proceso**. Introduzca una dirección URL para especificar el flujo de trabajo que se utilizará en el proceso de registro anónimo.
- **Habilitar notificaciones**. Si se selecciona, se notificará al usuario por correo electrónico cuando se cree su cuenta.
- **Dominio de correo electrónico**. Introduzca el nombre del dominio de correo electrónico empleado para generar la dirección de correo electrónico del usuario.

Pulse Guardar cuando termine.

Proceso de registro de usuarios

Cuando un usuario inicia la sesión en la interfaz de usuario, puede solicitar una cuenta pulsando Solicitar cuenta en la página de inicio de sesión.

Identity Manager muestra las dos primeras páginas de registro, donde se solicita el nombre, los apellidos y el ID de empleado. Si el atributo Habilitar validación está definido en sí (valor predeterminado), esta información deberá validarse para que el usuario pueda pasar a la siguiente página.

Las reglas `verifyFirstname`, `verifyLastname`, `verifyEmployeeId` y `verifyEligibility` de `EndUserLibrary` validan la información de cada atributo.

Nota – Quizá tenga que modificar alguna de estas reglas. En concreto, conviene modificar la regla que verifica el ID de empleado de manera que se use una llamada a servicios web o una clase de Java para comprobar la información.

Si el atributo Habilitar validación está inhabilitado, no aparecerá la página de registro inicial. En tal caso, deberá modificar el formulario de registro de usuario final anónimo para que el usuario puede introducir información que normalmente se captura en el formulario de validación inicial.

A partir de la información suministrada en la página Registro, Identity Manager genera:

- Un ID de cuenta (siguiendo la convención: inicial de nombre, inicial de apellido, ID de cuenta).
- Una dirección de correo electrónico con el formato:

  Nombre. *Apellido*@*DominioCorreoE*

  Donde *DominioCorreoE* es el dominio establecido por el atributo Dominio de correo electrónico en la configuración de registro anónimo.
- El atributo de administrador (`idmManager`). Este atributo puede definirse modificando la regla `EndUserRuleLibrary:getIdmManager`. El administrador definido de manera predeterminada es Configurator. El administrador designado como "Manager" debe aprobar la solicitud del usuario para que se pueda abastecer su cuenta.

- El atributo de organización. Este atributo puede definirse personalizando la regla `EndUserRuleLibrary:getOrganization`. Los usuarios se asignan de manera predeterminada a la organización superior de la jerarquía (“Top”).

Si la información suministrada por el usuario en la página Registro se valida correctamente, Identity Manager presenta al usuario la segunda página de registro. En ella deberá introducir una contraseña y su confirmación. Si el atributo Exigir aceptación de directiva de privacidad está definido en sí, el usuario también deberá seleccionar una opción para aceptar los términos de la directiva de privacidad.

Cuando el usuario hace clic en Registrarse, Identity Manager presenta una página de confirmación. Si el atributo Habilitar notificaciones está definido en sí, la página indica que el usuario recibirá una notificación por correo electrónico cuando se haya creado la cuenta.

La cuenta se crea una vez terminado el proceso estándar de creación de usuario (que incluye las aprobaciones exigidas por el atributo `idmManager` y la configuración de la directiva).

◆ ◆ ◆ CAPÍTULO 4

Configuración de objetos de administración de negocio

Este capítulo contiene información y procedimientos para configurar y mantener Identity Manager mediante la interfaz de administración. Para obtener más información sobre los objetos de Identity Manager, consulte "Objetos de Identity Manager" en la página 27 en el capítulo Introducción.

Nota – Encontrará información para configurar Identity Manager en una implementación de proveedor de servicios en el Capítulo 17, "Administración de Service Provider".

Este capítulo consta de los temas siguientes:

Configuración de directivas de Identity Manager

En esta sección encontrará información para configurar las directivas de usuario.

Se tratan los temas siguientes:

¿Qué son las directivas?

Las directivas de Identity Manager establecen limitaciones para los usuarios de Identity Manager mediante la definición de restricciones sobre sus características de ID de cuenta, inicio de sesión y contraseña.

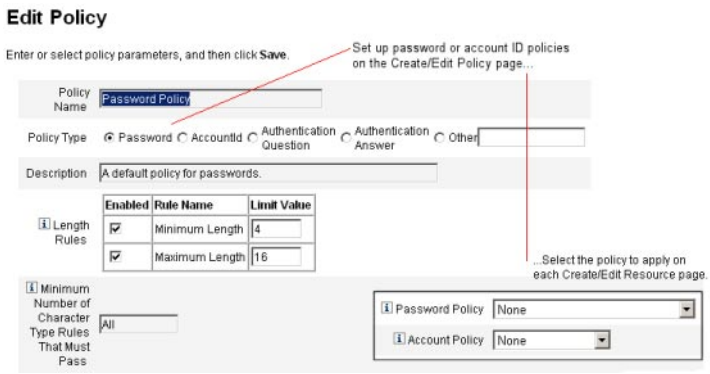
Nota – Identity Manager también ofrece directivas de auditoría ideadas específicamente para auditar el cumplimiento de los usuarios. Las directivas de auditoría se trata en el Capítulo 13, "Auditoría de identidades: Conceptos básicos"

Las directivas se clasifican en los tipos siguientes:

- **Directivas de cuentas de Identity System**. Definen opciones y restricciones de directivas de usuario, contraseña y autenticación. Las directivas de cuentas de Identity System se asignan a las organizaciones en las páginas Crear y Editar organización, o a los usuarios en las páginas Crear y Editar usuarios.

  Puede configurar o seleccionar las siguientes opciones:

  - **Opciones de directivas de cuenta de usuario**. Especifique cómo trata las cuentas de usuario Identity Manager si un usuario no responde correctamente a las preguntas de autenticación.
  - **Opciones de directivas de contraseña**. Puede definir las opciones de caducidad de la contraseña, tiempo de advertencia antes de que caduque y reinicialización.
  - **Opciones de directivas de autenticación secundarias**. Permiten especificar cómo se presentan las preguntas de autenticación al usuario, si éste puede aportar sus propias preguntas de autenticación, imponer la necesidad de autenticación al iniciar la sesión y establecer el conjunto de preguntas que pueden plantearse a un usuario.
- **Directiva de cuentas de sistema de Service Provider**. Este tipo de directiva se aplica en una implementación de proveedor de servicios para definir opciones y restricciones de usuario, contraseña y directiva de autenticación para los usuarios del proveedor de servicios. Las directivas se asignan a las organizaciones en las páginas Crear y Editar organización, o a los usuarios en las páginas Crear y Editar usuario de Service Provider.
- **Directivas de calidad de cadena**. Son tipos de directivas como las de contraseña, Id de cuenta y autenticación. Sirven para definir reglas de longitud y de tipo de caracteres, palabras permitidas y valores de atributo. Este tipo de directiva va ligado a cada recurso de Identity Manager y se configura en la página de cada recurso. La figura siguiente ofrece un ejemplo al respecto.



Es posible definir las siguientes opciones y reglas para las contraseñas e ID de cuenta:

- **Reglas sobre longitud**. Determinan la longitud máxima y mínima.
- **Reglas de tipo de carácter**. Establecen el número mínimo y máximo permitidos de caracteres alfabéticos, numéricos, mayúsculas, minúsculas, repetitivos y secuenciales.
- **Límites de reutilización de contraseñas** Especifican el número de contraseñas anteriores a la actual que no pueden reutilizarse. Cuando un usuario intenta cambiar su contraseña, la nueva se coteja con el historial de contraseñas para asegurarse de que sea única. Por razones de seguridad, se guarda una firma digital de la contraseña anterior, con la que se comparan las contraseñas nuevas.
- **Palabras y valores de atributo prohibidos**. Especifique las palabras y atributos que no pueden incluirse en un ID o una contraseña.

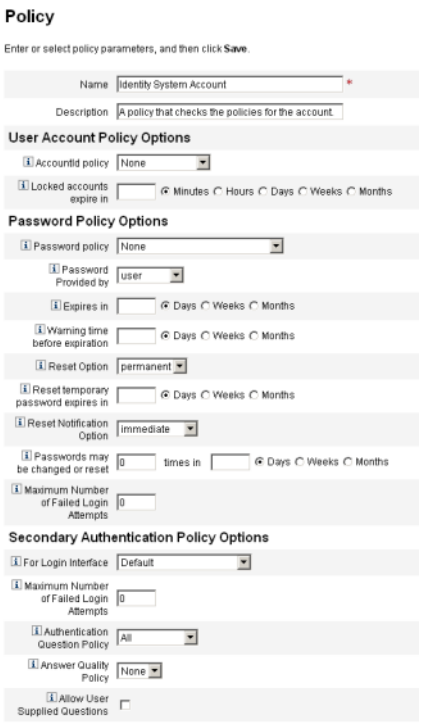
▼ Para abrir la página Directivas

Se pueden crear y editar directivas de usuario de Identity Manager en la página Directivas. Para abrir esta página, siga estos pasos:

1 **Inicie la sesión en la interfaz de administración.**

2 **Seleccione la ficha Seguridad y después la ficha secundaria Directivas.**

Aparece la página Directivas, ilustrada en la figura siguiente.



No debe contener atributos en directivas

Puede cambiar el conjunto de atributos “no debe contener" permitidos en el objeto de configuración `UserUIConfig`.

Los atributos se indican en `UserUIConfig` así:

- Atributo `<PolicyPasswordAttributeNames>`. Tipo de directiva: contraseña.
- Atributo `<PolicyAccountAttributeNames>`. Tipo de directiva: ID de cuenta.
- Atributo `<PolicyOtherAttributeNames>`. Tipo de directiva: otras.

¿Qué es una directiva de diccionario?

Una directiva de diccionario permite a Identity Manager comparar las contraseñas con una base de datos de palabras para asegurarse de que estén protegidas frente a posibles ataques simples de diccionario. Si se utiliza esta directiva con otras preferencias de directiva para asegurar la longitud y formación de las contraseñas, Identity Manager dificulta el uso de un diccionario para averiguar las contraseñas generadas o cambiadas en el sistema.

La directiva de diccionario amplía la lista de exclusión de contraseñas que se puede configurar con la directiva. (Esta lista se implementa con la opción "No debe contener palabras" de la página de edición de directivas de contraseña de la interfaz de administración.)

▼ Para configurar una directiva de diccionario

Para configurar una directiva de diccionario, es preciso:

- Configurar el soporte de servidor del diccionario.
- Cargar el diccionario.

1 Abra la página Directivas como se explica en "Para abrir la página Directivas" en la página 103

2 Seleccione Configurar diccionario para acceder a la página Configuración del diccionario.

3 Seleccione e introduzca la información sobre la base de datos.

La información sobre la base de datos incluye:

- **Tipo de base de datos**. Seleccione el tipo de base de datos (Oracle, DB2, SQLServer o MySQL) que utilizará para almacenar el diccionario.
- **Host**. Introduzca el nombre de host en el que se está ejecutando la base de datos.
- **Usuario**. Introduzca el nombre de usuario que se utilizará para conectarse a la base de datos.
- **Contraseña**. Introduzca la contraseña que se utilizará para conectarse a la base de datos.
- **Puerto**. Introduzca el puerto en el que la base de datos recibe las consultas.
- **URL de conexión**. Introduzca la dirección URL que se utilizará para la conexión. Están disponibles las siguientes variables de plantilla:
  - `%h` - host
  - `%p` - puerto
  - `%d` – nombre de la base de datos

  Clase del controlador. Introduzca la clase del controlador JDBC que se utilizará al interactuar con la base de datos.
- **Nombre de la base de datos**. Introduzca el nombre de la base de datos en la que se cargará el diccionario.
- **Nombre de archivo del diccionario**. Introduzca el nombre del archivo que se utilizará al cargar el diccionario.

4 Haga clic en Probar para comprobar la conexión de la base de datos.

5 Si se realiza con éxito la prueba de conexión, haga clic en Cargar palabras para cargar el diccionario. es posible que el proceso de carga tarde unos minutos en completarse.

6 Haga clic en Probar para asegurarse de que el diccionario se ha cargado con éxito.

▼ Para implementar una directiva de diccionario

Siga estos pasos para implementar una directiva de diccionario:

1. **Abra la página Directivas como se explica en "Para abrir la página Directivas" en la página 103.**
2. **Seleccione el vínculo Directiva de contraseñas para editar la directiva de contraseñas.**
3. **En la página "Editar directiva", seleccione la opción "Comparar contraseñas con las palabras del diccionario".**
4. **Haga clic en Guardar para guardar los cambios.**

   Una vez implementada, todas las contraseñas generadas y cambiadas se comprobarán en el diccionario.

Personalización de plantillas de correo electrónico

Identity Manager usa plantillas de correo electrónico para suministrar información y solicitudes de acciones a aprobadores y usuarios. El sistema incluye plantillas de:

- **Aviso de revisión de acceso**. Envía un notificación de que es preciso revisar los derechos de acceso de un usuario. El sistema envía esta notificación cuando hace falta remediar o mitigar una infracción de una directiva de acceso.
- **Aprobación de creación de cuenta**. Envía una notificación al aprobador en la que se indica que hay una nueva cuenta que espera su aprobación. El sistema envía esta aprobación cuando se ha definido la opción de notificación de abastecimiento para el rol asociado como aprobación.
- **Notificación de creación de cuenta**. Envía una notificación en la que se indica que se ha creado una cuenta con una asignación de rol específica. El sistema envía esta notificación cuando se seleccionan uno o varios administradores en el campo "Destinatarios de la notificación" en las páginas "Crear rol" o "Editar rol".
- **Aprobación de eliminación de cuenta**. Envía una notificación a un aprobador en la que se indica que hay una acción de eliminación de cuenta de usuario que espera su aprobación. El sistema envía esta notificación cuando se seleccionan uno o varios administradores en el campo "Destinatarios de la notificación" en las páginas "Crear rol" o "Editar rol".
- **Notificación de eliminación de cuenta**. Envía una notificación en la que se indica que se ha eliminado una cuenta.
- **Notificación de actualización de cuenta**. Notifica a las direcciones de correo electrónico o cuentas de usuario especificadas que se ha actualizado una cuenta.
- **Recurso externo**. Notifica a un abastecedor de recursos externos que es necesario realizar una tarea de abastecimiento.

- **Reinicialización de contraseña**. Notifica que se ha reinicializado una contraseña de Identity Manager. En función del valor seleccionado en Opción de notificación de reinicialización para la directiva de Identity Manager asociada, el sistema muestra inmediatamente una notificación (en el explorador web) al administrador que reinicializa la contraseña o envía un mensaje de correo electrónico al usuario cuya contraseña se está reinicializando.
- **Aviso de sincronización de contraseña**. Notifica al usuario que una contraseña se ha cambiado correctamente en todos los recursos. La notificación indica qué recursos se han actualizado correctamente y de dónde procede la solicitud para cambiar la contraseña.
- **Aviso de fallo de flujo de trabajo de sincronización**. Notifica al usuario que la contraseña no se ha cambiado correctamente en todos los recursos. La notificación incluye una lista de los errores e indica de dónde procede la solicitud para cambiar la contraseña.
- **Aviso de infracción de directiva**. Notifica la infracción de una directiva de cuentas.
- **Reconciliar evento de cuenta**. Reconciliar evento de recurso, Resumen de reconciliación. Se activa, respectivamente, desde los flujos de trabajo predeterminados Notificar respuesta de reconciliación, Notificar inicio de reconciliación y Notificar fin de reconciliación. La notificación se envía tal como se ha configurado en cada flujo de trabajo.
- **Informe**. Envía un informe generado a una lista de destinatarios especificados.
- **Solicitud de recurso**. Envía una notificación a un administrador de recursos para informarle de que se ha solicitado un recurso. El sistema envía esta notificación cuando el administrador solicita un recurso en el área "Recursos".

Nota – Los recursos de solicitud han sido rechazados en favor de los recursos externos a partir de la versión 8.1 de Identity Manager. Ya no se pueden crear nuevas conexiones utilizando el adaptador de peticiones. Utilice el adaptador de recursos externos en su lugar. Para obtener más información, consulte "Conceptos y administración de recursos externos" en la página 173.

- **Notificación de reintento**. Envía una notificación a un administrador para informarle de que se ha intentado realizar sin éxito una determinada operación en un recurso un número especificado de veces.
- **Análisis de riesgo**. Envía un informe de análisis de riesgo. El sistema envía este informe cuando se especifican uno o varios destinatarios de correo electrónico como parte de una exploración de recursos.
- **Restablecimiento de contraseña temporal**. Envía una notificación al usuario o al aprobador de roles indicándole que se ha proporcionado una contraseña temporal para la cuenta. En función del valor seleccionado en la opción de notificación de reinicialización de contraseña para la directiva de Identity Manager asociada, el sistema muestra inmediatamente una notificación al usuario (en el explorador web) o envía un mensaje de correo electrónico al usuario o a los aprobadores de roles.

- **Recuperar ID de usuario**. Envía un ID de usuario recuperado a la dirección de correo electrónico especificada.

Edición de plantillas de correo electrónico

Las plantillas de correo electrónico se pueden personalizar para dar instrucciones concretas a los destinatarios, indicándoles cómo realizar una tarea o ver resultados. Por ejemplo, es posible que desee personalizar la plantilla de aprobación de creación de cuenta para enviar a un aprobador a una página de aprobación de cuentas con el mensaje:

```
Vaya a http://host.example.com:8080/idm/approval/approval.jsp para aprobar la
creación de una cuenta para $(fullname).
```

Siga el procedimiento indicado a continuación para personalizar una plantilla de correo electrónico tomando como ejemplo la plantilla Aprobación de creación de cuenta.

▼ Para personalizar una plantilla de correo electrónico

1. **En la interfaz de administración, seleccione la ficha Configurar y después la ficha secundaria Plantillas de correo electrónico.**

   Aparece la página Plantillas de correo electrónico.

2. **Seleccione la plantilla Aprobación de creación de cuenta.**

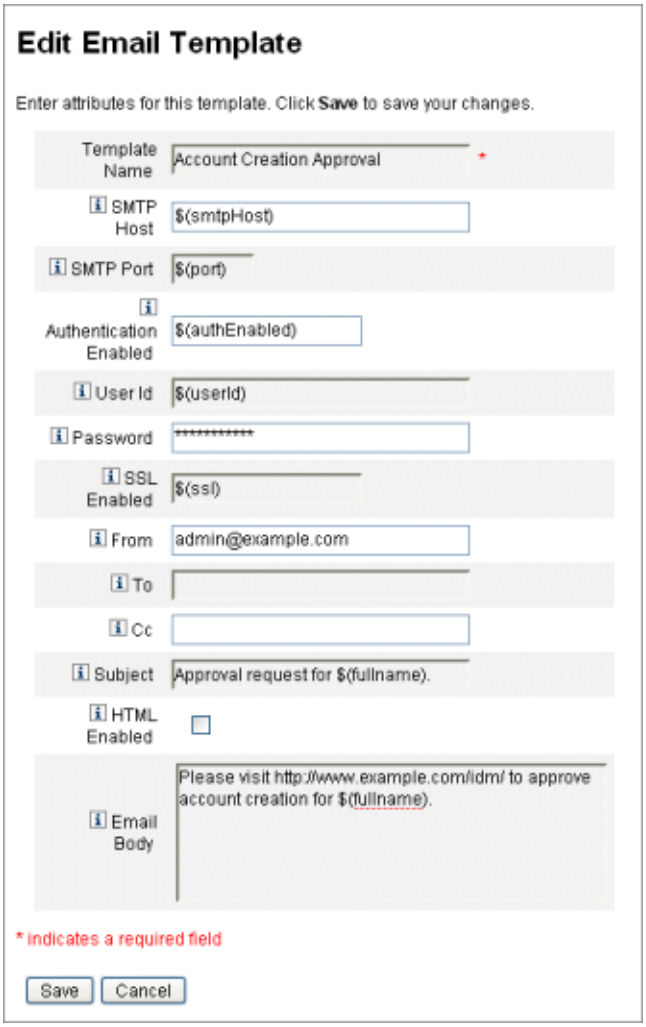


FIGURA 4–1 Edición de plantillas de correo electrónico

3 Introduzca información para la plantilla.

Puede introducir la información siguiente:

- En el campo Host SMTP, escriba el nombre del servidor SMTP para poder enviar la notificación de correo electrónico.
- En el campo De, personalice la dirección de correo electrónico originaria.
- En los campos Para y CC, escriba una o varias direcciones de correo electrónico o cuentas de Identity Manager a las que se deba destinar la notificación.

- En el campo Cuerpo del mensaje de correo electrónico, personalice el texto incluyendo un puntero a su ubicación de Identity Manager.

4 **Pulse Guardar.**

También es posible modificar las plantillas de correo electrónico con Sun Identity Manager Integrated Development Environment (Identity Manager IDE). Encontrará información sobre Identity Manager IDE en el sitio web: `https://identitymanageride.dev.java.net/`.

Nota – Es necesario registrarse e iniciar la sesión en este sitio.

HTML y vínculos en las plantillas de correo electrónico

Puede introducir contenido con formato HTML en una plantilla de correo electrónico para mostrarlo en el cuerpo del mensaje. Este tipo de contenido puede incluir texto, gráficos y enlaces Web a la información. Para habilitar contenido en formato HTML, seleccione la opción HTML habilitada.

Variables permitidas en el texto del mensaje de correo electrónico

En el cuerpo de la plantilla de correo electrónico también se pueden incluir referencias a variables, con la sintaxis `$(`*Nombre*`)`; por ejemplo: `Su contraseña $(contraseña) ha sido reinicializada.`

En la tabla se enumeran las variables permitidas en cada plantilla.

.

TABLA 4–1 Variables de plantillas de correo electrónico

Plantilla	Variables permitidas
Reinicialización de contraseña	`$(password)`: contraseña recién generada
Aprobación de actualización	`$(fullname)`: nombre completo del usuario
	`$(role)`: rol del usuario
Notificación de actualización	`$(fullname)`: nombre completo del usuario
	`$(role)`: rol del usuario

TABLA 4–1 Variables de plantillas de correo electrónico *(Continuación)*

Plantilla	Variables permitidas
Informe	`$(report)`: informe generado
	`$(id)`: ID cifrado de la instancia de la tarea
	`$(timestamp)`: hora a la que se envió el correo electrónico
Solicitud de recurso	`$(fullname)`: nombre completo del usuario
	`$(resource)`: tipo de recurso
Análisis de riesgo	`$(report)`: informe de análisis de riesgo
Restablecimiento de contraseña temporal	`$(password)`: contraseña recién generada
	`$(expiry)`: fecha de caducidad de la contraseña

Configuración de grupos y eventos de auditoría

Configurar grupos de auditoría le permite registrar e informar sobre los eventos del sistema que seleccione. También le sirve para ejecutar informes de registro de auditoría posteriormente.

▼ Para abrir la página Configuración de auditoría

En la página Configuración de auditoría se configuran los grupos de auditoría. Para abrir la página Configuración de auditoría, siga estos pasos:

1. **Abra la interfaz de administración.**
2. **Seleccione la ficha Configurar y después la ficha secundaria Auditoría.**

   Aparece la página Configuración de auditoría.

▼ Para configurar grupos de auditoría

Para configurar de grupos y eventos de auditoría se necesita la capacidad administrativa Configurar auditorías.

1. **Abra la página Configuración de auditoría como se explica en el apartado anterior.**

   La página Configuración de auditoría muestra la lista de grupos de auditoría, cada uno de los cuales puede contener uno o varios eventos. Es posible registrar los eventos correctos, fallidos o ambos para cada grupo.

2 **Seleccione un grupo de auditoría en la lista para acceder a la página Editar grupo de configuración de auditoría. En esta página se seleccionan los tipos de eventos de auditoría que se van a registrar como parte del grupo de configuración de auditoría en el registro de auditoría del sistema.**

3 **Asegúrese de que esté marcada la casilla de verificación Habilitar auditoría. Desactive la casilla para inhabilitar el sistema de auditoría.**

Nota – Para obtener más información sobre las grupos de auditoría, consulte "Configuración de auditoría" en la página 346 en el Capítulo 10, "Registro de auditoría".

▼ Para agregar eventos al grupo de configuración de auditoría

Siga estos pasos para agregar un evento al grupo:

1 **Pulse Nuevo.**

Identity Manager añade un evento al final de la página.

2 **Seleccione un tipo de objeto de la lista de la columna Tipo de objeto y, después, mueva uno o más elementos del área Disponibles de la columna Acciones al área Seleccionados para el nuevo tipo de objeto.**

3 **Pulse Aceptar para añadir el evento al grupo.**

▼ Para editar eventos en el grupo de configuración de auditoría

Puede editar eventos en un grupo añadiendo o eliminando acciones para un tipo de objeto, así:

1 **Traslade los elementos de la columna Acciones desde el área Disponible hasta el área Seleccionado correspondiente a ese tipo de objeto.**

2 **Haga clic en Aceptar.**

Integración de Remedy

Identity Manager puede integrarse con un servidor de Remedy, lo que le permitirá enviar tickets de Remedy según una plantilla especificada.

La integración de Remedy se configura en dos áreas de la interfaz de administración:

- **Parámetros del servidor de Remedy**. La configuración de Remedy se lleva a cabo creando un recurso de Remedy en el área Recursos. (Consulte "Administración de la lista de recursos" en la página 161.) Un vez configurado el recurso, compruebe la conexión para asegurarse de que la integración está habilitada.
- **Plantilla de Remedy**. Una vez configurado el recurso de Remedy, defina una plantilla de Remedy. Para ello, abra la interfaz de administración, seleccione la ficha Configurar y después Integración de Remedy. A continuación deberá seleccionar el esquema y el recurso de Remedy.

La creación de tickets de Remedy se configura mediante el flujo de trabajo de Identity Manager. Según sus preferencias, puede efectuar una llamada en el momento adecuado utilizando la plantilla definida para abrir un ticket de Remedy. Para obtener más información sobre la configuración de flujos de trabajo, consulte el Capítulo 1, "Workflow" de *Sun Identity Manager Deployment Reference*.

Configuración de la interfaz de usuario final

Los administradores pueden configurar ciertos aspectos de la interfaz de usuario final modificando un formulario en la interfaz de administración.

▼ Para definir opciones para mostrar información en la interfaz de usuario final

1. **En la interfaz de administración, seleccione Configurar en el menú principal.**
2. **Elija Interfaz de usuario en el menú secundario.**

   Aparece la página Interfaz de usuario.
3. **Rellene y guarde el Panel de usuario final del formulario. Haga clic en Ayuda si necesita ayuda con el formulario.**

   Encontrará información para rellenar el Registro anónimo del formulario en "Registro anónimo" en la página 96.

▼ Para habilitar los diagramas de proceso en la interfaz de usuario final

Los diagramas de proceso reflejan el flujo de trabajo que sigue Identity Manager cuando los usuarios finales inician una solicitud o actualizan sus perfiles. Si están habilitados, los diagramas de proceso aparecen en la página de resultados después de que el usuario final haya enviado un formulario.

Los diagramas de proceso deben habilitarse en la interfaz de administrador para poder habilitarse en la interfaz de usuario final. Para obtener más información, consulte "Habilitación de diagramas de proceso" en la página 58.

1. **Abra la página de configuración de la interfaz de usuario siguiendo los pasos de "Configuración de la interfaz de usuario final" en la página 113.**
2. **Seleccione la opción Habilitar diagramas de proceso de usuario final, que se encuentra en la sección Páginas de resultado del formulario.**

   Si la opción Habilitar diagramas de proceso de usuario final no está disponible, primero deberá habilitar los diagramas de proceso en la interfaz de administración. Consulte "Habilitación de diagramas de proceso" en la página 58.
3. **Pulse Guardar.**

Registro de Identity Manager

Se recomienda a los administradores que registren su instalación de Identity Manager.

Para registrarse hace falta una cuenta y una contraseña en Sun Online. Si no tiene una cuenta de Sun Online, puede registrarse rellenando el formulario en esta dirección:

`https://reg.sun.com/register`

Identity Manager puede registrarse desde la consola o mediante la interfaz de administración.

Registrarse desde la consola permite crear también una etiqueta de servicio local, que puede usarse con software Sun Service Tag para seguimiento de inventario de sistemas, software y servicios de Sun. El paquete de cliente de etiquetas de servicio debe instalarse antes de crear una etiqueta de servicio local. Para descargar este paquete, puede pulsar el botón Download Service Tags en la dirección:

`http://inventory.sun.com/inventory`

Para registrar Identity Manager, debe iniciar la sesión con una cuenta de administrador que le permita configurar objetos de Identity Manager. Esta cuenta debe tener la capacidad Registro del producto. Para obtener información sobre las capacidades, consulte "Asignación de capacidades a usuarios" en la página 219.

Nota – Para que la función de registro del producto funcione, debe tener Java correctamente configurado para SSL en los servidores de aplicaciones de Identity Manager. Todos los archivos JAR referenciados en el archivo `java.security` (o equivalente) deben estar presentes.

En resto de esta sección contiene información e instrucciones para registrar Identity Manager. Esta información se ha dividido en los temas siguientes:

Registro de Identity Manager desde la consola

En este apartado encontrará información necesaria para registrar Identity Manager desde la consola.

Con el comando `register`

Para registrar Identity Manager desde la consola se utiliza el comando `register`. A continuación se explica cómo utilizar dicho comando.

Uso del comando `register`

```
register -local
register -remote [-u <userid> [-p <password>]] [-prompt] -userSOA <userid>
-passSOA <password> [-proxy <proxyHost> [-port <proxyPortNumber>]]
register [-help | -?]
```

Opciones del comando `register`

En la tabla siguiente se describen las opciones que se pueden usar con el comando `register`.

TABLA 4–2 Opciones del comando

Opción	Descripción
`-local`	Crea una etiqueta de servicio en este host.

TABLA 4–2 Opciones del comando *(Continuación)*

Opción	Descripción
`-remote`	Registra la instalación de Identity Manager a través de la red directamente con Sun.
`-u <userid>`	El ID de usuario de Identity Manager del administrador Identity Manager que tiene autorización para efectuar el registro.
`-p <password>`	La contraseña de Identity Manager del administrador Identity Manager que tiene autorización para efectuar el registro.
`-prompt`	Solicitud interactiva de la contraseña cuando falta.
`-userSOA <userid>`	Id de usuario de la cuenta de Sun Online que se utilizará para registrar. Es necesario en caso de registrarse con la opción `-remote`.
`-passSOA <password>`	La contraseña de la cuenta de Sun Online que se utilizará para registrar. Es necesario en caso de registrarse con la opción `-remote`.
`-proxy <proxyHost>`	El proxy de red que debe usarse para acceder al servicio de registro online de Sun. Es necesario para registrarse con la opción `-remote` cuando la red está configurada para usar un proxy para conectarse a direcciones de Internet externas.
`-port <proxyPortNumber>`	El puerto del proxy de red que debe usarse para acceder al servicio de registro online de Sun. Es necesario para registrarse con la opción `-remote` cuando la red está configurada para usar un proxy para conectarse a direcciones de Internet externas.
`-help | -?`	Muestra ayuda para este comando en la consola.

▼ Para registrar Identity Manager desde la consola

Para registrar Identity Manager desde la consola debe crear una etiqueta de servicio local o registrarse con Sun a través de Internet. Siga estas instrucciones:

1 Inicie la interfaz de consola (línea de comandos) de Identity Manager.

- En una línea de comandos de Windows, escriba:

  `%WSHOME%\bin\lh`

- En una línea de comandos de UNIX, escriba:

  `$WSHOME/bin/lh`

2 Utilice el comando `register` así:

- Para crear una etiqueta de servicio local,

  `register -local`

- Para registrar Identity Manager por Internet, use este comando:

register -remote -u <*userid***> -p <***password***> -userSOA <***soaUserid***> -passSOA <***soaPassword* **> -proxy <***proxyHost***> -port <** *proxyPortNumber***>**

donde:

- **userid** es el ID de usuario del administrador Identity Manager que tiene autorización para efectuar el registro.
- **password** es la contraseña de Identity Manager del administrador Identity Manager que tiene autorización para efectuar el registro.
- **soaUserid** es el ID de usuario de la cuenta de Sun Online que se utilizará para registrar.
- **soaPassword** es la contraseña de la cuenta de Sun Online que se utilizará para registrar.
- **proxyHost** es el proxy de red que debe usarse para acceder al servicio de registro online de Sun. Sólo es necesario cuando la red está configurada para usar un proxy para conectarse a direcciones de Internet externas.
- **proxyPortNumber** es el puerto del proxy de red que debe usarse para acceder al servicio de registro online de Sun. Sólo es necesario cuando la red está configurada para usar un proxy para conectarse a direcciones de Internet externas.

▼ Para registrar Identity Manager desde la interfaz de administración

Si no necesita crear una etiqueta de servicio local, registre Identity Manager desde la interfaz de administración.

1. **En la interfaz de administración, seleccione Configurar.**
2. **En el menú secundario, elija Registro del producto.**

   Aparece la página Registro del producto.
3. **Rellene el formulario y haga clic en Registrarse ahora. Haga clic en los elementos i-Help para obtener información sobre los distintos campos.**

Nota –

- Si el servidor de aplicaciones no está configurado para permitir conexiones SSL de salida, puede aparecer el mensaje de error siguiente:

  ```
  Failed to register on Sun Connection server
  due to invalid Sun Online Account user/password.
  ```

  Para resolver este problema, incluya los correspondientes certificados raíz acreditados en el almacén de claves del servidor de aplicaciones. Consulte los detalles en la documentación del servidor de aplicaciones.
- Si la ruta de clase del servidor de aplicaciones contiene versiones antiguas de `xml-apis.jar` y `xercesImpl.jar`, quizá reciba este mensaje de error:

  ```
  java.lang.NoSuchMethodError:org.w3c.dom.Node.getTextContent()Ljava/lang/String;
  ```

  Para resolver este problema, modifique la ruta de clase de manera que sólo aparezcan las versiones más recientes de `xml-apis.jar` y `xercesImpl.jar`.

Edición de objetos de configuración de Identity Manager

Mientras administra Identity Manager, a veces se le pedirá que edite el objeto de configuración del sistema de Identity Manager (también denominado archivo de configuración del sistema) u otros objetos similares.

1. **Escriba la URL siguiente en el navegador para abrir la página de depuración de Identity Manager:**

   `http://<`*AppServerHost*`>:<`*Port*`>/idm/debug/session.jsp`

   Aparece la página Configuración del sistema.

   Nota – Para ver las páginas `/idm/debug/` se necesita capacidad de depuración.

2. **Busque el botón List Objects y seleccione Configuration en la lista desplegable Type adyacente.**
3. **Pulse el botón List Objects.**

   Aparece la página List Objects of type: Configuration.
4. **En la lista de objetos, busque el que le interesa y haga clic en edit.**

   Por ejemplo, para editar el objeto de configuración del sistema, busque System Configuration y después haga clic en edit.
5. **Edite el objeto como se indica y haga clic en Save.**

6. **Reinicie el servidor o servidores si así se le indica.**

◆ ◆ ◆ CAPÍTULO 5

Roles y recursos

En este capítulo se tratan los roles y recursos de Identity Manager.

Se ha dividido en los temas siguientes:

Conceptos y administración de roles

En esta sección encontrará información para configurar los roles en Identity Manager. Las asignaciones de recursos basadas en roles simplifican drásticamente la administración de recursos en las organizaciones grandes.

Nota – No hay que confundir los *roles* y los *roles de administrador*. Los roles sirven para gestionar el acceso de los usuarios finales a los recursos externos. En cambio, los roles de administrador se utilizan principalmente para gestionar el acceso del administrador a los objetos internos de Identity Manager, como usuarios, organizaciones y capacidades.

Aquí nos ocuparemos de los roles. Encontrará información sobre los roles de administrador en "Conceptos y administración de roles de admin" en la página 220.

¿Qué son los roles?

Un rol es un objeto de Identity Manager que permite agrupar los derechos de acceso a los recursos y asignarlos eficazmente a los usuarios.

Los roles se organizan en cuatro tipos:

- Roles de negocio
- Roles de TI
- Aplicaciones
- Activos

Los *roles de negocio* sirven para organizar en grupos los derechos de acceso que necesitan las personas que realizan tareas similares en una organización. Los roles de negocio suelen representar funciones de tareas de usuario. Por ejemplo, en una institución financiera, los roles de negocio podrían corresponder a funciones de trabajo como cajero, responsable de préstamos, director de sucursal, secretario, contable o auxiliar administrativo.

Los roles de TI, las aplicaciones y los *activos* organizan los derechos de recursos en grupos. Para proporcionar a los usuarios finales acceso a los recursos, los roles de negocio se asignan a roles de TI, aplicaciones y activos, lo que permite a los usuarios acceder a los recursos que necesitan para realizar sus tareas. Los roles de TI contienen un conjunto específico de aplicaciones, activos o recursos, incluidos derechos concretos sobre los recursos asignados. Los roles de TI también pueden contener otros roles de TI.

Nota – El concepto de tipos de roles nuevo en la versión 8.0 de Identity Manager. Si su organización ha actualizado a esta versión desde otra anterior de Identity Manager, sus roles anteriores se habrán importado como roles de TI. Para obtener más información, consulte "Administración de roles creados en versiones anteriores a la 8.0" en la página 123.

Los roles de TI, las aplicaciones y los activos pueden ser *requeridos, condicionales* u *opcionales.*

- Los roles requeridos se asignan siempre a usuarios finales.
- Los roles condicionales tienen condiciones que deben evaluarse como verdaderas para poder ser asignados.
- Los roles opcionales se pueden solicitar por separado y, una vez aprobados, asignar a los usuarios finales.

Los roles requeridos, condicionales y opcionales permiten a un diseñador de roles de negocio definir un acceso genérico a los roles contenidos para cumplir las normativas, dejando flexibilidad al administrador para definir con precisión los derechos de acceso del usuario final. Los usuarios que tienen asignados roles condicionales u opcionales pueden compartir el mismo rol de negocio asignado, pero tienen asignados derechos de acceso distintos. Así no hace falta definir un nuevo rol de negocio cada vez que cambian las necesidades de acceso dentro de la organización (problema que se conoce como *explosión de roles).*

Uso práctico de los roles

A continuación se explica cómo usar los roles con eficacia. Los tipos de roles se describen en la sección anterior.

Administración de roles creados en versiones anteriores a la 8.0

En las organizaciones que han actualizado desde versiones de Identity Manager anteriores a la 8.0, sus roles anteriores se convertirán automáticamente en roles de TI. Estos roles de TI permanecerán asignados directamente a los usuarios. En el proceso de actualización no se asignará ningún propietario de roles a los roles anteriores, aunque sí es posible asignárselo después. (Encontrará información sobre los propietarios de roles en "Designación de propietarios y aprobadores de roles" en la página 134.)

De manera predeterminada, las organizaciones que actualizan a la versión 8.0 pueden asignar a los usuarios directamente tanto roles de TI como de negocio (consulte la Figura 5–2).

A las organizaciones que tienen roles anteriores quizá les interese crear nuevos roles con las instrucciones indicadas en la próxima sección.

Uso de tipos de roles para diseñar roles flexibles

Los roles de TI, aplicaciones y activos son las piezas fundamentales de los diseñadores de roles. Estos tres tipos de roles se combinan para confeccionar derechos de usuario (o *derechos de acceso*). Después, los roles de TI, aplicaciones y activos se asignan a roles de negocio.

Diseño de roles de negocio

En Identity Manager, a un usuario se le puede asignar un rol, varios o ninguno. Con la introducción de los tipos de roles en Identity Manager 8.0, se recomienda sólo asignar directamente roles de negocio a los usuarios. De manera predeterminada, no es posible asignar directamente ningún otro tipo de rol a los usuarios, salvo que previamente se tuviera instalada una versión de Identity Manager anterior y se haya actualizado a la versión 8.0. Esta restricción predeterminada se puede cambiar modificando el objeto de configuración de rol ("Configuración de tipos de roles" en la página 155).

Para evitar mayor complejidad, los roles de negocio no pueden anidarse. Es decir, un rol de negocio no puede contener a su vez otros roles de negocio. Además, los roles de negocio no pueden contener directamente recursos ni grupos de recursos. En vez de ello, los recursos y grupos de recursos deben asignarse a un rol de TI o una aplicación, que entonces pueden asignarse a uno o más roles de negocio.

Diseño de roles de TI

Los roles de TI pueden contener aplicaciones, activos y otros roles de TI. Los roles de TI también pueden contener recursos y grupos de recursos.

Los roles de TI deben ser creados y administrados por el personal de TI de la organización o por los propietarios del recurso que conocen los derechos necesarios para habilitar privilegios concretos dentro del recurso.

Diseño de aplicaciones y activos

Las aplicaciones y activos son tipos de roles concebidos para representar términos de negocio habituales descriptivos de lo que necesitan los usuarios finales para realizar sus trabajos. Por ejemplo, un rol de aplicación podría denominarse “Herramientas de atención al cliente” o “Herramienta admin. HHRR Intranet“.

- Las aplicaciones no pueden contener roles, pero sí recursos y grupos de recursos. Las aplicaciones también pueden definir derechos específicos que restrinjan el acceso únicamente a determinadas aplicaciones en los recursos contenidos.
- Los activos suelen ser recursos no conectados o no digitales que requieren abastecimiento manual, como teléfonos móviles y equipos portátiles. Por tanto, los activos no pueden contener roles, recursos ni grupos de recursos.

Las aplicaciones y los activos están pensados para asignarse a roles de negocio y de TI.

Nota –

A los administradores de roles se les asigna una o varias de las siguientes capacidades:

- Administrador de activos
- Administrador de aplicaciones
- Administrador de roles de negocio
- Administrador de roles de TI

Para obtener más información, consulte “Asignación de capacidades a usuarios” en la página 219.

Sinopsis de los tipos de roles

En la figura siguiente se resumen los tipos de roles, recursos y grupos de recursos que pueden asignarse a cada uno de los cuatro tipos de roles. La figura también muestra que es posible asignar exclusiones de tipos de roles a los cuatro tipos de roles. (Las exclusiones de roles se tratan en “Para asignar recursos y grupos de recursos” en la página 129.)

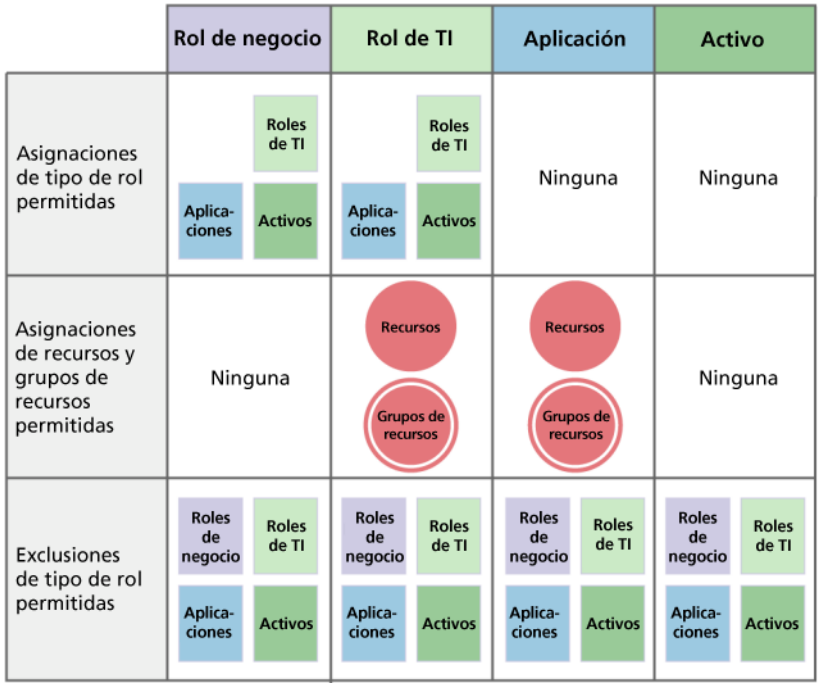


FIGURA 5–1 Los tipos de roles de negocio, TI, aplicación y activo

Los roles contenidos opcionales, condicionales y requeridos ("¿Qué son los roles?" en la página 121) aumentan la flexibilidad. Las definiciones de roles flexibles pueden reducir el número total de roles que necesita administrar la organización.

La Figura 5–2 muestra que los roles de negocio y de TI pueden asignarse directamente a los usuarios si se ha actualizado a la versión 8.0 una versión anterior de Identity Manager. Al actualizar, los roles anteriores se convierten en roles de TI y, para garantizar la compatibilidad con versiones anteriores, los roles de TI se asignan directamente a los usuarios. Si Identity Manager no se ha actualizado desde una versión anterior a la 8.0, sólo se podrán asignar directamente a los usuarios roles de negocio.

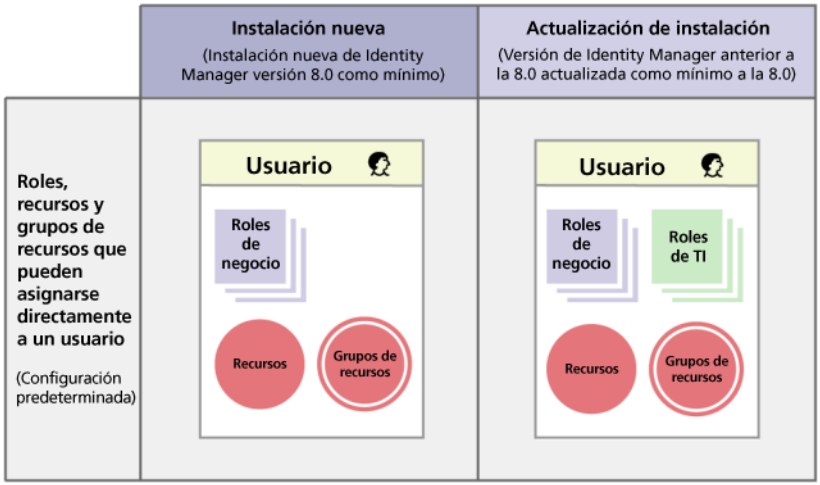


FIGURA 5–2 Roles y recursos que se pueden asignar directamente a los usuarios.

Creación de roles

En esta sección se explica cómo crear roles a lo largo de los siguientes apartados:

- "Para crear roles con el formulario de creación de roles" en la página 126
- "Para asignar recursos y grupos de recursos" en la página 129
- "Para editar valores de atributos de recursos asignados" en la página 130
- "Para asignar roles y exclusiones de roles" en la página 132
- "Designación de propietarios y aprobadores de roles" en la página 134
- "Designación de notificaciones" en la página 136
- "Inicio de elementos de trabajo de aprobaciones de cambio y de aprobación" en la página 137

Nota – Dentro de "Uso de tipos de roles para diseñar roles flexibles" en la página 123 encontrará consejos para diseñar roles.

Cuando se crea o edita un rol, Identity Manager inicia el flujo de trabajo `ManageRole`. Este flujo de trabajo guarda el rol nuevo o actualizado en el depósito y le permite insertar aprobaciones u otras acciones antes de crear o guardar el rol.

▼ Para crear roles con el formulario de creación de roles

1 **En la interfaz de administración, seleccione Roles en el menú principal.**

Aparece la página Roles (ficha Listar roles).

2 **Haga clic en Nuevo en la parte inferior de la página.**

Aparece la página Crear rol de TI. Para crear otro tipo de rol, use el menú desplegable Tipo.

3 **Rellene los campos del formulario de la ficha Identidad.**

La figura siguiente muestra la ficha Identidad.

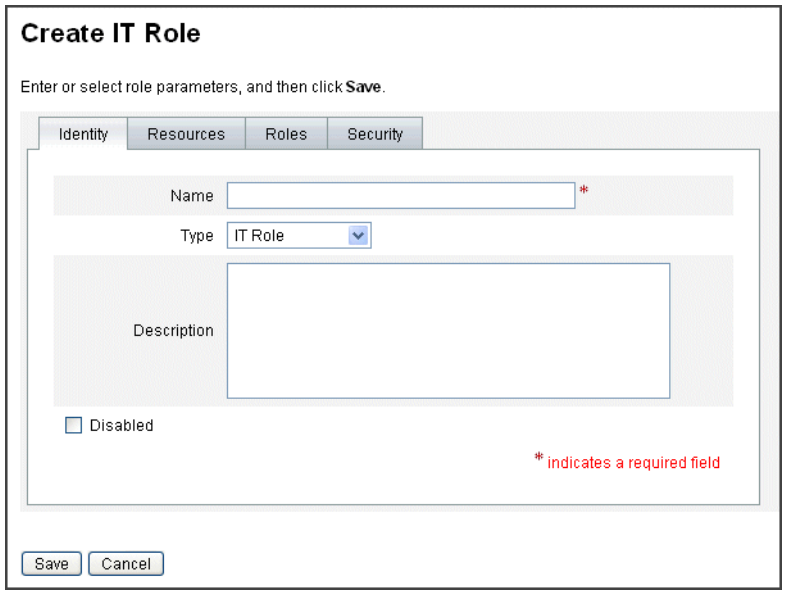


FIGURA 5–3 Ficha Identidad en la página Crear rol de TI

4 **Rellene los campos del formulario de la ficha Recursos (si procede. Encontrará ayuda para rellenar los campos de esta ficha en la ayuda en línea y en el apartado "Para asignar recursos y grupos de recursos" en la página 129.**

Para aprender a definir valores de atributos extendidos en los roles, consulte el apartado "Para ver o editar atributos de cuentas de recursos" en la página 169.

La figura siguiente muestra la ficha Recursos.

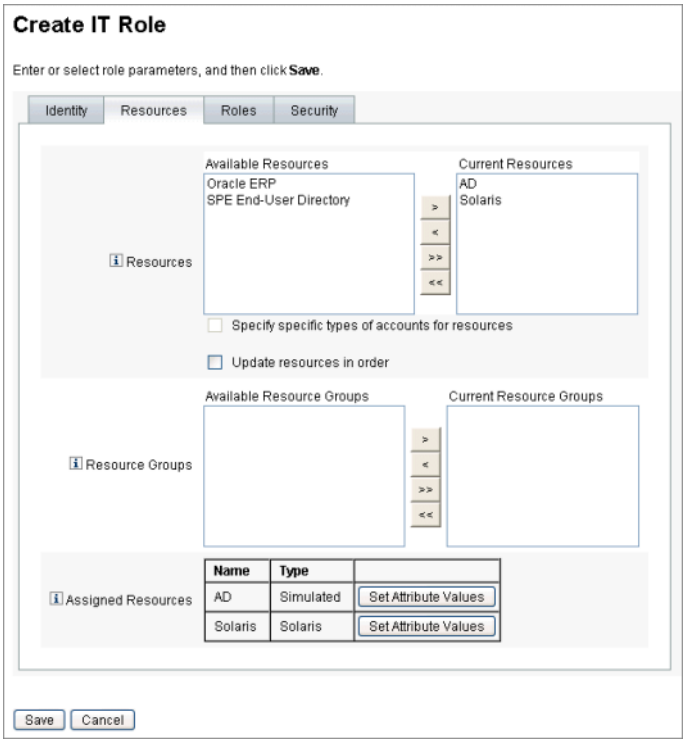


FIGURA 5–4 Ficha Recursos en la página Crear rol de TI

5 **Rellene los campos del formulario de la ficha Recursos (si procede). Encontrará ayuda para rellenar los campos de esta ficha en la ayuda en línea y en el apartado "Para asignar roles y exclusiones de roles" en la página 132.**

La Figura 5–6 muestra la ficha Roles.

6 **Rellene los campos del formulario de la ficha Seguridad. Encontrará ayuda para rellenar los campos de esta ficha en la ayuda en línea y en los apartados "Designación de propietarios y aprobadores de roles" en la página 134 y "Designación de notificaciones" en la página 136.**

"Designación de propietarios y aprobadores de roles" en la página 134 muestra la ficha Seguridad.

7 **Haga clic en Guardar en la parte inferior de la página.**

8 **Introduzca un nombre y una descripción del rol en la ficha Identidad del formulario de creación de roles. Si va a crear un rol nuevo, seleccione el tipo en el menú desplegable Tipo.**

La Figura 5–4 muestra el área Identidad de la ficha Identidad del formulario de creación de roles. En la ayuda en línea se explica cómo utilizar este formulario.

▼ Para asignar recursos y grupos de recursos

Los recursos y grupos de recursos pueden asignarse directamente a roles de TI y de aplicación en la ficha Recursos del formulario de creación de roles. Los recursos se describen más adelante en la sección "Conceptos y administración de recursos de Identity Manager" en la página 160. Los grupos de recursos se describen en la sección "Grupos de recursos" en la página 170.

- Los recursos y grupos de recursos no se pueden asignar directamente a los roles de negocio, porque a los roles de negocio sólo se les pueden asignar roles de negocio.
- Los recursos y grupos de recursos no se pueden asignar a roles de activo, ya que los roles de activo se reservan para los recursos no conectados o no digitales que requieren abastecimiento manual.

A continuación se explica cómo asignar recursos y grupos de recursos a un rol al rellenar el formulario de creación de roles. Consulte el procedimiento inicial en "Para crear roles con el formulario de creación de roles" en la página 126.

1. **Haga clic en la ficha Recursos de la página Crear rol.**
2. **Para asignar un recurso, selecciónelo en la columna Recursos disponibles y trasládelo a la columna Recursos vigentes mediante los botones de flecha.**
3. **Si va a asignar varios recursos, puede especificar el orden en el que se actualizarán: seleccione la casilla Actualizar recursos en orden y utilice los botones + y - para cambiar el orden de los recursos en la columna Recursos vigentes.**
4. **Para asignar un grupo de recursos a este rol, selecciónelo en la columna Grupos disponibles de recursos y trasládelo a la columna Grupos vigentes de recursos mediante los botones de flecha. Un grupo de recursos es un conjunto de recursos que ofrece otra manera de especificar el orden en que se crean y actualizan las cuentas de recursos.**
5. **Para especificar atributos de cuenta para este rol en función del recurso, haga clic en Configurar valores de atributo dentro de la sección Recursos asignados. Encontrará más información en el apartado "Para ver o editar atributos de cuentas de recursos" en la página 169.**
6. **Pulse Guardar para guardar el rol, o bien haga clic en las fichas Identidad, Roles o Seguridad para proseguir con el proceso de creación de roles.**

   La figura siguiente muestra la ficha Recursos del formulario de creación de roles.

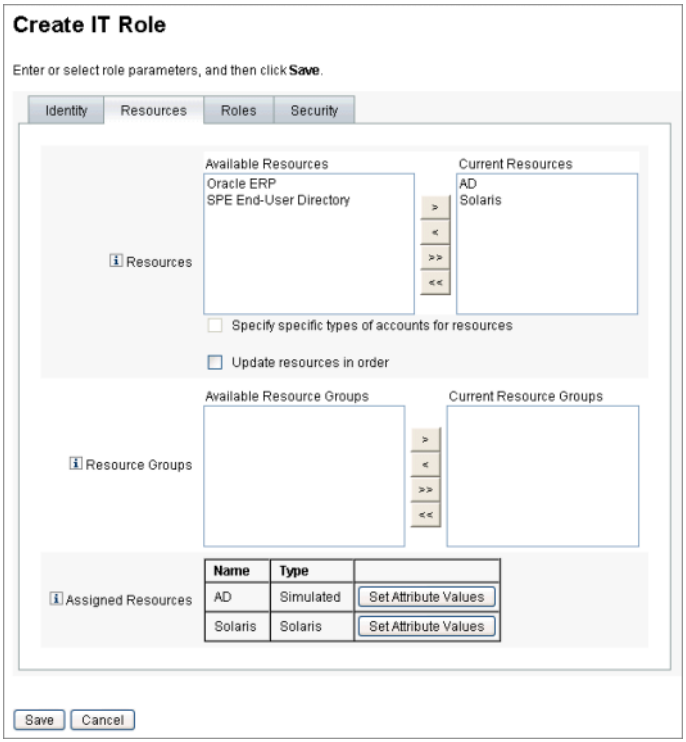
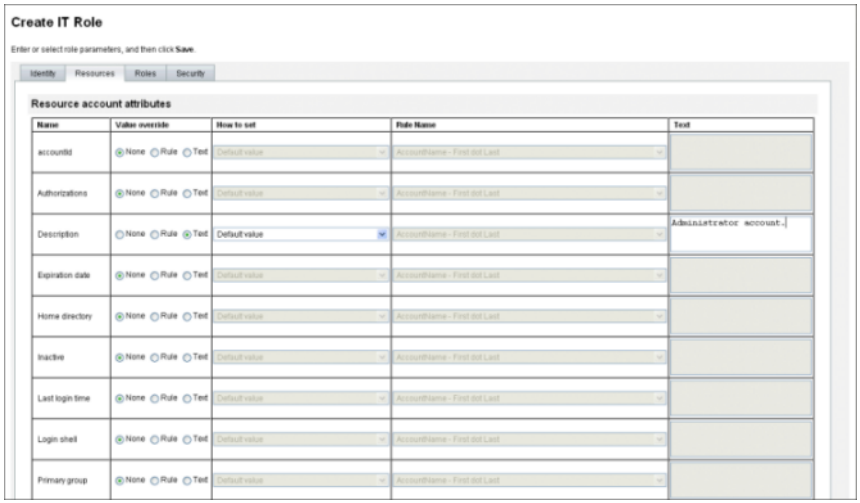


FIGURA 5–5 Área Recursos del formulario con fichas de creación de roles.

▼ Para editar valores de atributos de recursos asignados

Utilice la tabla Recursos asignados para definir o modificar valores de atributos de recursos asignados a un rol. Un recurso puede adoptar distintos valores de atributo por rol. Al pulsar el botón Configurar valores de atributo, aparece la página Atributos de cuentas de recursos.

La figura siguiente muestra la página Atributos de cuentas de recursos, que sirve para definir valores de atributo extendidos en los recursos asignados a un rol.



1 **En la página Atributos de cuentas de recursos, especifique nuevos valores para cada atributo y cómo se definen los valores.**

Identity Manager permite configurar los valores directamente o aplicando una regla, y ofrece diversas opciones para sustituir los valores existentes o fusionarlos con otros. Encontrará información general sobre los valores de atributos de recursos en el apartado "Para ver o editar atributos de cuentas de recursos" en la página 169.

Utilice las opciones siguientes para establecer los valores de cada atributo de cuenta de recursos.

- **Toma de precedencia sobre valor**. Elija una de estas opciones:
  - **Ninguno** (*valor predeterminado)*. No se establece ningún valor.
  - **Regla**. Utiliza una regla para definir el valor.

    Si selecciona esta opción, debe seleccionar también un nombre de regla de la lista.
  - **Texto**. Utiliza el texto especificado para definir el valor.

    Si elige esta opción, deberá introducir el texto en el campo Texto adyacente.
- **Cómo configurar**. Elija una de estas opciones:
  - **Valor predeterminado**. Define la regla o texto como el valor de atributo predeterminado.

    El usuario puede cambiar o sustituir este valor.
  - **Definir como valor**. Define el valor de atributo en la forma especificada por la regla o texto.

    Se definirá el valor y se sustituirán todos los cambios del usuario.
  - **Combinar con valor**. Fusiona el valor de atributo actual con los valores especificados por la regla o el texto.

- **Combinar con valor, eliminar valor existente**. Elimina los valores de atributo actuales, y define el valor como una combinación de los valores especificados por éste y otros roles asignados.
- **Suprimir de valor**. Elimina el valor especificado por la regla o el texto del valor de atributo.
- **Configuración autoritativa a valor**. Define el valor de atributo en la forma especificada por la regla o texto.

  Se definirá el valor y se sustituirán todos los cambios del usuario. Si elimina el rol, el nuevo valor será nulo, aunque haya existido anteriormente en el atributo.
- **Combinación autoritativa con valor**. Fusiona el valor de atributo actual con los valores especificados por la regla o el texto.

  Al eliminar el rol, se suprime el valor asignado al asignar el rol y el valor original del atributo permanece intacto.
- **Combinación autoritativa con valor, eliminar valor existente**. Elimina los valores de atributo actuales, y define el valor como una combinación de los valores especificados por éste y otros roles asignados.

  Si se ha eliminado el rol, borra el valor de atributo especificado por ese rol, aunque haya existido anteriormente en el atributo.

- **Nombre de regla**. Si selecciona Regla en el área de sustitución de valores, debe seleccionar también una regla de la lista.
- **Texto**. Si ha seleccionado "Texto" en el área de sustitución de valores, introduzca un texto para añadirlo al valor de atributo, eliminarlo o utilizarlo como valor.

2 Haga clic en Aceptar para guardar los cambios y regresar a la página de creación o edición de roles.

▼ Para asignar roles y exclusiones de roles

Los roles se pueden asignar a roles de negocio y a roles de TI con la ficha Roles del formulario Crear rol. Los roles asignados deben incluirse en la tabla Roles contenidos.

- No se pueden asignar roles a roles de aplicación ni de activo.
- Los roles de negocio no se pueden asignar a ningún tipo de rol.

Las exclusiones de roles pueden asignarse a los cuatro tipos de roles en la ficha Roles del formulario de creación de roles. Si un usuario tiene asignado un rol con una exclusión de rol, el rol excluido no se puede asignar a dicho usuario. Las exclusiones de roles deben incluirse en la tabla Exclusiones de rol.

A continuación se explica cómo asignar uno o varios recursos a un rol al rellenar el formulario de creación de roles. Consulte el procedimiento inicial en "Para crear roles con el formulario de creación de roles" en la página 126.

Para rellenar la ficha Roles

1 **Haga clic en la ficha Roles de la página Crear rol.**

2 **Seleccione Agregar en la sección Roles contenidos.**

La ficha se actualiza con el formulario Buscar roles para contener.

3 **Busque el rol o roles que desea asignar a éste. Empiece por los roles *requeridos*. (Después añadirá los roles condicionales y opcionales.)**

Encontrará información sobre el uso del formulario de búsqueda en el apartado "Para buscar roles" en la página 138. Los roles de negocio no se pueden anidar ni asignar a otros tipos de roles.

4 **Seleccione los roles que desea asignar mediante las casillas de verificación y después pulse Agregar.**

La ficha se actualiza con el formulario Agregar rol contenido.

5 **En el menú desplegable Tipo de asociación, elija el tipo de rol requerido (o condicional u opcional, según proceda).**

Haga clic en Aceptar.

6 **Repita los cuatro pasos anteriores para agregar roles condicionales (en su caso). Repita los cuatro pasos anteriores para agregar roles opcionales (en su caso).**

7 **Pulse Guardar para guardar el rol, o bien haga clic en las fichas Identidad, Recursos o Seguridad para proseguir con el proceso de creación de roles.**

La Figura 5–6 ilustra la ficha Roles del formulario de creación de roles. En la ayuda en línea se explica cómo utilizar este formulario.

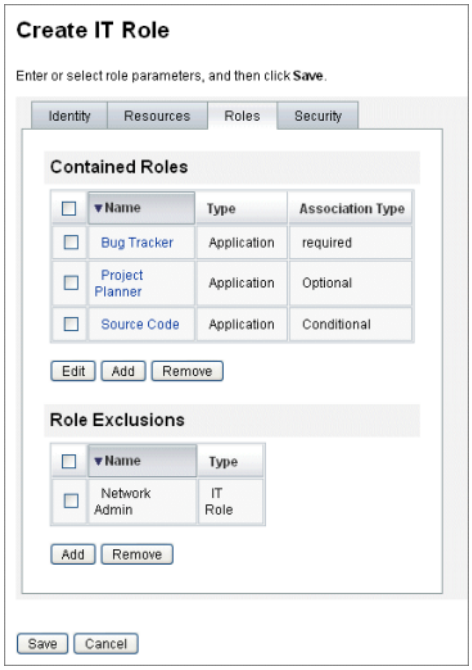


FIGURA 5–6 Área Roles del formulario con fichas de creación de roles.

Designación de propietarios y aprobadores de roles

Los roles tienen *propietarios* y *aprobadores* designados. Sólo los propietarios de roles pueden autorizar modificaciones en los parámetros que definen el rol, mientras que sólo los aprobadores de roles pueden autorizar la asignación del rol a los usuarios finales.

Nota – Si tiene Identity Manager integrado con Sun™ Role Manager, debe permitir que Role Manager gestione todas las aprobaciones y notificaciones de cambios, para lo cual deben inhabilitar manualmente la capacidad de realizar estas acciones de Identity Manager.

Debe editar como sigue el objeto de configuración `RoleConfiguration` en Identity Manager:

- Busque todas las instancias de `changeApproval` y defina el valor en **`false`**.
- Busque todas las instancias de `changeNotification` y defina el valor en **`false`**.

Ser propietario de un rol es ser el responsable propietario del negocio para los derechos de la cuenta de recursos subyacente asignados mediante el rol. Si un administrador modifica un rol, un propietario del rol debe aprobar los cambios para que se apliquen. Esta función impide que un administrador cambie un rol sin el conocimiento y la aprobación de un propietario de

negocio. No obstante, si se han inhabilitado las aprobaciones de cambios en el objeto de configuración de rol, no se necesita la aprobación de un propietario de rol para que se apliquen los cambios.

Además de aprobar los cambios de rol, los roles no se pueden habilitar, inhabilitar ni eliminar sin la aprobación de su propietario.

Los propietarios y aprobadores de roles pueden agregarse a un rol directamente o bien dinámicamente mediante una regla de asignación de roles. En Identity Manager es posible (pero no aconsejable) crear roles sin propietarios y aprobadores.

Nota – Las reglas de asignación de roles tienen un tipo de autenticación `RoleUserRule authType`.

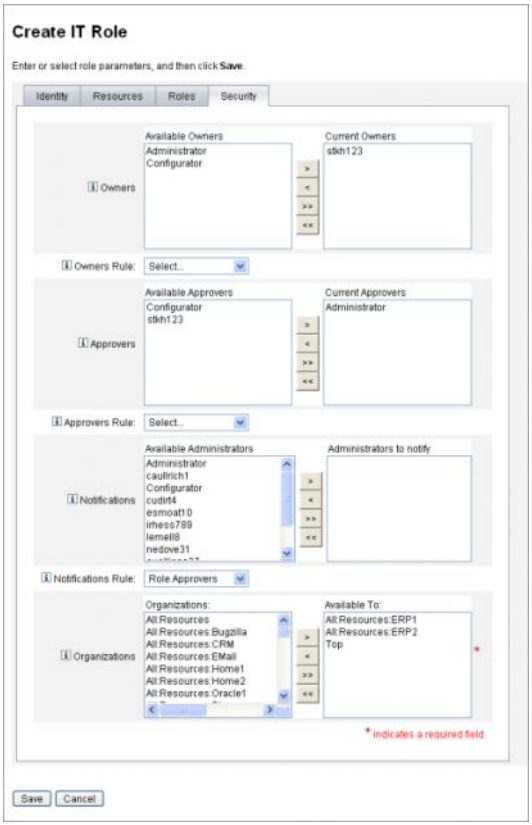
Para crear una regla de asignación de roles personalizada, guíese por los tres objetos de regla de asignación de roles predeterminados.

- Aprobadores de roles
- Notificaciones de roles
- Propietarios de roles

Cuando un elemento de trabajo requiere la aprobación de los propietarios y los aprobadores, se les notifica por correo electrónico. Los elementos de trabajo de aprobaciones de cambio y de aprobación se tratan en la sección "Inicio de elementos de trabajo de aprobaciones de cambio y de aprobación" en la página 137.

Los propietarios y aprobadores se agregan a los roles en la ficha Seguridad del formulario de creación de roles.

"Designación de propietarios y aprobadores de roles" en la página 134 muestra la ficha Seguridad del formulario de creación de roles. En la ayuda en línea se explica cómo utilizar este formulario.



Designación de notificaciones

Se puede enviar una notificación a uno o varios administradores cuando se asigne un rol a un usuario.

Especificar el destinatario de la notificación es optativo. Puede decidir notificar a un administrador si prefiere no exigir aprobación cuando se asigne un rol a un usuario. O quizá designe un administrador para que actúe como aprobador y otro administrador para que reciba las notificaciones cuando se efectúe la aprobación.

Como los propietarios y aprobadores, las notificaciones pueden agregarse a un rol directamente o bien dinámicamente mediante una regla de asignación de roles. Cuando se asigna un rol a un usuario, se avisa a los destinatarios de la notificación por correo electrónico. Sin embargo, no se crea ningún elemento de trabajo, ya que no se requiere aprobación.

Las notificaciones se asignan a roles en la ficha Seguridad del formulario de creación de roles. "Designación de propietarios y aprobadores de roles" en la página 134 muestra la ficha Seguridad del formulario de creación de roles.

Inicio de elementos de trabajo de aprobaciones de cambio y de aprobación

Cuando se efectúan cambios en un rol, sus propietarios pueden recibir por correo electrónico una *aprobación de cambio*, *una notificación de cambio* o no recibir nada. Cuando se asigna un rol a un usuario, los aprobadores del rol reciben mensajes de *aprobación* del rol por correo electrónico.

De manera predeterminada, los propietarios de roles reciben mensajes de aprobación de cambio por correo electrónico siempre que se modifican los roles que detentan. No obstante, este comportamiento se puede modificar por tipo de rol. Por ejemplo, puede optar por habilitar aprobaciones de cambio para los roles de negocio y de TI y notificaciones de cambio para los roles de aplicaciones y activos.

En "Configuración de tipos de roles" en la página 155 encontrará instrucciones para habilitar e inhabilitar los mensajes de aprobación y notificación de cambio por correo electrónico.

Las aprobaciones y las notificaciones de cambio funcionan así:

- Si las *aprobaciones de cambio* están habilitadas, cuando un administrador modifica un rol se genera un elemento de trabajo y se envía un mensaje de aprobación por correo electrónico al propietario del rol. Para que el cambio sea efectivo, un propietario de roles debe aprobar el elemento de trabajo. Es posible delegar los elementos de trabajo de aprobación de cambio. Para obtener más información, consulte "Aprobación de cuentas de usuario" en la página 237.

  Si las aprobaciones de cambio están inhabilitadas, no se genera ningún elemento de trabajo ni se envía ningún mensaje de aprobación por correo electrónico al propietario del rol.
- Si las *notificaciones de cambio* están habilitadas, cuando un administrador modifica un rol el cambio tiene efecto de inmediato y se envía un mensaje de notificación por correo electrónico al propietario del rol.

  Si las notificaciones de cambio están inhabilitadas, no envía ninguna notificación al propietario del rol.

Cuando se asigna un rol a un usuario, los aprobadores del rol reciben mensajes de *aprobación* del rol por correo electrónico. En Identity Manager no se puede inhabilitar el correo electrónico de aprobación de roles.

En el caso de las aprobaciones de roles, cuando se asigna un rol a un usuario se genera un elemento de trabajo y se envía un mensaje de aprobación por correo electrónico al aprobador del rol. Para que el rol se asigne al usuario, un aprobador de roles debe aprobar el elemento de trabajo.

Es posible delegar los elementos de trabajo de aprobación de cambio y de aprobación. Para obtener más información sobre la delegación de elementos de trabajo, consulte "Delegación de elementos de trabajo" en la página 234.

Edición y administración de roles

La mayoría de las tareas de edición y administración de roles se pueden realizar en las fichas Buscar roles y Listar roles, que se encuentran dentro de la ficha Roles en el menú principal.

Se tratan los temas siguientes:

▼ Para buscar roles

Use la ficha Roles para buscar roles que cumplan los criterios de búsqueda que especifique.

En la ficha Roles puede buscar roles según muy diversos criterios, como propietarios y aprobadores de roles, tipos de cuentas asignados, roles contenidos, etc.

Encontrará información para buscar usuarios asignados a un rol en el apartado "Para buscar usuarios asignados a un rol específico" en la página 153.

1 En la interfaz de administración, seleccione la ficha Roles.

Se abre la ficha Listar roles.

2 Haga clic en la ficha secundaria Buscar roles.

La Figura 5–7 muestra la ficha Buscar rol. En la ayuda en línea se explica cómo utilizar este formulario.

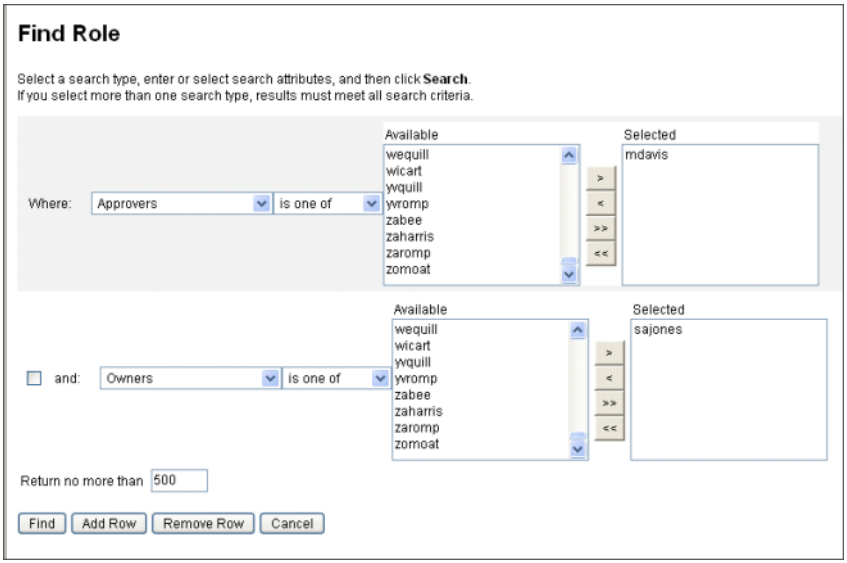


FIGURA 5–7 Ficha Buscar rol

Utilice los menús desplegables para definir los parámetros de búsqueda. Pulse el botón Agregar fila para añadir otros parámetros.

▼ Para ver roles

Para ver roles, use la ficha Listar roles. Los campos de filtro situados en la parte superior de la página Listar roles sirven para buscar roles por su nombre o tipo. Al filtrar no se distinguen mayúsculas de minúsculas.

- **En la interfaz de administración, seleccione la ficha Roles.**

  Se abre la ficha Listar roles.

  La Figura 5–8 muestra la ficha Listar roles. En la ayuda en línea se explica cómo utilizar este formulario.

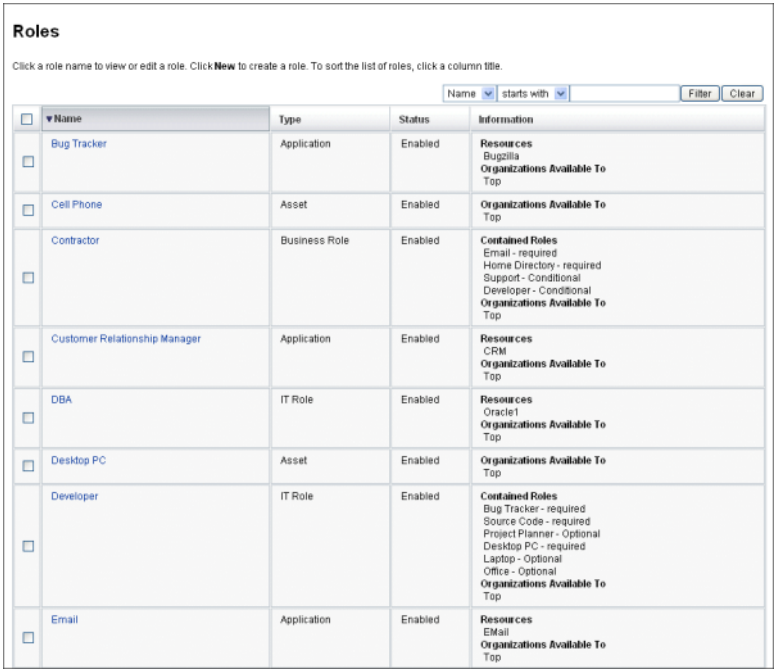


FIGURA 5–8 Ficha Listar roles

▼ Para editar roles

Para buscar el rol que desea editar, utilice las fichas Listar roles o Buscar roles. Si modifica un rol y las aprobaciones de cambio están definidas en el valor verdadero (true), un propietario de roles deberá aprobar los cambios para que sean efectivos.

Encontrará información para actualizar los usuarios con los cambios de rol en el apartado "Para actualizar roles asignados a usuarios" en la página 149.

1 **Para buscar el rol que desea editar, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Haga clic en el nombre del rol que desea editar.**

Aparece la página Editar rol.

3 **Edite el rol según convenga. Consulte el procedimiento del apartado "Para crear roles con el formulario de creación de roles" en la página 126, donde se explica cómo rellenar las fichas Identidad, Recursos, Roles y Seguridad.**

Pulse Guardar. Aparece la página Confirmar cambios de rol.

4 **Si este rol está asignado a usuarios, puede especificar cuándo se actualizan los cambios del rol para los usuarios. Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.**

5 **Haga clic en Guardar para guardar los cambios.**

Para clonar roles

1 **Para buscar el rol que desea editar, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Haga clic en el nombre del rol que desea clonar.**

Aparece la página Editar rol.

3 **Introduzca un nombre nuevo en el campo Nombre y haga clic en Guardar.**

Aparece la página Rol: ¿Crear o cambiar nombre? .

4 **Haga clic en Crear para hacer una copia del rol.**

Para asignar un rol a otro rol

Los requisitos de Identity Manager para asignar roles se explican en "¿Qué son los roles?" en la página 121 y en "Uso práctico de los roles" en la página 123. Antes de asignar roles debe conocer dicha información.

Identity Manager cambia las asignaciones de rol de un rol si el propietario del rol principal lo aprueba.

1 **Busque el rol de negocio o de TI al que desea asignar uno o más roles *contenidos*. (Los roles sólo pueden asignarse a roles de negocio y de TI.) Para buscar roles, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Haga clic en el rol de negocio o de TI para abrirlo.**

Aparece la página Editar rol.

3 **Haga clic en la ficha Roles de la página Editar rol.**

4 **Seleccione Agregar en la sección Roles contenidos.**

La ficha se actualiza con el formulario Buscar roles para contener.

5 **Busque el rol o roles que desea asignar a éste. Empiece por los roles *requeridos*. (Después añadirá los roles condicionales y opcionales.)**

Encontrará información sobre el uso del formulario de búsqueda en el apartado "Para buscar roles" en la página 138. Los roles de negocio no se pueden anidar ni asignar a otros tipos de roles.

6 **Seleccione los roles que desea asignar mediante las casillas de verificación y después pulse Agregar.**

La ficha se actualiza con el formulario Agregar rol contenido.

7 **En el menú desplegable Tipo de asociación, elija el tipo de rol requerido (o condicional u opcional, según proceda).**

Haga clic en Aceptar.

8 **Repita los cuatro pasos anteriores para agregar roles condicionales (en su caso). Repita los cuatro pasos anteriores para agregar roles opcionales (en su caso).**

9 **Haga clic en Guardar para abrir la página Confirmar cambios de rol.**

Aparece la página Confirmar cambios de rol.

10 **En el área Actualizar usuarios asignados, elija una opción del menú Actualizar usuarios asignados y haga clic en Guardar para guardar las asignaciones de rol.**

Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.

▼ Para suprimir un rol asignado a otro rol

Identity Manager suprime un rol contenido de otro rol si el propietario del rol principal lo aprueba. El rol suprimido se eliminará de los usuarios cuando éstos reciban actualizaciones de roles. (Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.) Una vez eliminado el rol, los usuarios pierden los derechos que les otorgaba.

- Encontrará información sobre la supresión de roles asignados a uno o más usuarios en el apartado "Para suprimir uno o más roles de un usuario" en la página 154.
- Para obtener información sobre la inhabilitación de roles, consulte "Para habilitar o inhabilitar roles" en la página 143.
- Para obtener información sobre la eliminación de roles de Identity Manager, consulte "Para eliminar roles" en la página 144.

1 **Busque el rol de negocio o de TI del que desea suprimir un rol. Para buscar roles, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Haga clic en el rol para abrirlo.**

Aparece la página Editar rol.

3 **Haga clic en la ficha Roles de la página Editar rol.**

4 **En el área Roles contenidos, marque la casilla de verificación adjunta al rol que desea suprimir y haga clic en Suprimir. Para suprimir varios roles, marque varias casillas.**

La tabla se actualiza para mostrar los roles contenidos que quedan.

5 **Pulse Guardar.**

Aparece la página Confirmar cambios de rol.

6 **En el área Actualizar usuarios asignados, elija una opción del menú Actualizar usuarios asignados. Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.**

7 **Haga clic en Guardar para terminar los cambios.**

Para habilitar o inhabilitar roles

Los roles se pueden habilitar e inhabilitar en la ficha Listar roles. El estado del rol aparece en la columna Estado. Haga clic en el encabezado de la columna Estado para ordenar la tabla por estado de rol.

Los roles inhabilitados no aparecen en la ficha Roles del formulario Crear/Editar usuario y no se pueden asignar directamente a los usuarios. Los roles que contienen roles inhabilitados se pueden asignar a los usuarios, pero los roles inhabilitados no se pueden asignar.

Los usuarios que tienen asignados roles que después se inhabilitan no pierden sus derechos. La inhabilitación de roles sólo impide futuras asignaciones de roles.

Para inhabilitar y rehabilitar un rol se requiere el permiso de su propietario.

Cuando se habilita o inhabilita un rol que está asignado a usuarios, Identity Manager pide que se actualicen dichos usuarios. Encontrará información al respecto en el apartado "Para actualizar roles asignados a usuarios" en la página 149.

1 **Para buscar el rol que desea eliminar, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Marque las casillas de verificación adjuntas a los roles que desea habilitar o inhabilitar.**

3 **Haga clic en Habilitar o Inhabilitar en la parte inferior de la tabla Roles.**

Se abre la página de confirmación para habilitar o inhabilitar los roles.

4 **Haga clic en Aceptar para habilitar o inhabilitar los roles.**

Para eliminar roles

A continuación se explica cómo eliminar un rol de Identity Manager.

- Encontrará información para suprimir roles asignados a otros roles en el apartado "Para suprimir un rol asignado a otro rol" en la página 142.
- Encontrará información sobre la supresión de roles asignados a uno o más usuarios en el apartado "Para suprimir uno o más roles de un usuario" en la página 154.

Si se va a eliminar un rol que está asignado a un usuario, Identity Manager impide la eliminación cuando se intenta guardar el rol. Para que Identity Manager puede eliminar un rol, antes hay que anular la asignación (o reasignar) de todos los usuarios asignados al rol. También debe eliminar el rol de cualquier otro rol.

Identity Manager requiere la aprobación de un propietario de rol para eliminar un rol.

1 **Para buscar el rol que desea eliminar, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Marque la casilla de verificación adjunta a cada rol que desee eliminar.**

3 **Haga clic en Eliminar.**

Aparece la página de confirmación de eliminación de roles.

4 **Haga clic en Aceptar para eliminar uno o varios roles.**

Para asignar un recurso o un grupo de recursos a un rol

Los requisitos de Identity Manager para asignar recursos y grupos de recursos se explican en "¿Qué son los roles?" en la página 121 y en "Uso práctico de los roles" en la página 123. Antes de asignar recursos a roles debe conocer dicha información.

Identity Manager cambia las asignaciones de recursos y grupos de recursos de un rol si el propietario del rol lo aprueba.

1 **Busque el rol de TI o de aplicación al que desea agregar un recurso o un grupo de recursos. Para buscar un rol, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Haga clic en el rol para abrirlo.**

3 **Haga clic en la ficha Recursos de la página Editar rol.**

4 **Para asignar un recurso, selecciónelo en la columna Recursos disponibles y trasládelo a la columna Recursos vigentes mediante los botones de flecha.**

5 **Si va a asignar varios recursos, puede especificar el orden en el que se actualizarán: seleccione la casilla Actualizar recursos en orden y utilice los botones + y - para cambiar el orden de los recursos en la columna Recursos vigentes.**

6 **Para asignar un grupo de recursos a este rol, selecciónelo en la columna Grupos disponibles de recursos y trasládelo a la columna Grupos vigentes de recursos mediante los botones de flecha. Un grupo de recursos es un conjunto de recursos que ofrece otra manera de especificar el orden en que se crean y actualizan las cuentas de recursos.**

7 **Para especificar atributos de cuenta para este rol en función del recurso, haga clic en Configurar valores de atributo dentro de la sección Recursos asignados. Encontrá más información en el apartado "Para ver o editar atributos de cuentas de recursos" en la página 169.**

8 **Haga clic en Guardar para abrir la página Confirmar cambios de rol.**

Aparece la página Confirmar cambios de rol.

9 **En el área Actualizar usuarios asignados, elija una opción del menú Actualizar usuarios asignados. Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.**

10 **Haga clic en Guardar para guardar las asignaciones de recursos.**

▼ Para suprimir un recurso o un grupo de recursos asignado a un rol

Identity Manager suprime un recurso o un grupo de recursos de un rol si el propietario del rol lo aprueba. El recurso suprimido se eliminará de los usuarios cuando éstos reciban actualizaciones de roles. (Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.) Cuando se elimina un recurso, los usuarios pierden sus derechos sobre él, a no ser que el recurso también esté asignado directamente al usuario.

1 **Busque el rol de TI o de aplicación del que desea suprimir un recurso o un grupo de recursos. Para buscar roles, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2 **Haga clic en el rol para abrirlo.**

Aparece la página Editar rol.

3 **Haga clic en la ficha Recursos de la página Editar rol.**

4 **Para suprimir un recurso, selecciónelo en la columna Recursos vigentes y trasládelo a la columna Recursos disponibles mediante los botones de flecha.**

Para suprimir un grupo de recursos, selecciónelo en la columna Grupos vigentes de recursos y trasládelo a la columna Grupos disponibles de recursos mediante los botones de flecha.

5 **Pulse Guardar.**

Aparece la página Confirmar cambios de rol.

6 **En el área Actualizar usuarios asignados, elija una opción del menú Actualizar usuarios asignados. Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.**

7 **Haga clic en Guardar para terminar los cambios.**

Administración de asignaciones de roles

Los roles se asignan a los usuarios en el área Cuentas de Identity Manager.

▼ Para asignar roles a un usuario

A continuación se indica el procedimiento para asignar uno o más roles a uno o varios usuarios.

Los usuarios finales también pueden solicitar asignaciones de roles. (Sólo pueden solicitar los roles opcionales cuyo rol principal ya se les haya asignado.) Encontrará información sobre cómo los usuarios finales pueden solicitar roles disponibles en el apartado "Ficha Solicitudes" en la página 41 de la sección "Interfaz de usuario final de Identity Manager" en la página 40.

1 **En la interfaz de administración, seleccione la ficha Cuentas.**

Se abre la ficha secundaria Listar cuentas.

2 **Para asignar un rol a un usuario existente, siga estos pasos:**

a. **Seleccione el nombre del usuario en la Lista de usuarios.**

b. **Haga clic en la ficha Roles.**

c. **Pulse Agregar para agregar uno o más roles a la cuenta del usuario.**

De manera predeterminada, sólo es posible asignar directamente roles de negocio a los usuarios. (Si ha actualizado la instalación de Identity Manager desde una versión anterior a la 8.0, podrá asignar directamente a los usuarios roles de negocio y de TI.)

d. En la tabla de roles, elija los que desea asignar al usuario y pulse Aceptar.

Para ordenar la tabla alfabéticamente por Nombre, Tipo o Descripción, haga clic en los encabezados de columna. Si vuelve a hacer clic se invertirá el orden. Para filtrar la lista por tipo de rol, selecciónelo en el menú desplegable Actual.

La tabla se actualiza con las asignaciones de roles seleccionadas y todas las asignaciones de roles necesarias que estén conectadas con las asignaciones del rol principal.

e. Haga clic en Agregar para ver las asignaciones de roles opcionales que también pueden asignarse al usuario.

Elija los roles opcionales que desea asignar al usuario y pulse Aceptar.

f. (Opcional) En la columna Activar en, seleccione la fecha en que debe activarse el rol. Si no especifica ninguna fecha, la asignación del rol se activará en cuanto la apruebe un aprobador designado.

Para que la asignación de rol sea temporal, seleccione la fecha en que debe inactivarse el rol en la columna Desactivar en. La desactivación del rol se producirá al empezar el día seleccionado.

Para obtener más información, consulte "Para activar y desactivar roles en fechas específicas" en la página 147.

g. Pulse Guardar.

Para activar y desactivar roles en fechas específicas

Al asignar un rol a un usuario, puede especificar una fecha de activación y otra de desactivación. Las solicitudes de elementos de trabajo de asignación de roles se crean al efectuar la asignación. No obstante, si una asignación de roles no se ha aprobado para la fecha de activación programada, el rol no se asigna. Las activaciones y desactivaciones de roles se producen un poco después de la media noche (12:01 AM) en la fecha programada.

De manera predeterminada, sólo los roles de negocio pueden tener fechas de activación y de desactivación. Todos los demás tipos de roles heredan las fechas de activación y desactivación del rol de negocio que está asignado directamente al usuario. Identity Manager se puede configurar para que otros tipos de roles tengan fechas de activación y desactivación directamente asignables. Consulte las instrucciones en "Configuración de tipos de roles" en la página 155.

▼ Para editar la programación del Analizador de tareas aplazadas

El Analizador de tareas aplazadas explora las asignaciones de roles de usuario y las activa y desactiva según proceda. De manera predeterminada, la tarea del Analizador de tareas aplazadas se ejecuta cada hora.

1 En la interfaz de administración, seleccione Tareas del servidor.

2 **Elija Administrar programación en el menú secundario.**

3 **Dentro de la sección Tareas disponibles para programación, haga clic en la definición de tarea Analizador de tareas aplazadas.**

Aparece la página "Crear nueva programación de tareas Analizador de tareas aplazadas".

4 **Rellene el formulario. Para obtener información, consulte los elementos i-Help y la ayuda en línea.**

Para especificar la fecha y la hora en que debe ejecutarse la tarea, utilice el formato `mm/dd/aaaa hh:mm:ss` en Fecha de inicio. Por ejemplo, para programar el inicio de la ejecución de una tarea a las 7:00 P.M. del 29 de septiembre de 2009, escriba `09/29/2009 19:00:00`.

En el menú desplegable Opciones de resultados, seleccione cambiar nombre. Si elige esperar, las futuras instancias de esta tarea no se ejecutarán hasta que suprima los resultados anteriores. Encontrará más información sobre los distintos valores de configuración de Opciones de resultados en la ayuda en línea.

5 **Haga clic en Guardar para guardar la tarea.**

La Figura 5–9 muestra el formulario de la tarea programada para el Analizador de tareas aplazadas.

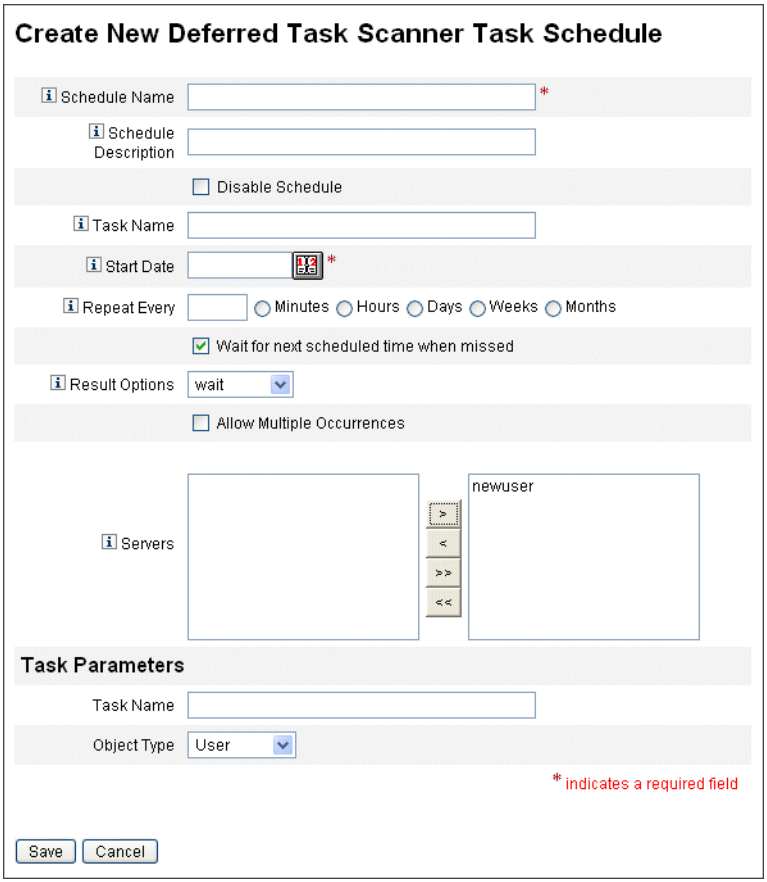


FIGURA 5–9 Formulario de la tarea programada para el Analizador de tareas aplazadas

Para actualizar roles asignados a usuarios

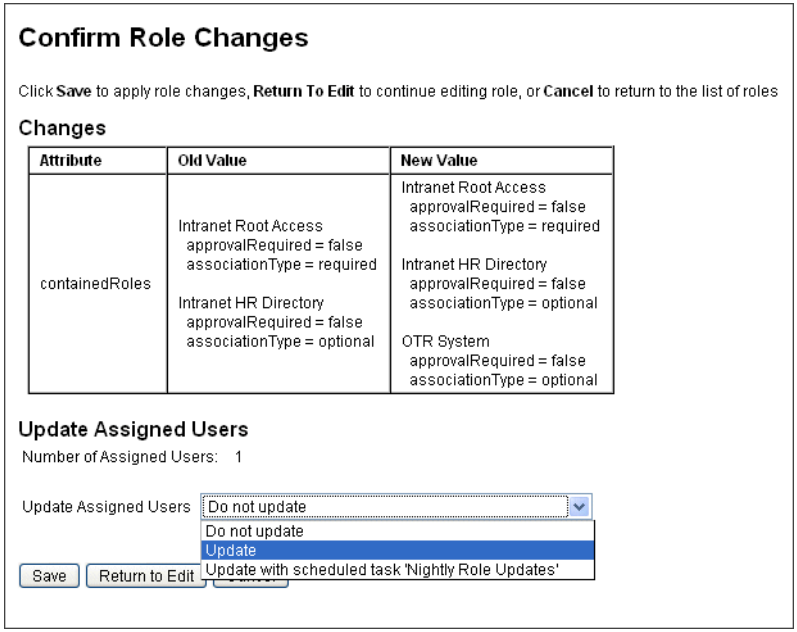
Al editar roles asignados a usuarios tiene la opción de actualizar los usuarios con los nuevos roles inmediatamente o bien aplazar la actualización para ejecutarla durante un periodo de mantenimiento programado.

Tras modificar un rol, aparece la página Confirmar cambios de rol. La página Confirmar cambios de rol se muestra en "Para actualizar roles asignados a usuarios" en la página 149.

- En dicha página, el área Actualizar usuarios asignados indica el número de usuarios a los que está asignado el rol actualmente.
- El menú Actualizar usuarios asignados permite especificar si los usuarios se actualizan de inmediato con los nuevos cambios de rol (Actualizar), si se aplaza dicha actualización (No actualizar) o si se elige una tarea de actualización programada y personalizada.

- Como Actualizar actualiza los usuarios inmediatamente, conviene evitar esta opción si afecta a muchos usuarios. La actualización de los usuarios puede tardar y acaparar muchos recursos. Cuando hay que actualizar muchos usuarios, es preferible programar la actualización para las horas de poca actividad.
- Si se elige No actualizar para un rol, los usuarios que lo tienen asignado no recibirán las actualizaciones del rol hasta que un administrador visualice el perfil de usuario o hasta que el usuario se actualice con una tarea de actualización de usuarios de rol. Para obtener información sobre la programación de tareas de actualización de usuarios de rol, consulte la próxima sección.
- Si ha programado una tarea de actualización de usuarios de rol, puede seleccionarla en el menú. Dicha tarea actualizará los usuarios asignados al rol tal como ha sido programada. Para obtener más información, consulte la próxima sección.

  "Para actualizar roles asignados a usuarios" en la página 149 muestra la página Confirmar cambios de rol. El área Actualizar usuarios asignados indica el número de usuarios a los que está asignado el rol actualmente. El menú Actualizar usuarios asignados tiene dos opciones predeterminadas: No actualizar y Actualizar. También es posible seleccionar en una lista de tareas de actualización de usuarios de rol programadas. Encontrará instrucciones para crear tareas de actualización de usuarios de rol programadas en el apartado "Para programar una tarea de actualización de usuarios de rol" en la página 152.



▼ Para actualizar a mano usuarios asignados

Los usuarios que tienen roles asignados se pueden actualizar seleccionando uno o varios y pulsando el botón Actualizar usuarios asignados. Mediante este procedimiento se ejecuta una instancia de la tarea Actualizar roles de usuario para los roles especificados.

1. **Para buscar el rol (o roles) cuyos usuarios desea actualizar, siga las instrucciones de los apartados "Para buscar roles" en la página 138 o "Para ver roles" en la página 139.**

2. **Seleccione los roles mediante las casillas de verificación.**

3. **Haga clic en Actualizar usuarios asignados.**

   Aparece la página Actualizar usuarios asignados a los roles (Figura 5–10).

4. **Pulse Ejecutar para iniciar la actualización.**

5. **Para comprobar el estado de la tarea Actualizar roles de usuario, elija Tareas del servidor en el menú principal y después Todas las tareas en el menú secundario.**

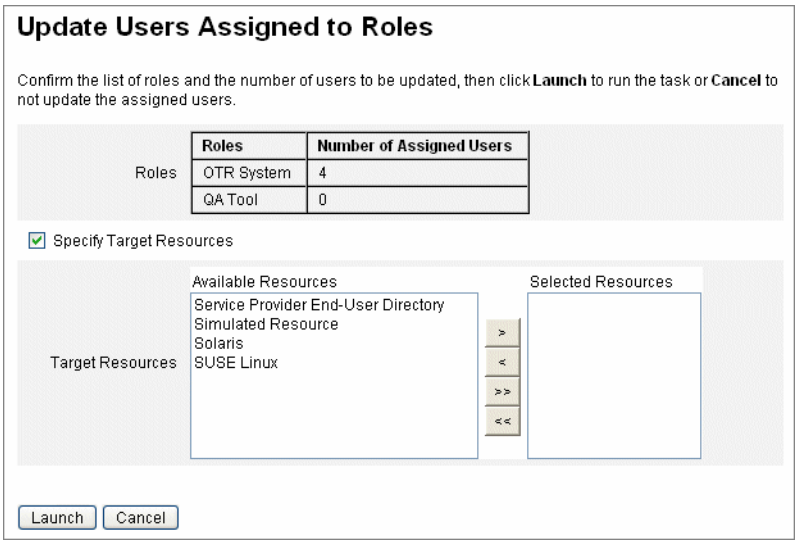


FIGURA 5–10 Página Actualizar usuarios asignados a los roles

▼ Para programar una tarea de actualización de usuarios de rol

Nota – Conviene programar una tarea de actualización de usuarios de rol para que se ejecute periódicamente.

Una tarea de actualización de usuarios de rol se programa así para actualizar los usuarios con los cambios de rol:

1. **En la interfaz de administración, seleccione Tareas del servidor.**

2. **Elija Administrar programación en el menú secundario.**

3. **Dentro de la sección Tareas disponibles para programación, haga clic en la definición de tarea Actualizar roles de usuario.**

   Aparece la página "Crear nueva programación de tareas Actualizar roles de usuario" o, si está editando una tarea existente, la página "Editar programación de tareas" (Figura 5–11).

4. **Rellene el formulario. Para obtener información, consulte los elementos i-Help y la ayuda en línea.**

   Para especificar la fecha y la hora en que debe ejecutarse la tarea, utilice el formato `mm/dd/aaaa hh:mm:ss` en Fecha de inicio. Por ejemplo, para programar el inicio de la ejecución de una tarea a las 7:00 P.M. del 29 de septiembre de 2009, escriba `09/29/2009 19:00:00`.

   En el menú desplegable Opciones de resultados, seleccione cambiar nombre. Si elige esperar, las futuras instancias de esta tarea no se ejecutarán hasta que suprima los resultados anteriores. Encontrará más información sobre los distintos valores de configuración de Opciones de resultados en la ayuda en línea.

5. **Haga clic en Guardar para guardar la tarea.**

   La Figura 5–11 muestra el formulario de la tarea programada para Actualizar roles de usuario. Se pueden asignar roles a tareas Actualizar roles de usuario específicas (como se explica en la sección Parámetros de tarea). Para obtener más información, consulte "Para actualizar roles asignados a usuarios" en la página 149.

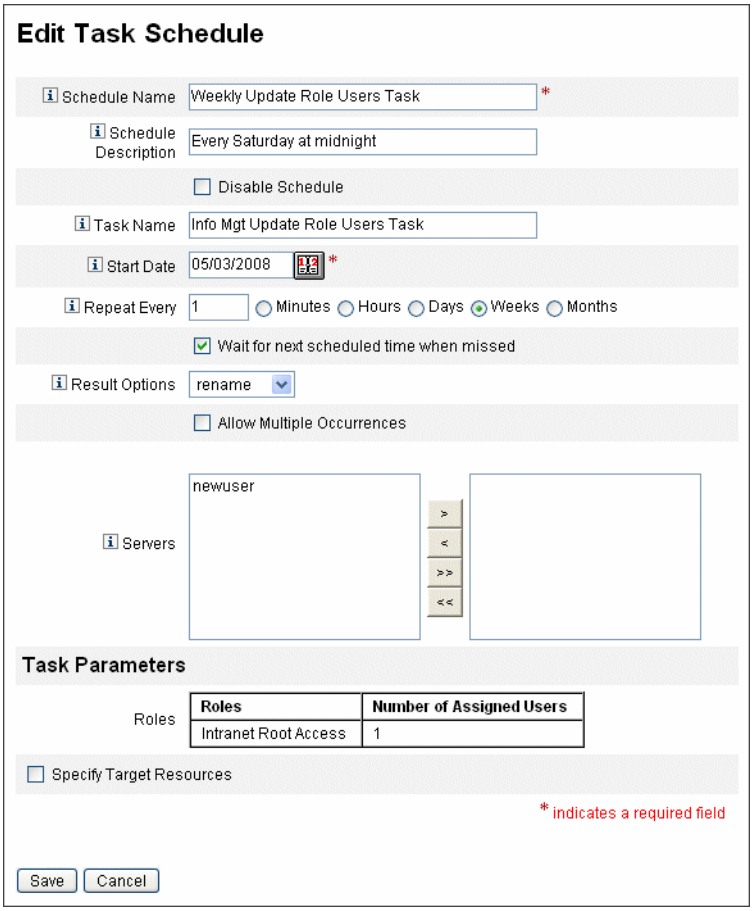


FIGURA 5–11 Formulario de la tarea programada para Actualizar roles de usuario

▼ Para buscar usuarios asignados a un rol específico

Es posible buscar usuarios que tienen asignado un rol específico.

1. **En la interfaz de administración, seleccione Cuentas.**
2. **Elija Buscar usuarios en el menú secundario. Aparece la página Buscar usuarios.**
3. **Elija el tipo de búsqueda El usuario tiene [seleccione el tipo de rol] roles asignados.**
4. **Marque la casilla correspondiente y filtre la lista de roles disponibles con el menú desplegable Seleccionar tipo de rol.**

   Aparece otro menú de roles.

5 **Seleccione un rol.**

6 **Desactive las demás casillas de tipo de búsqueda si no quiere delimitar más la búsqueda.**

7 **Haga clic en Buscar.**

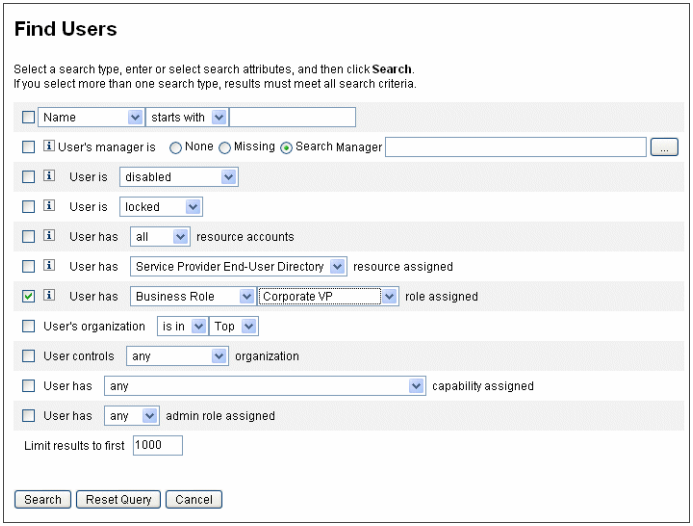


FIGURA 5–12 Búsqueda de usuarios que tienen un rol asignado en la página Buscar usuarios

▼ Para suprimir uno o más roles de un usuario

En la página Editar usuario se pueden suprimir uno o varios roles de una cuenta de usuario. Sólo es posible suprimir los roles asignados directamente. Los roles asignados indirectamente (es decir, *roles contenidos* condicionales o requeridos) se eliminan al eliminar el rol principal. Otra forma de suprimir un rol asignado indirectamente de un usuario es quitar dicho rol del rol principal (consulte "Para suprimir un rol asignado a otro rol" en la página 142).

Los usuarios finales también pueden solicitar que se les supriman roles asignados de sus cuentas de usuario. Consulte la ficha "Ficha Solicitudes" en la página 41 en la sección "Interfaz de usuario final de Identity Manager" en la página 40.

Encontrará información para suprimir un rol aplicando una fecha de desactivación programada en el apartado "Para activar y desactivar roles en fechas específicas" en la página 147.

1 **En la interfaz de administración, seleccione la ficha Cuentas.**

Se abre la ficha secundaria Listar cuentas.

2 **Seleccione el usuario de quien desea suprimir una o más reglas.**

Aparece la página Editar usuario.

3 **Haga clic en la ficha Roles.**

4 **En la tabla de roles, elija los que desea quitar al usuario y pulse Aceptar.**

Para ordenar la tabla alfabéticamente por Nombre, Tipo, Activar en, Desactivar en, Asignados por o Estado, haga clic en los encabezados de columna. Si vuelve a hacer clic se invertirá el orden. Para filtrar la lista por tipo de rol, selecciónelo en el menú desplegable Actual.

La tabla muestra las asignaciones de roles principales (los roles que pueden seleccionarse) y todas las asignaciones de roles que estén conectadas con las asignaciones del rol principal (los roles que no pueden seleccionarse).

5 **Pulse Suprimir.**

La tabla de roles asignados se actualiza para mostrar los roles asignados que quedan.

6 **Pulse Guardar.**

Aparece la página de actualización de cuentas de recursos. Deseleccione las cuentas de recursos que no quiera eliminar.

7 **Haga clic en Guardar para guardar los cambios.**

Configuración de tipos de roles

La funcionalidad de tipo de rol puede modificarse editando el objeto de configuración de rol.

▼ Para configurar tipos de roles como directamente asignables a los usuarios

De manera predeterminada, sólo es posible asignar directamente tipos de roles concretos a los usuarios. Para cambiar esta configuración, proceda como sigue.

Nota – Es una práctica recomendada sólo asignar directamente roles de negocio a los usuarios. Encontrará más información en "Uso de tipos de roles para diseñar roles flexibles" en la página 123.

Para cambiar los tipos de roles que se pueden asignar directamente a los usuarios, siga estos pasos:

1 **Abra el objeto de configuración de rol para editarlo mediante el procedimiento que se explica en "Edición de objetos de configuración de Identity Manager" en la página 118.**

2 **Busque el objeto de rol correspondiente al tipo de rol que desea editar.**

- Para editar un rol de TI, busque `Object name='ITRole'`
- Para editar un rol de aplicación, busque `Object name='ApplicationRole'`
- Para editar un rol de activo, busque `Object name='AssetRole'`

3 **Especifique un conjunto de instrucciones para actualizar la configuración.**

Elija uno de los siguientes según cómo quiera actualizar la configuración:

- Para modificar un tipo de rol con el fin de poderlo asignar directamente a un usuario, busque el atributo `userAssignment` siguiente dentro del objeto de rol:

```
<Attribute name='userAssignment'>
        <Object/>
    </Attribute>
```

Y sustitúyalo por esto:

```
<Attribute name='userAssignment'>
        <Object>
            <Attribute name='manual' value='true'/>
         </Object>
    </Attribute>
```

- Para modificar un tipo de rol con el fin de impedir su asignación directa a un usuario, busque el atributo `userAssignment` dentro del objeto de rol y elimine el atributo `manual` así:

```
<Attribute name='userAssignment'>
        <Object>
        </Object>
    </Attribute>
```

4 **Guarde el objeto de configuración de rol. No es necesario reiniciar los servidores de aplicaciones para que los cambios surtan efecto.**

▼ Para habilitar tipos de roles con fechas de activación y desactivación asignables

De manera predeterminada, sólo los roles de negocio pueden tener fechas de activación y de desactivación que se especifican al asignar los roles. Todos los demás roles heredan las fechas de activación y desactivación del rol de negocio que está asignado directamente al usuario.

Nota – Es una práctica recomendada sólo asignar directamente roles de negocio a los usuarios. Encontrará más información en "Uso de tipos de roles para diseñar roles flexibles" en la página 123.

Si decide que otro tipo de rol sea directamente asignable a los usuarios (por ejemplo, el rol de TI), quizá también le interese poder asignar fechas de activación y de desactivación a ese tipo de rol.

Proceda como se indica a continuación para cambiar los tipos de roles que pueden tener fechas de activación y desactivación asignables.

1 **Abra el objeto de configuración de rol para editarlo mediante el procedimiento que se explica en "Edición de objetos de configuración de Identity Manager" en la página 118.**

2 **Busque el objeto de rol correspondiente al tipo de rol que desea editar.**

- Para editar un rol de negocio, busque `Object name='BusinessRole'`
- Para editar un rol de TI, busque `Object name='ITRole'`
- Para editar un rol de aplicación, busque `Object name='ApplicationRole'`
- Para editar un rol de activo, busque `Object name='AssetRole'`

3 **Especifique un conjunto de instrucciones para actualizar la configuración.**

Elija uno de los siguientes según cómo quiera actualizar la configuración:

- Para modificar un tipo de rol con el fin de que pueda tener fechas de activación y de desactivación directamente asignables, busque el atributo `userAssignment` siguiente dentro del objeto de rol:

```
<Attribute name='userAssignment'>
        <Attribute name='manual' value='true'/>
     </Attribute>
```

Y sustitúyalo por esto:

```
<Attribute name='userAssignment'>
        <Object>
            <Attribute name='activateDate' value='true'/>
             <Attribute name='deactivateDate' value='true'/>
             <Attribute name='manual' value='true'/>
        </Object>
    </Attribute>
```

- Para modificar un tipo de rol con el fin de impedir que tenga fechas de activación y de desactivación directamente asignables, busque el atributo `userAssignment` dentro del objeto de rol y elimine los atributos `activateDate` y `deactivateDate` así:

```
<Attribute name='userAssignment'>
        <Object>
        </Object>
    </Attribute>
```

4 **Guarde el objeto de configuración de rol. No es necesario reiniciar los servidores de aplicaciones para que los cambios surtan efecto.**

▼ Para habilitar o inhabilitar elementos de trabajo de aprobaciones de cambio y notificaciones de cambio

Los elementos de trabajo de aprobaciones de cambio están habilitados de manera predeterminada para todos los tipos de roles. Esto significa que cada vez que se cambia un rol (ya sea de negocio, TI, aplicación o activo), si tiene un propietario éste debe aprobar el cambio para que sea efectivo.

Para obtener más información sobre elementos de trabajo de aprobaciones de cambio y de notificaciones de cambios, consulte "Inicio de elementos de trabajo de aprobaciones de cambio y de aprobación" en la página 137.

Para habilitar o inhabilitar elementos de trabajo de aprobaciones de cambio y notificaciones de cambio para tipos de roles, siga estos pasos:

1 **Abra el objeto de configuración de rol para editarlo mediante el procedimiento que se explica en "Edición de objetos de configuración de Identity Manager" en la página 118.**

2 **Busque el objeto de rol correspondiente al tipo de rol que desea editar.**

- Para editar un rol de negocio, busque `Object name='BusinessRole'`
- Para editar un rol de TI, busque `Object name='ITRole'`
- Para editar un rol de aplicación, busque `Object name='ApplicationRole'`
- Para editar un rol de activo, busque `Object name='AssetRole'`

3 **Busque los siguientes atributos en el elemento `<Object>`, que se encuentra en el elemento `<Attribute name='features'>`:**

```
<Attribute name='changeApproval' value='true'/>
 <Attribute name='changeNotification' value='true'/>
```

4 **Defina los valores de atributo en true o false según convenga.**

5 **Si es preciso, repita los pasos 2 - 4 para configurar otro tipo de rol.**

6 **Guarde el objeto de configuración de rol. No es necesario reiniciar los servidores de aplicaciones para que los cambios surtan efecto.**

▼ Para configurar el número máximo de filas que pueden cargarse en la página Listar roles

La página Listar roles de la interfaz de administración puede mostrar un número máximo de filas que es configurable. El número predeterminado es 500. Utilice los pasos indicados en la sección para cambiar el número.

Proceda como sigue para cambiar el número máximo de filas que puede mostrar la página Listar roles.

1. **Abra el objeto de configuración de rol para editarlo mediante el procedimiento que se explica en "Edición de objetos de configuración de Identity Manager" en la página 118.**
2. **Busque el atributo siguiente y cambie el valor:**

   ```
   <Attribute name='roleListMaxRows' value='500'/>
   ```

3. **Guarde el objeto de configuración de rol. No es necesario reiniciar los servidores de aplicaciones para que los cambios surtan efecto.**

Sincronización de roles y roles de recursos de Identity Manager

Los roles de Identity Manager pueden sincronizarse con los roles creados nativamente en un recurso. Al sincronizarlo, el recurso se asigna al rol de manera predeterminada. Esto se aplica a los roles creados con la tarea de sincronización y a los roles de Identity Manager que coinciden con uno de los nombres de rol de recursos.

▼ Para sincronizar un rol de Identity Manager con un rol de recursos

1. **En la interfaz de administración, seleccione Tareas de servidor en el menú principal.**
2. **Haga clic en Ejecutar tareas. Aparece la página Tareas disponibles.**
3. **Haga clic en la tarea Sincronizar roles de Identity System (Sistema de identidad) con los roles de recursos.**
4. **Rellene el formulario. Haga clic en Ayuda para obtener más información.**
5. **Seleccione Ejecutar.**

Conceptos y administración de recursos de Identity Manager

En esta sección encontrará información y procedimientos para configurar los recursos de Product_IDMgr;.

¿Qué son los recursos?

Los recursos de Identity Manager almacenan información sobre cómo conectarse a un recurso o un sistema en el que se crean las cuentas. Los recursos de Identity Manager definen los atributos relevantes de un recurso y ayudan a especificar cómo se muestra la información de los recursos en Identity Manager.

Identity Manager ofrece recursos para una gran variedad de tipos, entre ellos:

- Administradores de seguridad de sistemas centrales (mainframe)
- Bases de datos
- Servicios de directorio
- Sistemas operativos
- Sistemas ERP (Planificación de recursos empresariales)
- Plataformas de mensajería

El área Recursos de la interfaz

Identity Manager muestra información sobre los recursos existentes en la página Recursos.

Para acceder a los recursos, seleccione Recursos en la barra de menús.

Los recursos de la lista se agrupan por tipos. Cada tipo de recurso se representa mediante un icono de carpeta. Para ver los recursos definidos actualmente, haga clic en el indicador existente junto a la carpeta. Haga clic de nuevo en el indicador para contraer la vista.

Cuando se expande una carpeta de tipo de recurso, se actualiza dinámicamente y muestra el número de objetos de recurso que contiene (si se trata de un tipo de recurso que admite grupos).

Algunos recursos tienen otros objetos que puede administrar, por ejemplo:

- Organizaciones
- Unidades organizativas
- Grupos
- Roles

Elija un objeto en la lista de recursos y después seleccione en las listas de opciones siguientes para iniciar una tarea de administración:

- **Acciones de recurso**. Permite efectuar numerosas acciones en los recursos, como edición, sincronización activa, cambio de nombre y eliminación, además de trabajar con objetos de recurso y gestionar conexiones de recursos.
- **Acciones de objeto de recurso**. Edición, creación, eliminación, cambio de nombre, guardar como y búsqueda de objetos de recurso.
- **Acciones de tipo de recurso**. Edición de directivas de recursos, uso del índice de cuentas y configuración de los recursos administrados.

Cuando se crea o edita un recurso, Identity Manager inicia el flujo de trabajo `ManageResource`. Este flujo de trabajo guarda el recurso nuevo o actualizado en el depósito y le permite insertar aprobaciones u otras acciones antes de crear o guardar el recurso.

Administración de la lista de recursos

Para poder crear un recurso nuevo, debe indicar a Identity Manager qué tipos de recursos desea poder administrar. Para habilitar recursos y crear recursos personalizados, utilice la página Configurar recursos administrados.

▼ Para abrir la página Configurar recursos administrados

Siga estos pasos para abrir la página Configurar recursos administrados:

1. **Inicie la sesión en la interfaz de administración.**

2. **Haga clic en la ficha Recursos.**

   Utilice uno de estos métodos para abrir la página Configurar recursos administrados:

   - Busque la lista desplegable Acciones de tipo de recurso y elija Configurar recursos administrados.
   - Haga clic en la ficha Configurar tipos.

   Aparece la página Configurar recursos administrados.

   Esta página consta de tres secciones:

   - **Conectores de recursos**. Esta sección contiene los tipos de conectores de recursos, la versión del conector y el servidor de conectores.
   - **Adaptadores de recursos**. En esta sección aparecen los tipos de recursos que suelen encontrarse en los grandes entornos de empresa. En la columna Versión se indica la versión del adaptador de Identity Manager que se conecta al recurso.
   - **Adaptadores de recursos personalizados**. En esta sección se agregan recursos personalizados a la lista Recursos.

▼ Para habilitar tipos de recursos

Puede habilitar un tipo de recurso desde la página Configurar recursos administrados como se indica a continuación.

1. **Abra la página Configurar recursos administrados si aún no está abierta ("Administración de la lista de recursos" en la página 161).**
2. **En la sección Recursos, marque la casilla de la columna ¿Administrado? correspondiente al tipo de recurso que desea habilitar.**

   Para habilitar todo los tipos de recursos enumerados, seleccione Administrar todos los recursos.
3. **Haga clic en Guardar en la parte inferior de la página.**

   El recurso se agrega a la lista Recursos.

▼ Para agregar un recurso personalizado

Puede agregar un recurso personalizado desde la página Configurar recursos administrados como se indica a continuación.

1. **Abra la página Configurar recursos administrados si aún no está abierta ("Administración de la lista de recursos" en la página 161).**
2. **En la sección Recursos personalizados, seleccione Añadir recurso personalizado**
3. **Introduzca la ruta de clase del recurso o un recurso personalizado creado. En el caso de los adaptadores suministrados con Identity Manager, consulte la ruta de clase completa en *Sun Identity Manager 8.1 Resources Reference* .**
4. **Pulse Guardar para añadir el recurso a la lista Recursos.**

▼ Para crear un recurso

Una vez habilitado un tipo de recurso, puede crear una instancia del recurso en Identity Manager. Use el *Asistente de recursos* para crear un recurso.

El Asistente de recursos le guía por la configuración de los siguientes elementos.

- **Parámetros específicos del recurso**. Estos valores se pueden modificar mediante la interfaz de Identity Manager al crear una instancia concreta de este tipo de recurso.
- **Atributos de cuenta**. Se definen en la asignación de esquemas para el recurso. Determinan cómo se asignan los atributos de usuario de Identity Manager a los atributos del recurso.
- **ND de cuenta o plantilla de identidad**. Incluye la sintaxis del nombre de cuenta para los usuarios, que adquiere especial importancia con los espacios de nombres jerárquicos.

- **Parámetros de Identity Manager para el recurso** Configura las directivas, establece los aprobadores de recursos y configura el acceso de la organización al recurso.

1 **Inicie la sesión en la interfaz de administración.**

2 **Haga clic en la ficha Recursos. Asegúrese de que esté seleccionada la ficha secundaria Listar recursos.**

3 **Busque la lista desplegable Acciones de tipo de recurso y elija Nuevo recurso.**

Aparece la página "Nuevo recurso".

4 **Seleccione un tipo de recurso en la lista desplegable. (Si no aparece el tipo de recurso que busca, deberá habilitarlo. Consulte "Administración de la lista de recursos" en la página 161.)**

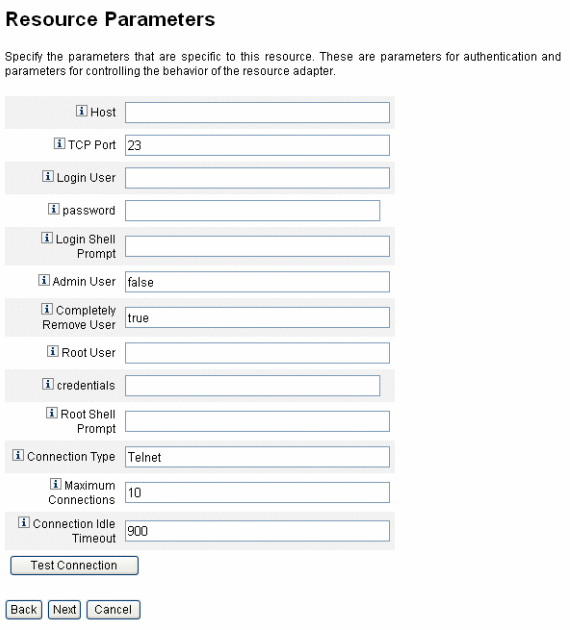
5 **Pulse Nuevo para acceder a la página de bienvenida del Asistente de recursos.**

6 **Pulse Siguiente para empezar a definir el recurso.**

El Asistente de recursos recorre y muestra las páginas por el orden siguiente:

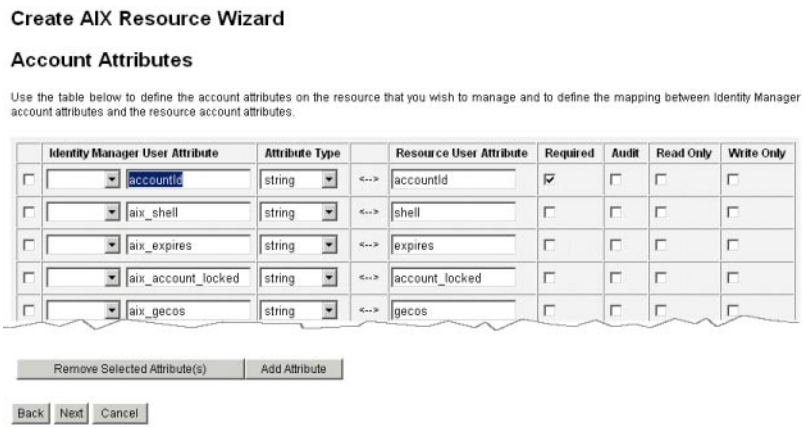
- **Parámetros de recurso**. Configure los parámetros específicos del recurso que controlan la autenticación y el comportamiento del adaptador de recursos. Introduzca los parámetros y pulse Conexión de prueba para asegurarse de que la conexión es válida. Al confirmar, pulse Siguiente para configurar los atributos de cuenta.

  La figura siguiente muestra la página Parámetros de recurso para recursos de Solaris. Los campos del formulario de esta página varían según los recursos.



- **Atributos de cuenta** *(asignación de esquema)*. Asigna atributos de cuenta de Identity Manager a atributos de cuenta de recursos. Encontrará más información sobre los atributos de cuentas de recursos en el apartado "Para ver o editar atributos de cuentas de recursos" en la página 169.
  - Para agregar un atributo, haga clic en Añadir atributo.
  - Para suprimir uno o varios atributos, marque las casillas correspondientes a los mismos y pulse Suprimir atributos seleccionados.

    La figura siguiente muestra la página Atributos de cuenta en el Asistente de recursos.



Nota – Si desea exportar atributos a la tabla `EXT_RESOURCEACCOUNT_ACCTATTR` , debe marcar la casilla Auditar para cada atributo que quiera exportar.

Cuando termine, pulse Siguiente para configurar la plantilla de identidad.

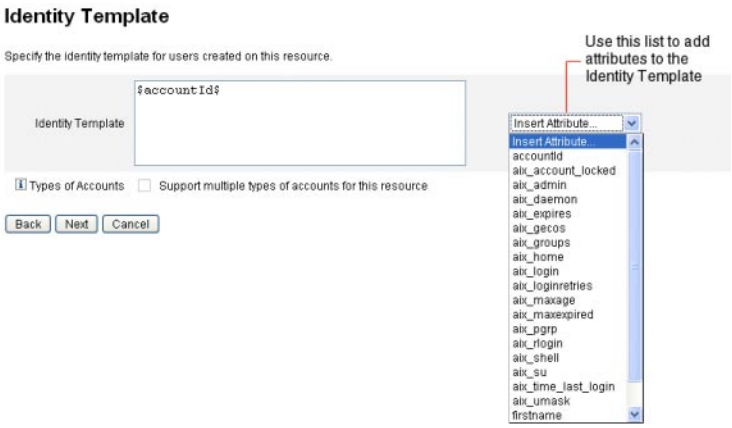
- **Plantilla de identidad**. Define la sintaxis de nombre de cuenta para los usuarios. Esta función adquiere especial relevancia con los espacios de nombres jerárquicos.
  - Para agregar un atributo a la plantilla, selecciónelo en la lista Insertar atributo.
  - Para eliminar un atributo, resáltelo en la cadena y pulse la tecla de supresión. Elimine el nombre de atributo, así como los caracteres $ (símbolo del dólar) que aparecen delante y detrás del nombre.
  - **Tipo de cuentas**. Identity Manager permite asignar varias cuentas de recursos a un mismo usuario. Por ejemplo, un usuario puede necesitar tanto una cuenta de nivel de administrador como una cuenta normal para un recurso particular. Para permitir varios tipos de cuenta en este recurso, marque la casilla Tipos de cuentas.

    Nota – No es posible seleccionar la casilla Tipos de cuentas sin haber creado una o varias reglas de generación de identidades con el subtipo `IdentityRule`. Como los id de cuenta deben ser distintos, los diferentes tipos de cuenta deben generar diferentes id de cuenta para un usuario específico. Las reglas de generación de identidades determinan cómo se crean esos id de cuenta únicos.

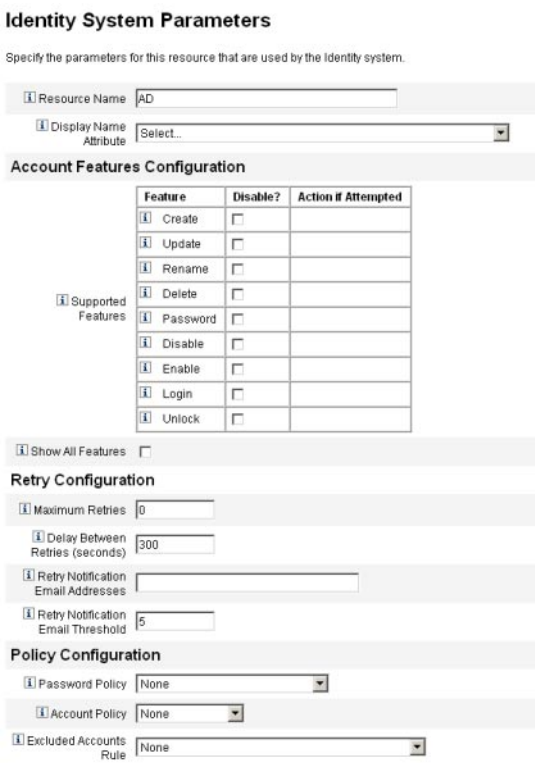
    El archivo `sample/identityRules.xml` ofrece ejemplos de reglas de identidades.

    No es posible suprimir un tipo de cuenta mientras otros objetos hagan referencia a él dentro de Identity Manager. Tampoco es posible cambiar de nombre un tipo de cuenta.

Encontrará más información para rellenar el formulario de tipo de cuentas en la ayuda en línea de Identity Manager. Para obtener más información sobre la creación de varias cuentas de recursos para un usuario, consulte "Creación de varias cuentas de recursos para un usuario" en la página 61.



- **Parámetros del sistema Identity**. Define los parámetros de Identity Manager para el recurso, incluida la configuración de directivas y reintentos, como se indica en el apartado "Para crear un recurso" en la página 162.



7 **Use Siguiente y Retroceder para moverse entre las páginas. Cuando haya seleccionado todo lo que le interesa, pulse Guardar para guardar el recurso y volver a la página de la lista.**

Administración de recursos

A continuación se explica cómo administrar los recursos existentes.

Esta información se ha dividido como sigue:

▼ Para ver la lista de recursos

Los recursos existentes pueden verse en la Lista de recursos.

1 **Inicie la sesión en la interfaz de administración.**

2 **Seleccione Recursos en el menú principal.**

Aparece la Lista de recursos en la ficha secundaria Listar recursos.

▼ Para editar un recurso con el Asistente de recursos

El Asistente de recursos sirve para editar parámetros de recurso, atributos de cuenta y parámetros del sistema de identidades. También es posible especifique la plantilla de identidad que debe aplicarse a los usuarios creados en el recurso.

1 **En la interfaz de administración de Identity Manager, seleccione Recursos en el menú principal.**

Aparece la Lista de recursos en la ficha secundaria Listar recursos.

2 **Elija el tipo de recurso que desea editar.**

3 **En el menú desplegable Acciones de recurso, seleccione Asistente de recursos (dentro de Editar).**

El Asistente de recursos se abre en el modo de edición para el recurso seleccionado.

▼ Para editar un recurso con comandos de la lista de recursos

Además del Asistente de recursos, también se pueden realizar diversas acciones en un recurso con los comandos de la lista de recursos.

1 **Seleccione una o más opciones en la lista de recursos.**

Las opciones incluyen:

- **Eliminar recursos**. Seleccione uno o varios recursos y después elija Eliminar en la lista Acciones de recurso. Es posible seleccionar recursos de varios tipos simultáneamente. No se puede eliminar un recurso si tiene asociado algún rol o grupo de recursos.
- **Buscar objetos de recurso**. Seleccione un recurso y después Buscar objeto de recurso en la lista Acciones de objeto recurso para buscar un objeto de recurso (como una organización, unidad organizativa, grupo o persona) según las características del objeto.
- **Administrar objetos de recurso**. Es posible crear objetos nuevos para algunos tipos de recursos. Seleccione el recurso y, a continuación, seleccione Crear objeto de recurso en la lista Acciones de objeto de recurso.
- **Cambiar nombre de recursos**. Elija un recurso y seleccione Cambiar nombre en la lista Acciones de recurso. Introduzca un nombre nuevo en el cuadro de entrada que aparece y pulse Cambiar nombre.
- **Clonar recursos**. Elija un recurso y seleccione Guardar como en la lista Acciones de recurso. Introduzca un nombre nuevo en el cuadro de entrada que aparece. El recurso clonado aparece en la lista de recursos con el nombre elegido.

- **Operaciones masivas con recursos**. Especifique una lista de recursos y acciones (en formato de entrada CSV) para aplicar a todos los recursos de la lista. A continuación, ejecute las operaciones masivas para iniciar la tarea correspondiente en segundo plano.

2 **Guarde las modificaciones.**

▼ Para ver o editar atributos de cuentas de recursos

Los atributos de cuentas de recursos (o asignaciones de esquemas) ofrecen un método abstracto para hacer referencia a los atributos en los recursos administrados. La asignación de esquemas le permite especificar cómo se hace referencia a los atributos dentro de Identity Manager (la parte izquierda de la asignación de esquema) y cuál será la equivalencia de cada nombre con el nombre del atributo en el recurso real (la parte derecha de la asignación de esquema). Tras ello puede hacer referencia al nombre de atributo de Identity Manager dentro de los formularios y las definiciones de flujo de trabajo, así como referirse efectivamente al atributo en el propio recurso.

Éste es un ejemplo de asignación entre atributos de Identity Manager y de un recurso LDAP:

Atributo de Identity Manager		Atributo de recurso LDAP
`firstname`	`<-->`	`givenName`
`lastname`	`<-->`	`sn`

Cualquier referencia al atributo de Identity Manager, `firstname`, es en realidad una referencia al atributo LDAP, `givenName`, cuando se realiza una acción en ese recurso.

Cuando se administran diversos recursos desde Identity Manager, la asignación de un atributo de cuenta común de Identity Manager a muchos atributos de recurso puede simplificar rotundamente la administración de los recursos. Por ejemplo, el atributo `fullname` de Identity Manager puede asignarse al atributo de recurso `displayName` de Active Directory. Por otro lado, en un recurso LDAP resource, el mismo atributo `fullname` de Identity Manager puede asignarse al atributo LDAP `cn`. En consecuencia, al administrador le basta con suministrar el valor de `fullname` una vez. Al guardar el usuario, el valor de `fullname` se transfiere a los recursos que tienen distintos nombres de atributo.

Si configura una asignación de esquemas en la página Atributos de cuenta del Asistente de recursos, puede hacer lo siguiente:

- Definir nombres de atributo y tipos de datos para los atributos procedentes de recursos administrados.
- Limitar los atributos de recursos únicamente a los esenciales para su empresa u organización.

- Crear nombres de atributos comunes de Identity Manager para usarlos con múltiples recursos.
- Identificar los atributos de usuario y los tipos de atributo necesarios.

Para ver o editar atributos de cuentas de recursos, siga estos pasos:

1 **En la interfaz de administración, seleccione Recursos.**

2 **Seleccione el recurso cuyos atributos de cuenta desea ver o editar.**

3 **En la lista Acciones de recurso, elija Editar esquema de recurso.**

Aparece la página Editar Atributos de cuenta de recursos.

La columna izquierda de la asignación de esquemas (denominada Atributo de usuario de Identity System (Sistema de identidad)) contiene los nombres de los atributos de cuenta de Identity Manager referenciados en los formularios que se utilizan en las interfaces de administración y de usuario de Identity Manager. La columna derecha de la asignación de esquemas (denominada Atributo de usuario de recurso) contiene los nombres de los atributos del origen externo.

Grupos de recursos

Aproveche el área de recursos para administrar los grupos de recursos, lo que permite actualizar los recursos de los grupos por el orden elegido. Al incluir y ordenar recursos en un grupo y asignarlo a un usuario, determina el orden en que se crean, actualizan y eliminar los recursos de ese usuario.

Las actividades se realizan sucesivamente en cada recurso. Si falla una acción en un recurso, los demás recursos no se actualizan. Este tipo de relación es importante para los recursos relacionados.

Por ejemplo, un recurso de Exchange Server 2007 depende de una cuenta existente de Windows Active Directory. Esta cuenta ya debe existir para poder crear correctamente la cuenta de Exchange. Al crear un grupo de recursos (ordenados) con un recurso de Windows Active Directory y un recurso de Exchange Server 2007, se asegura de que la secuencia es correcta al crear usuarios. Recíprocamente, este orden garantiza que los recursos se eliminan en la secuencia correcta cuando se eliminan usuarios.

Seleccione Recursos y después Listar grupos de recursos para ver una lista de los grupos de recursos definidos actualmente. En esa página, pulse Nuevo para definir un grupo de recursos. Al definir un grupo de recursos, un área de selección permite elegir y después ordenar los recursos elegidos, así como seleccionar las organizaciones para las que debe estar disponible el grupo.

Directiva global de recursos

En esta sección se explica cómo editar la Directiva global de recursos y configurar valores de tiempo de espera para un recurso.

▼ Para editar atributos de directiva

Puede editar atributos de directiva de recursos en la página Editar atributos de directiva de recurso global.

1 **Abra la página Editar atributos de directiva de recurso global y edite los atributos como interese.**

Los atributos incluyen:

- **Tiempo predeterminado de espera de captura**. Introduzca un valor en milisegundos que especifique el máximo tiempo que el adaptador debe esperar en el indicador de línea de comandos antes de que finalice el tiempo de espera. Este valor se aplica únicamente a los adaptadores GenericScriptResourceAdapter o ShellScriptSourceBase. Utilícelo cuando los resultados de un comando o secuencia de comandos sean importantes y los vaya a analizar el adaptador.

  El valor predeterminado es 30000 (30 segundos).
- **Espera predeterminada para tiempo de espera** Introduzca un valor en milisegundos para especificar el máximo tiempo que un adaptador con secuencia de comandos debe esperar entre sondeos antes de comprobar si un comando tiene preparados caracteres (o resultados). Este valor se aplica únicamente a los adaptadores GenericScriptResourceAdapter o ShellScriptSourceBase. Utilícelo cuando el adaptador no examine los resultados de un comando o secuencia de comandos.
- **Tiempo de espera de Ignorar MAY/min**. Introduzca un valor en milisegundos para especificar el tiempo máximo que el adaptador debe esperar a recibir el indicador de línea de comandos antes de que finalice el tiempo de espera. Este valor se aplica únicamente a los adaptadores GenericScriptResourceAdapter o ShellScriptSourceBase. Utilícelo cuando la diferenciación entre mayúsculas y minúsculas sea irrelevante.
- **Directiva de contraseñas de cuentas de recursos**. Si procede, seleccione una directiva de contraseñas de cuentas de recurso para aplicarla al recurso elegido. La selección predeterminada es Ninguna.
- **Regla de cuentas de recursos excluidos**. Si procede, seleccione una regla para regir las cuentas de recursos excluidos. La selección predeterminada es Ninguna.

2 **Debe pulsar Guardar para guardar los cambios realizados en la directiva.**

▼ Para definir otros valores de tiempo de espera

La propiedad `maxWaitMilliseconds` se puede modificar editando el archivo `Waveset.properties`. La propiedad `maxWaitMilliseconds` determina la frecuencia con que se supervisa el tiempo de espera de una operación. Si especifica este valor, el sistema utilizará un valor predeterminado de 50.

1. **Incluya la línea siguiente en el archivo** `Waveset.properties`**:**

   ```
   com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
   ```

2. **Guarde el archivo.**

Acciones masivas de recurso

Se pueden realizar operaciones masivas en los recursos utilizando un archivo con formato CSV o creando o especificando los datos que deben aplicarse en la operación.

La Figura 5–13 muestra la página de inicio de operaciones masivas utilizando una acción Crear.

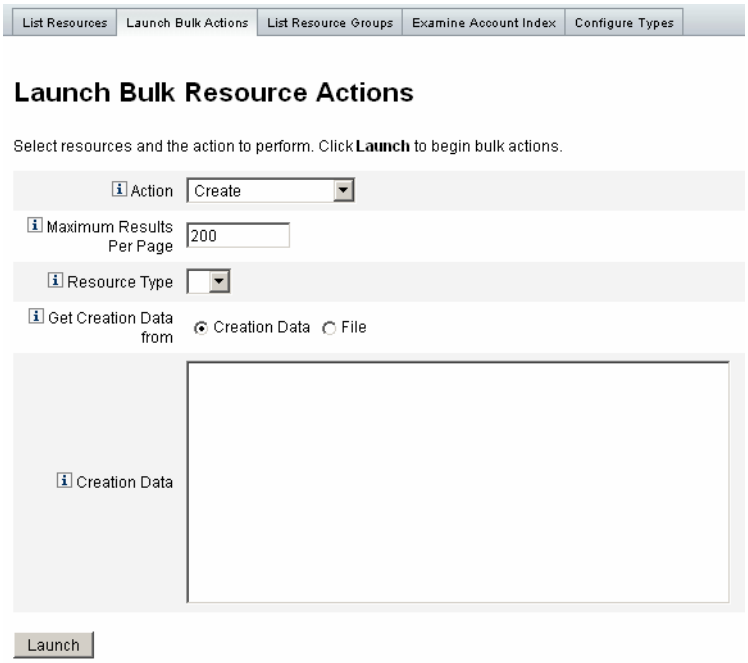


FIGURA 5–13 Página Iniciar acciones masivas de recurso

Las opciones disponibles para la operación masiva de recurso dependen de la acción seleccionada para la operación. Puede especificar una sola acción para aplicarla a la operación o bien elegir diversas acciones De lista de acciones.

- **Acciones**. Para especificar una única acción, elija una de estas opciones: crear, clonar, actualizar, eliminar, cambiar contraseña, reinicializar contraseña.

  Si selecciona una sola acción, se le ofrecen opciones para indicar el recurso implicado en la acción. En el caso de una acción Crear, debe especificar el tipo de recurso.

  Si indica De lista de acciones, utilice el área Obtener lista de acciones de para especificar bien el archivo que contiene las acciones o bien las acciones que indique en el área Entrada.

  Nota – Debe utilizar un formato de valores separados por comas para las acciones introducidas en la lista del área de entrada o en el archivo.

- **Número máximo de resultados por página**. Con esta opción se especifica el número máximo de resultados de acciones masivas que se deban mostrar en cada página de resultados de tareas. El valor predeterminado es 200.

Pulse Ejecutar para comenzar la operación, que se ejecuta como una tarea en segundo plano.

Conceptos y administración de recursos externos

Identity Manager también sirve para crear, abastecer y administrar centralizadamente los *recursos externos* de la empresa.

En esta sección se explica cómo trabajar con recursos externos a lo largo de los siguientes apartados:

¿Qué son los recursos externos?

Un *recurso externo* es un tipo de recurso único que no almacena directamente información de cuentas de usuario. Se trata de un recurso ajeno a las labores de Identity Manager. Estos recursos pueden ser equipos de sobremesa, portátiles, teléfonos móviles, dispositivos de seguridad, etc.

Para abastecer los recursos externos siempre se necesitan uno o varios procesos manuales. Por ejemplo, tras efectuar la solicitud inicial y obtener las aprobaciones adecuadas para abastecer un equipo portátil para un nuevo empleado, quizá debe enviar una solicitud de pedido de compra al sistema de peticiones de compra de la empresa. Una vez rellenado el pedido, tal vez alguien deba preconfigurar el portátil con las aplicaciones de la empresa y después entregárselo personalmente al nuevo empleado para completar la solicitud de abastecimiento.

¿Por qué utilizar recursos externos?

El uso de Identity Manager para abastecer recursos externos le permite notificar las solicitudes pendientes a uno o varios abastecedores, con información detallada sobre lo que se debe abastecer.

Por ejemplo, un abastecedor de recursos externos podría ser un responsable de TI que necesita solicitar y preconfigurar manualmente un portátil para un usuario.

Identity Manager también mantiene información sobre los recursos externos abastecidos para un determinado usuario y actualiza dicha información al completar la solicitud de abastecimiento. A continuación, Identity Manager deja disponible esta información para visualizarla, generar informes, auditar la validación del cumplimiento y exportarla.

Nota – Para configurar recursos externos se necesita la capacidad Administrador de recursos externos. Para crear nuevos recursos externos se necesita la capacidad Administrador de recursos.

Configuración de recursos externos

En esta sección se describe el proceso de configuración del almacén de datos de recursos externos y la notificación al abastecedor de recursos externos.

Configuración del almacén de datos de recursos externos

El almacén de datos de recursos externos de Identity Manager constituye un único alojamiento para la información sobre los recursos externos y sus asignaciones. Este almacén puede ser una base de datos o un directorio.

- Si el almacén de datos de recursos externos es una *base de datos*, lo gestiona el adaptador ScriptedJdbcResourceAdapter.
- Si el almacén de datos de recursos externos es un *directorio*, lo gestiona el adaptador LDAPResourceAdapter.

Nota – Para configurar el almacén de datos de recursos externos se necesita la capacidad Administrador de recursos externos.

El almacén de datos de recursos externos le permite almacenar la información en los valores de atributo que le interesen, así como incluir dichos valores en una o varias tablas.

Por ejemplo, si utiliza una base de datos MySQL, Identity Manager almacena la información de recursos externos en las tablas siguientes:

- La tabla `extres.accounts`, que contiene los ID de cuenta y de recurso (accountID y resourceID). Como el almacén de datos de recursos externos es un alojamiento único, Identity Manager proporciona una clave de ID única, `<accountId>@<resourceId>` , que identifica a una cuenta en exclusiva por su ID de recurso.
- La tabla `extres.attributes`, que contiene un conjunto de atributos de par nombre/valor. Estos atributos se definen en la asignación de esquemas al crear un recurso externo.

Las secuencias de comandos de ejemplo utilizadas para crear las tablas de base de datos se incluyen con Identity Manager en la siguiente ubicación:

wshome`/sample/ScriptedJdbc/External`

Identity Manager es compatible con numerosos tipos de bases de datos, para cada uno de los cuales ofrece secuencias de comandos de ejemplo. Puede modificar estas secuencias de comandos como requiera su entorno específico.

El almacén de datos de recursos externos también es compatible con LDAP mediante el adaptador LDAPResourceAdapter, que permite almacenar la información en clases existentes o personalizadas. Con Identity Manager también se incluye una secuencia de comandos de ejemplo LDIF en la siguiente ubicación:

wshome`/sample/other/externalResourcePerson.ldif`

Puede modificar esta secuencia de comandos al configurar un almacén de datos de directorio de recursos externos.

▼ Para configurar un almacén de datos de base de datos

Aunque es muy fácil introducir cambios, el almacén de datos de recursos externos sólo suele configurarse una vez. Si modifica la configuración, Identity Manager actualiza automáticamente todos los recursos externos existentes para utilizar el almacén de datos recién configurado.

Siga estos pasos para configurar un almacén de datos de base de datos:

1 **Seleccione Configurar → Recursos externos en la barra de menús de la interfaz de administración de Identity Manager.**

2 Cuando aparezca la página Configuración de almacén de datos, elija Base de datos en el menú Tipo de almacén de datos. Aparecen más opciones.

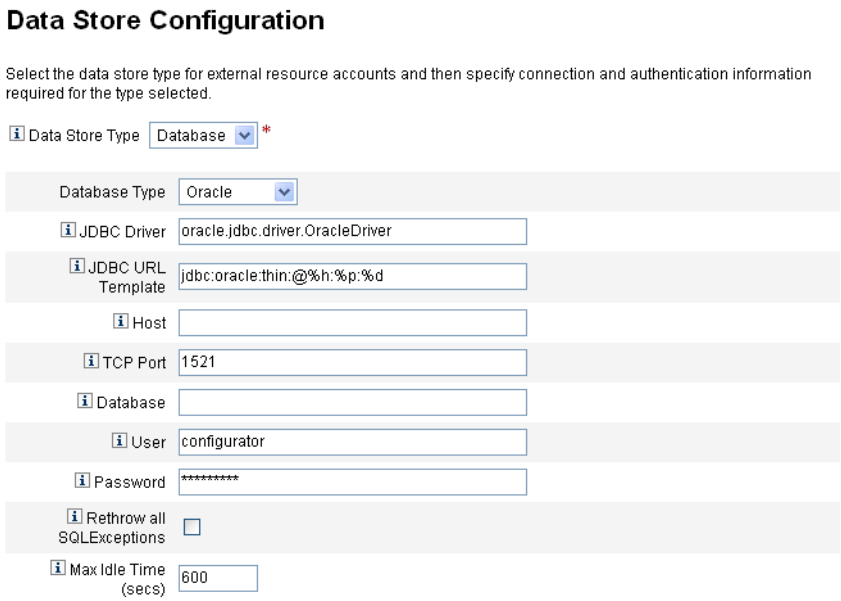


FIGURA 5–14 Página Configuración de almacén de datos: base de datos

3 Especifique la siguiente información de conexión y autenticación:

Nota – Identity Manager rellena automáticamente con los valores predeterminados los campos Controlador JDBC, Plantilla URL de JDBC, Puerto y Tiempo máx. de inactividad (segs). Si es preciso, puede cambiar estos valores.

- **Controlador JDBC**. Especifique el nombre de la clase del controlador JDBC.
- **Plantilla URL de JDBC**. Especifique la plantilla URL del controlador JDBC.
- **Host**. Introduzca el nombre del servidor en el que se está ejecutando la base de datos.
- **Puerto TCP**. Introduzca el puerto en el que la base de datos recibe las consultas.
- **Base de datos**. Introduzca el nombre de la base de datos presente en el servidor de base de datos que contiene la tabla.
- **Usuario**. Introduzca el ID de un usuario de base de datos con permisos suficientes para leer, actualizar y eliminar filas de la tabla de la base de datos. Por ejemplo, root.
- **Password**. Introduzca la contraseña del usuario de la base de datos.

- **Volver a enviar todas las SQLExceptions**. Marque esta casilla para volver a enviar las excepciones SQL a las sentencias SQL si los códigos de error de excepción son 0.

  Si no habilita esta opción, Identity Manager intercepta y elimina estas excepciones.
- **Tiempo máx. de inactividad (segs)**. Introduzca el tiempo máximo de inactividad en segundos que una conexión JDBC deba permanecer sin usar en un grupo.

  Si la conexión no se utiliza antes de que transcurra el tiempo especificado, Identity Manager la cerrará y la quitará del grupo.
  - El valor predeterminado es 600 segundos.
  - Con el valor `-1` la conexión nunca caduca.

4 **Tras conectarse satisfactoriamente al almacén de datos, debe especificar una varias secuencias de comandos para que se ejecuten con cada acción de recurso admitida. Consulte las instrucciones en el apartado "Para configurar secuencias de comandos de acción" en la página 177.**

▼ Para configurar secuencias de comandos de acción

Debe especificar un conjunto de secuencias de comandos de BeanShell (`bsh`) que Identity Manager pueda utilizar para efectuar un seguimiento y ejecutar los estados Obtener, Crear, Actualizar, Eliminar, Habilitar, Inhabilitar y Probar de una solicitud determinada.

Encontrará secuencias de comandos de ejemplo en:

wshome`/sample/ScriptedJdbc/External/beanshell`

Nota – Estos ejemplos se pueden modificar para crear sus propias secuencias de comandos personalizadas. Las secuencias de comandos se añaden a la herramienta de selección Secuencias de comandos de acción y se muestran bajo la línea de las listas Disponible y Seleccionado.

Identity Manager proporciona secuencias de comandos de ejemplo para las acciones de recurso y los tipos de bases de datos admitidos para los recursos externos. Para acceder a estas secuencias de comandos, utilice las denominadas ResourceAction, que se encuentran en:

wshome`/sample/ScriptedJdbc/External/beanshell`

De manera predeterminada, el nombre de la base de datos, el de usuario y la contraseña son `extres`.

- Si elige cualquiera de las demás opciones de base de datos o prefiere utilizar otro nombre de usuario o de base de datos, debe modificar consiguientemente los valores de los ejemplos de secuencias de comandos de creación de base de datos y ResourceAction.

Por ejemplo, si elige una base de datos MySQL y quiere cambiar el nombre de la base de datos, de usuario y la contraseñas existentes, deberá realizar estos cambios: actualizar la secuencia de comandos `create_external_tables.mysql` cambiando el valor predeterminado `extres` del nombre de base de datos, el nombre de usuario y la contraseña a `externalresources`, `externaladmin` y `externalpassword`, respectivamente.

- A continuación, en las secuencias ResourceAction cambie los valores predeterminados `extres.accounts` y `extres.attributes` a `externalresources.accounts` y `externalresources.attributes` , respectivamente.

Para configurar las secuencias de comandos de acción, siga estos pasos:

1 **Use las herramientas de selección Secuencias de comandos de acción de la página Configuración de almacén de datos para especificar una o más secuencias de comandos de acción para cada acción de recurso. Debe seleccionar al menos una secuencia por acción de recurso.**

FIGURA 5–15 Área Secuencias de comandos de acción

Ha de seleccionar la secuencia de comandos de acción correspondiente a la acción de recurso. Por ejemplo, utilice:

- `External-getUser-bsh` para las acciones de recurso GetUser

Nota – Las acciones de recurso GetUser se utilizan en las operaciones de búsqueda.

- `External-createUser-bsh` para las acciones de recurso CreateUser
- `External-deleteUser-bsh` para las acciones de recurso DeleteUser

- `External-updateUser-bsh` para las acciones de recurso UpdateUser
- `External-disableUser-bsh` para las acciones de recurso DisableUser
- `External-enableUser-bsh` para las acciones de recurso EnableUser
- `External-test-bsh` para las acciones de recurso Test

Nota – Las acciones de recurso Test se utilizan para habilitar la funcionalidad completa del botón Conexión de prueba.

Cualquier otra secuencia de comandos `bsh` de ejemplo que seleccione no funcionará.

2 Elija un Modo de contexto de acción en el menú para especificar cómo deben transferirse los valores de atributo a las secuencias de comandos de acción.

- **Cadenas**. Los valores de atributo se transfieren como valores de cadena.
- **Directo**. Los valores de atributo se transfieren como un objeto `com.waveset.object.AttributeValues`.

3 Éste es un buen momento para probar la configuración de la conexión al almacén de datos. Pulse el botón Conexión de prueba, que se halla en la parte inferior de la página.

Aparece un mensaje para indicar si la conexión es correcta o errónea.

4 Cuando termine, pulse Siguiente para continuar en la página Configuración de notificación a abastecedores.

▼ Para configurar un almacén de datos de directorio

Siga estos pasos para configurar un almacén de datos de directorio:

1 Seleccione Directorio en el menú Tipo de almacén de datos. Aparecen más opciones.

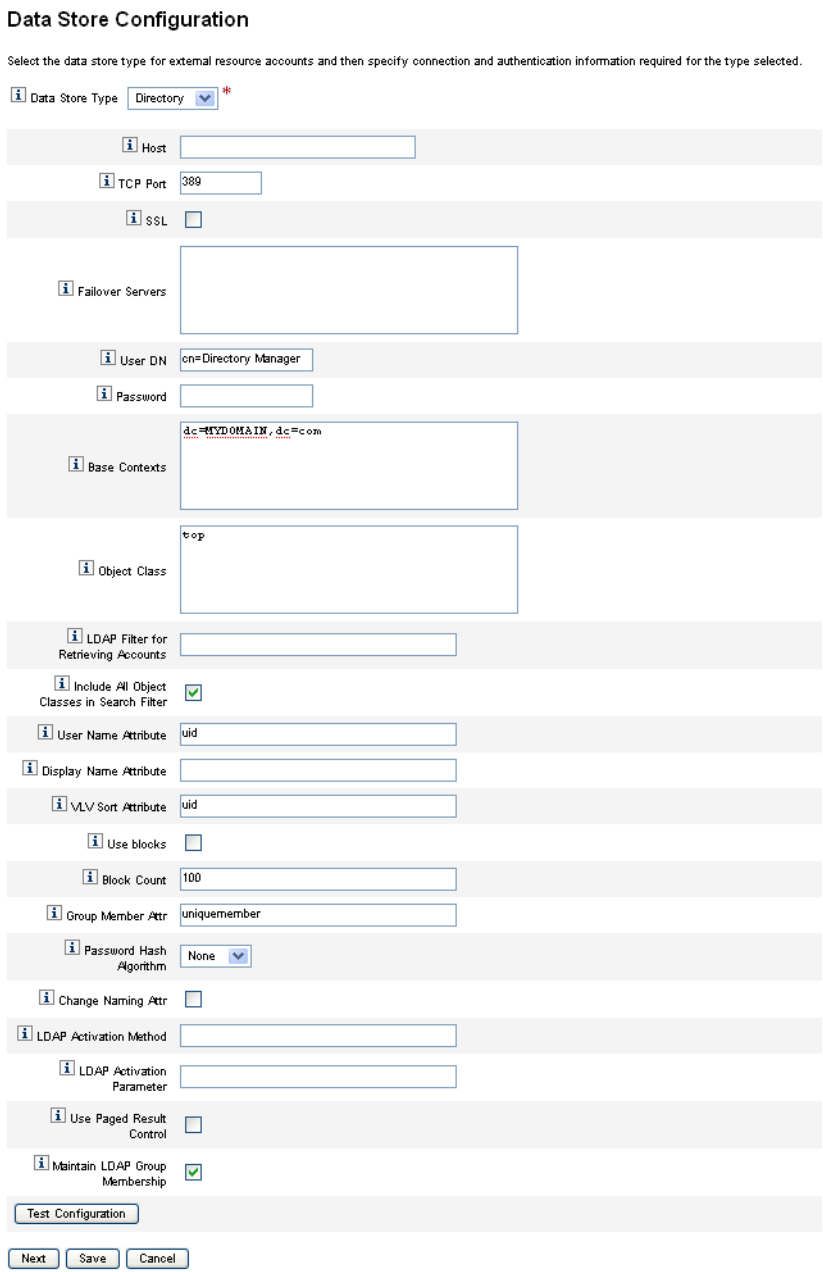


FIGURA 5–16 Página Configuración de almacén de datos: directorio

2 Debe especificar la información de conexión y autenticación para un almacén de datos de tipo directorio.

Configure las opciones siguientes:

- **Host**. Introduzca el nombre o la dirección IP del servidor donde se está ejecutando el servidor LDAP.
- **Puerto TCP**. Introduzca el puerto TCP/IP utilizado para comunicarse con el servidor LDAP.
  - Si utiliza SSL, este puerto suele ser 636.
  - Si no utiliza SSL, este puerto suele ser 389.
- **SSL**. Elija esta opción para conectar con el servidor LDAP mediante SSL.
- **Servidores de conmutación por errores**. Lista de todos los servidores que se utilizan para la reconexión de emergencia si falla el servidor preferido. Esta información se debe introducir en el formato indicado a continuación, que respeta las URL estándar de la versión 3 de LDAP descritas en RFC 2255:

  ```
  ldap://ldap.example.com:389/o=LdapFailover
  ```

  En esta configuración sólo son relevantes las porciones de host, puerto y nombre distinguido (nd) de la URL.

  Si falla el servidor preferido, JNDI se conectará automáticamente al siguiente servidor de esta lista.
- **ND de usuario**. Introduzca el nd con el que se autenticará en el servidor LDAP cuando se efectúen actualizaciones. (El valor predeterminado es `cn=Directory Manager`)
- **Password**. Introduzca la contraseña del responsable titular.
- **Contextos base**. Introduzca uno o más puntos de partida que Identity Manager puede usar al buscar usuarios en el árbol LDAP. (El valor predeterminado es `dc=MYDOMAIN,dc=com`)

  Identity Manager efectúa búsquedas al intentar descubrir usuarios del servidor LDAP o cuando se buscan los grupos a los que están afiliados los usuarios.
- **Clase del objeto**. Indique la clase o clases de objeto que se utilizarán al crear nuevos objetos de usuario en el árbol LDAP. (El valor predeterminado es top)

  Cada entrada debe ocupar una línea distinta. No utilice coma ni punto y coma para separar las entradas.

  Determinados servidores LDAP requieren que se especifiquen todas las clases de objeto presentes en la jerarquía de clases. Por ejemplo, tal vez necesite especificar `top`, `person`, `organizationalperson` e `inetorgperson` en lugar de sólo `inetorgperson`.
- **Filtro de LDAP para recuperar cuentas**. Introduzca un filtro de LDAP opcional para controlar las cuentas que se van a devolver procedentes del recurso LDAP. Si no introduce ningún filtro, Identity Manager devolverá todas las cuentas que contienen todas las clases de objeto especificadas.

- **Incluir todas las clases de objeto en el filtro de búsqueda**. Marque esta casilla para que todas las cuentas deban incluir todas las clases de objetos especificadas y coincidir con el filtro indicado en el campo Filtro de LDAP para recuperar cuentas.

  Nota – Esta opción debe habilitarse cuando no se introduce ningún filtro de búsqueda. Si esta opción está inhabilitada, las cuentas que no incluyan todas las clases de objeto especificadas se podrán cargar en Identity Manager con las funciones de reconciliación o carga desde recurso.

  Una vez cargadas, el atributo `objectclass` de la cuenta no se actualiza automáticamente. Si se expone a la interfaz de administración un atributo de una clase sin objeto, se producirá un error si se otorga un valor a este atributo sin modificar el atributo `objectclass`. Para evitar este problema, anule el valor de `objectclass` del formulario de Reconciliación o Cargar desde recurso.
- **Atributo de nombre de usuario**. Introduzca el nombre del atributo LDAP que se asigna al nombre del usuario de Identity Manager cuando se descubren usuarios en el directorio. Este nombre suele ser `uid` o `cn`.
- **Mostrar nombre de atributo**. Introduzca el atributo de cuenta de recursos cuyo valor será utilizado cuando se muestre este nombre de cuenta.
- **Atributo de clasificación VLV**. Especifique el nombre del atributo de clasificación que se utilizará para los índices VLV en el recurso.
- **Utilizar bloques**. Marque esta casilla para recuperar y procesar los usuarios en bloques.

  Cuando se ejecutan operaciones con un gran número de usuarios, éstos se procesan en bloques para reducir la cantidad de memoria utilizada por la operación.
- **Número de bloques**. Introduzca el número máximo de usuarios que pueden agruparse en bloques para procesar.
- **Atributos de miembro de grupo**. Introduzca el nombre del atributo de pertenencia al grupo que se actualizará con el nombre distinguido (ND) del usuario cuando éste se añada al grupo.

  El nombre de atributo depende de la clase de objeto del grupo. Por ejemplo, Sun Java™ System Enterprise Edition Directory Server y otros servidores LDAP utilizan grupos con la clase de objeto `groupOfUniqueNames` y el atributo `uniqueMember`. Otros servidores LDAP utilizan grupos con la case de objeto `groupOfNames` y el atributo member.
- **Algoritmo de cálculo de claves de contraseñas**. Introduzca el algoritmo que deberá utilizar Identity Manager para incluir claves en la contraseña. Los valores admitidos son:
  - `SSHA`
  - `SHA`
  - `SMD5`
  - `MD5`

Si indica 0 o deja vacío este campo, Identity Manager no incluirá calves en las contraseñas y almacenará contraseñas de texto simple en LDAP, a no ser que el servidor LDAP realice el cálculo de claves. Por ejemplo, Sun Java System Enterprise Edition Directory Server incluye claves en las contraseñas.

- **Modificar atributos de nombre**. Marque esta casilla para permitir modificaciones del atributo de usuario que representa el nombre distinguido (ND) relacionado que se encuentra más a la izquierda. Las modificaciones suelen cambiar los atributos de asignación de nombre a `uid` o `cn`.
- **Método de activación de LDAP**.
  - Deje este campo en blanco si quiere que el recurso utilice asignación de contraseñas para habilitar o inhabilitar las acciones.
  - Introduzca la palabra clave (`nsmanageddisabledrole` o `nsaccountlock`), o el nombre de clase que se debe usar para realizar una acción de activación para usuarios de este recurso.
- **Parámetro de activación de LDAP**. Introduzca un valor según cómo haya rellenado el campo Método de activación de LDAP:
  - Si ha especificado la palabra clave `nsmanageddisabledrole`, deberá introducir un valor con este formato:

    IDMAttribute`=CN=nsmanageddisabledrole,`*baseContext*
  - Si ha especificado la palabra clave `nsaccountlock`, deberá introducir un valor con este formato:

    IDMAttribute`=true`
  - Si ha especificado un nombre de clase, deberá introducir un valor con este formato:

    IDMAttribute

Nota – Para obtener más información sobre el Método de activación de LDAP y el Parámetro de activación de LDAP, consulte la guía *Sun Identity Manager 8.1 Resources Reference* .

- **Usar control de resultados paginados**. Marque esta casilla para utilizar el control de resultados paginados de LDAP en lugar del control de VLV para iterar las cuentas durante la reconciliación.

Nota – El recurso debe ser compatible con el control de paginación simple.

- **Mantener miembros de grupo de LDAP** . Marque esta casilla para que el adaptador mantenga los miembros de grupo de LDAP al renombrar o eliminar usuarios.

Si no habilita esta opción, el recurso LDAP mantiene la pertenencia a los grupos.

3 **Pruebe la configuración de la conexión al almacén de datos con el botón Conexión de prueba.**

Aparece un mensaje para indicar si la conexión es correcta o errónea.

4 **Cuando termine, pulse Guardar y después Siguiente para continuar en la página Configuración de notificación a abastecedores.**

Nota – Debe configurar atributos de cuenta válidos y una plantilla de identidad para poder crear usuarios en un recurso LDAP.

Configuración de notificaciones a abastecedores

Una vez configurado el almacén de datos para los recursos externos, debe configurar las notificaciones a los abastecedores. También es posible configurar las notificaciones a los solicitantes. A continuación se explica el proceso para configurar notificaciones con correo electrónico o Remedy.

▼ Para configurar notificaciones por correo electrónico

Nota – Encontrará más información sobre las plantillas de correo electrónico en Configuración de plantillas de tareas.

Siga estas instrucciones para configurar y enviar notificaciones por correo electrónico a uno o varios abastecedores.

1 **En la página Configuración de notificación a abastecedores, seleccione Correo electrónico en el menú Tipo de notificación a abastecedor. Aparecen otras opciones, como ilustra la figura siguiente.**

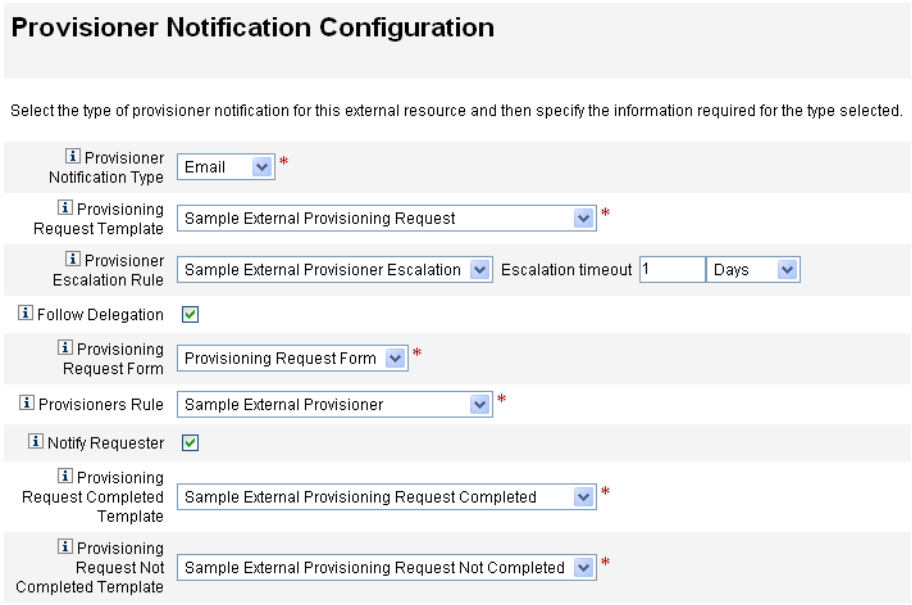


FIGURA 5–17 Página Configuración de notificación a abastecedores: Tipo de notificación por correo electrónico

2 Configure las opciones siguientes:

- **Plantilla de solicitud de abastecimiento**. Elija Ejemplo de solicitud de abastecimiento externa en el menú. Con esta plantilla debe configurar el correo electrónico empleado para notificar a los abastecedores de solicitudes de recursos externos.
- **Seguir delegación**. Marque esta casilla si quiere que Identity Manager siga las delegaciones definidas para el abastecedor.
- **Regla de escalada a abastecedor** (*opcional*). Elija una regla para establecer a qué abastecedor se traslada una solicitud en caso de que el abastecedor actual no responda antes del tiempo de espera indicado.

Nota – Aunque este menú contiene varias reglas de ejemplo, debe seleccionar la regla *Ejemplo de escalada a abastecedor externo* o utilizar una regla propia. La regla Ejemplo de escalada a abastecedor externo aplica una regla de escalada a abastecedor externo para establecer el abastecedor en caso de escalada.

- **Tiempo de espera de escalada**. Indique el máximo tiempo de espera antes de traslada una solicitud de abastecimiento al siguiente abastecedor.

Nota –

- Si deja este campo vacío o introduce un cero, la solicitud nunca se escala.
- Si especifica un tiempo de espera, pero no una Regla de escalada a abastecedor, Identity Manager escalará la solicitud al configurador cuando transcurra el tiempo de espera especificado. Si no hay configurador, la solicitud se clasificará como no completada una vez caducado el tiempo de espera.

- **Formulario de solicitud de abastecimiento**. Elija un formulario que los abastecedores de recursos externos puedan utilizar para marcar como completada o no completada una solicitud de abastecimiento.
- **Regla de abastecedores**. Debe elegir una regla para definir el abastecedor a quien se envían las solicitudes de abastecimiento cuando se asignan recursos externos a los usuarios.

Nota –

- Puede elaborar sus propias reglas al respecto. También es posible definir varios abastecedores. Cuando alguno de ellos complete la tarea, ésta desaparecerá de las colas de todos los abastecedores. Para obtener más información sobre la creación de reglas, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.
- Aunque este menú contiene varias reglas de ejemplo, debe seleccionar la regla *Ejemplo de solicitud de abastecimiento externa* o utilizar una regla propia. La regla Ejemplo de solicitud de abastecimiento externa convierte al configurador en abastecedor.

- **Notificar a solicitante**. Marque esta casilla para devolver por correo electrónico al solicitante original información sobre lo acontecido con la solicitud. Por ejemplo, si se ha completado o no la solicitud de abastecimiento, si se precisa más información, etc.

  Cuando se habilita esta opción, aparecen además estos campos:

Nota –

- **Plantilla de solicitud de abastecimiento completada**. Seleccione la plantilla de solicitud de abastecimiento completada para avisar a los solicitantes cuando se hayan completado sus solicitudes.
- **Plantilla de solicitud de abastecimiento no completada**. Seleccione la plantilla de solicitud de abastecimiento no completada para avisar a los solicitantes cuando no se hayan completado sus solicitudes.

3 **Pulse Guardar.**

Aparece la página Configurar, donde se le indica que puede continuar realizando otra tarea de configuración.

4 **Vaya a la ficha Recursos → Listar recursos. Ahora ya puede crear recursos externos individuales basándose en esta configuración. Consulte las instrucciones en el apartado "Para crear un recurso" en la página 162.**

▼ Para configurar notificaciones de Remedy

Siga estas instrucciones para crear y enviar un ticket de Remedy a los abastecedores.

1 **Seleccione Remedy en el menú Tipo de notificación a abastecedor. Aparecen otras opciones, como ilustra la figura siguiente.**

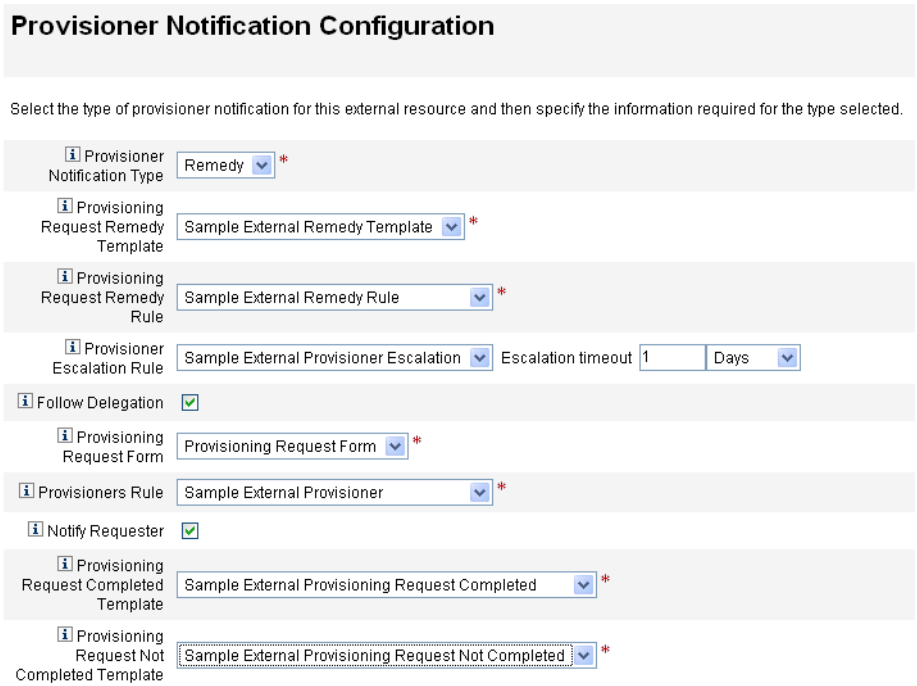


FIGURA 5–18 Página Configuración de notificación a abastecedores: Tipo de notificación de Remedy

2 **Configure las opciones siguientes:**

- **Plantilla de Remedy de solicitud de abastecimiento**. Elija Ejemplo de plantilla de Remedy externa en el menú.

Nota – Identity Manager incluye un ejemplo de plantilla de Remedy que puede utilizar o modificar según convenga.

Una plantilla de Remedy contiene un conjunto de campos que sirven para crear un ticket de Remedy. Identity Manager también utiliza esta plantilla para consultar el estado del ticket de Remedy con el fin de comprobar si se ha completado o no una tarea.

- **Regla de Remedy de solicitud de abastecimiento**. En este menú debe elegir una regla para definir los valores de configuración de Remedy.

Nota – Aunque este menú contiene varias reglas de ejemplo, debe seleccionar el *Ejemplo de regla de Remedy externa* o utilizar una regla propia. En el ejemplo de regla de Remedy externa se utiliza una regla de Remedy para saber si el estado actual de un ticket de Remedy es completado o no completado.

Una plantilla de Remedy contiene un conjunto de campos que sirven para crear un ticket de Remedy. Identity Manager también utiliza esta plantilla para consultar el estado del ticket de Remedy con el fin de comprobar si se ha completado o no una tarea.

Identity Manager aplica esta regla para consultar la información de estado de un ticket de Remedy. Si el estado del ticket es completado o no completado, Identity Manager marca el elemento de trabajo respectivamente como completado o no completado.

Nota – Puede elaborar sus propias reglas al respecto. Se incluye un ejemplo de regla de Remedy externa que puede utilizar directamente o modificarlo como interese. Para obtener más información sobre la creación de reglas, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.

- **Seguir delegación**. Marque esta casilla si quiere que Identity Manager siga las delegaciones definidas para el abastecedor.
- **Regla de escalada a abastecedor** (*opcional*). Elija una regla para establecer a qué abastecedor se traslada una solicitud en caso de que el abastecedor actual no responda antes del tiempo de espera indicado.

Nota – Aunque este menú contiene varias reglas de ejemplo, debe seleccionar la regla *Ejemplo de escalada a abastecedor externo* o utilizar una regla propia. La regla Ejemplo de escalada a abastecedor externo aplica una regla de escalada a abastecedor externo para establecer el abastecedor en caso de escalada.

- **Tiempo de espera de escalada**. Indique el máximo tiempo de espera antes de traslada una solicitud de abastecimiento al siguiente abastecedor.

Nota –

- Si deja este campo vacío o introduce un cero, la solicitud nunca se escala.
- Si especifica un tiempo de espera, pero no una Regla de escalada a abastecedor, Identity Manager escalará la solicitud al configurador cuando transcurra el tiempo de espera especificado. Si no hay configurador, la solicitud se clasificará como no completada una vez caducado el tiempo de espera.

- **Formulario de solicitud de abastecimiento**. Elija un formulario que los abastecedores de recursos externos puedan utilizar para marcar como completada o no completada una solicitud de abastecimiento.
- **Regla de abastecedores**. Seleccione una regla que establezca uno o más abastecedores para esta solicitud de recursos externa.

Nota – Puede elaborar sus propias reglas al respecto. También es posible definir varios abastecedores. Cuando alguno de ellos complete la tarea, ésta desaparecerá de las colas de todos los abastecedores. Para obtener más información sobre la creación de reglas, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.

  - **Ejemplo de abastecedor externo**. Convierte al configurador en abastecedor.
  - **Ejemplo de escalada a abastecedor externo**. Aplica una regla de ejemplo de escalada a abastecedor externo para establecer el abastecedor en caso de escalada.
  - **Ejemplo de regla de Remedy externa**. Define los valores de configuración de Remedy.
- **Notificar a solicitante**. Marque esta casilla si desea avisar por correo electrónico al solicitante cuando su solicitud se haya completado o no. Cuando se habilita esta opción, aparecen además estos campos:
  - **Plantilla de solicitud de abastecimiento completada**. Seleccione la plantilla de correo electrónico que se utilizará cuando se hayan completado las solicitudes.
  - **Plantilla de solicitud de abastecimiento no completada**. Seleccione la plantilla de correo electrónico que se utilizará cuando no se hayan completado las solicitudes.

Nota – Encontrará más información sobre las plantillas de correo electrónico en "Configuración de las plantillas de tarea" en la página 306.

---

3 **Pulse Guardar.**

Aparece la página Configurar, donde se le indica que puede continuar realizando otra tarea de configuración.

4 **Vaya a la ficha Recursos → Listar recursos. Ahora ya puede crear recursos externos individuales basándose en esta configuración. Consulte las instrucciones en "Creación de recursos externos" en la página 191.**

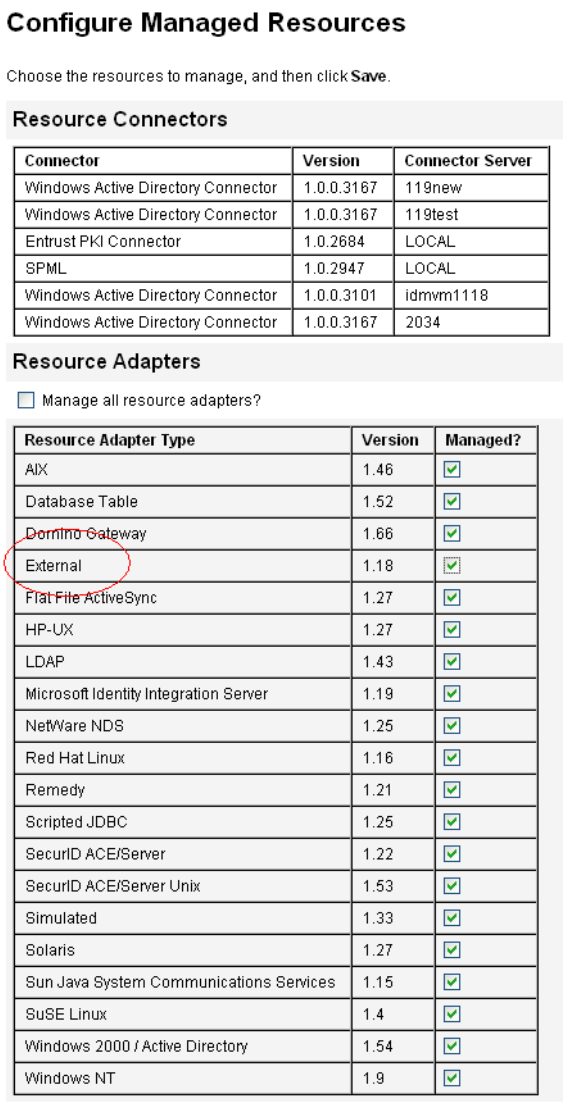
Creación de recursos externos

Tras configurar el almacén de datos de recursos externos y las notificaciones a los abastecedores, puede crear un recurso externo nuevo.

Nota – Para crear recursos externos nuevos se necesita la capacidad Administrador de recursos.

Siga estos pasos para crear un recurso externo nuevo:

1. Seleccione la ficha Recursos en la barra de menús principal. De manera predeterminada aparece la ficha Listar recursos.
2. Haga clic en la ficha Configurar tipos para abrir la página Configurar recursos administrados.



Configure Managed Resources

Choose the resources to manage, and then click **Save**.

Resource Connectors

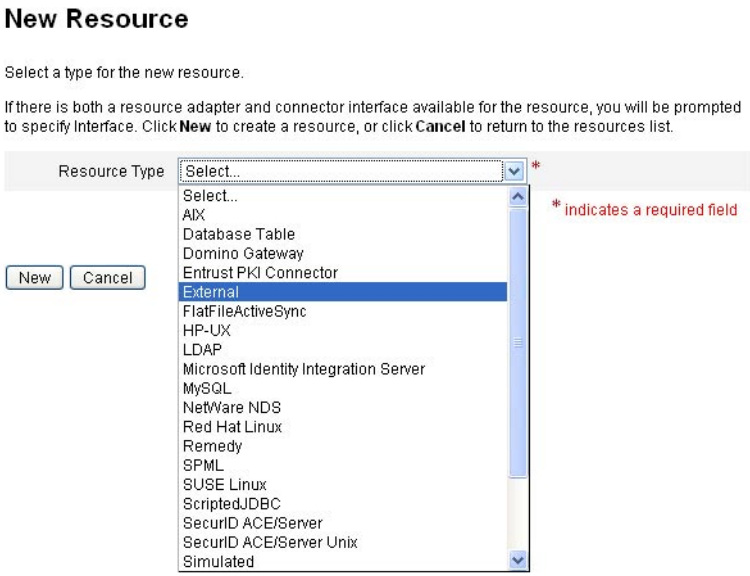
Connector	Version	Connector Server
Windows Active Directory Connector	1.0.0.3167	119new
Windows Active Directory Connector	1.0.0.3167	119test
Entrust PKI Connector	1.0.2684	LOCAL
SPML	1.0.2947	LOCAL
Windows Active Directory Connector	1.0.0.3101	idmvm1118
Windows Active Directory Connector	1.0.0.3167	2034

Resource Adapters

☐ Manage all resource adapters?

Resource Adapter Type	Version	Managed?
AIX	1.46	☑
Database Table	1.52	☑
Domino Gateway	1.66	☑
External	1.18	☑
Flat File ActiveSync	1.27	☑
HP-UX	1.27	☑
LDAP	1.43	☑
Microsoft Identity Integration Server	1.19	☑
NetWare NDS	1.25	☑
Red Hat Linux	1.16	☑
Remedy	1.21	☑
Scripted JDBC	1.25	☑
SecurID ACE/Server	1.22	☑
SecurID ACE/Server Unix	1.53	☑
Simulated	1.33	☑
Solaris	1.27	☑
Sun Java System Communications Services	1.15	☑
SuSE Linux	1.4	☑
Windows 2000 / Active Directory	1.54	☑
Windows NT	1.9	☑

3. Examine la tabla Adaptadores de recursos para comprobar si el tipo de recurso externo está disponible.
4. Regrese a la ficha Listar recursos y elija Nuevo recurso en el menú Acciones de tipo de recurso.
5. Cuando aparezca la página Nuevo recurso, elija Externo en el menú Tipo de recurso y pulse Nuevo.



6. Aparece la página de bienvenida del asistente para crear recursos externos. Pulse Siguiente.

   Aparece una vista de sólo lectura de la página Configuración de almacén de datos con la información de conexión y autenticación que había definido antes.

   Como ya mencionamos, este almacén de datos sólo se suele configurar una vez, ya que la configuración se aplica a todos los recursos externos. Si desea modificar esta información, debe retroceder a la ficha Configurar → Recursos externos.

Nota – Puede usar el botón Probar configuración situado al final de la página para volver a comprobar la configuración actual del almacén de datos antes de continuar.

---

7. Pulse Siguiente para abrir la página Configuración de notificación a abastecedores, que es idéntica a la utilizada en la ficha Configurar → Recursos externos.
8. Repase los valores actuales de notificación a abastecedores e introduzca las modificaciones pertinentes para el nuevo recurso.

Nota – Si es preciso, vuelva a consultar las instrucciones de configuración de "Configuración de notificaciones a abastecedores" en la página 185. Los cambios realizados en esta página sólo se aplicarán a este recurso.

---

9. Pulse Siguiente.

A partir de este momento, el proceso de creación de un recurso externo es igual que para crear cualquier otro recurso. El asistente le guiará por varias páginas más:

- **Atributos de cuenta**. En esta página se definen atributos de cuenta opcionales para el recurso y se asignan atributos del sistema Identity a los atributos de cuenta del nuevo recurso. Por ejemplo, si va a crear un recurso externo denominado "portátil", tal vez le interese incluir atributos de modelo y tamaño.

  Nota – En esta página no se especifican valores predeterminados.

- **Plantilla de identidad**. Esta página sirve para definir la sintaxis de nombre de cuenta de los usuarios creados en este recurso externo. Puede utilizar la plantilla de identidad predeterminada, `$accountId$`, o bien elegir otra.
- **Parámetros de Identity System (Sistema de identidad)**. En esta página se configuran los parámetros del sistema de identidad para los recursos externos. Por ejemplo, puede inhabilitar directivas, configurar reintentos o especificar aprobadores.

En el apartado "Para crear un recurso" en la página 162 encontrará más información sobre estas páginas y las instrucciones necesarias para terminar de configurar este recurso.

10. Cuando termine de configurar la página Parámetros de Identity System (Sistema de identidad), pulse Guardar. Ahora puede asignar este recurso a un usuario, igual que si se tratara de cualquier otro recurso.

Abastecimiento de recursos externos

A continuación se explica el proceso de abastecimiento en los apartados:

▼ Para asignar un recurso externo a un usuario

Siga estos pasos para asignar un recurso externo a un usuario:

Nota – Para asignar recursos externos se necesita la capacidad Administrador de recursos.

1 Seleccione Cuentas → Listar cuentas y haga clic sobre el nombre del usuario en la página.

2 Cuando aparezca la página Editar usuario, seleccione la ficha Recursos.

3 Busque el recurso externo en la lista Recursos disponibles de Asignación individual de recursos, trasládelo a la lista Recursos vigentes y pulse Guardar.

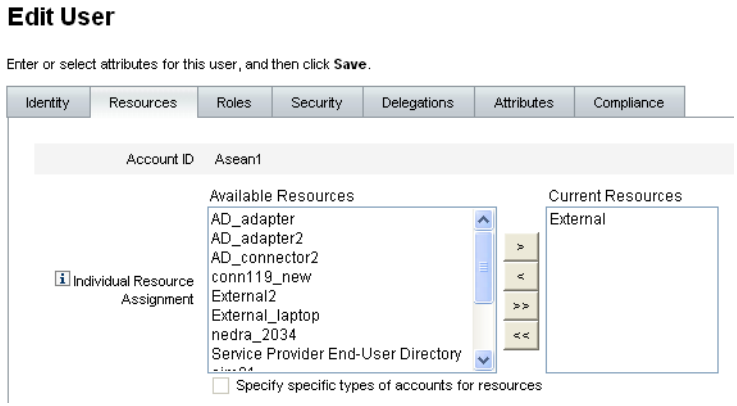


FIGURA 5–19 Página Editar usuario

Identity Manager crea una tarea de abastecimiento y le envía un mensaje donde le indica quién es el propietario de dicha tarea. Recuerde que se habían definido uno o varios abastecedores con la regla de abastecedores al configurar la página de notificación a abastecedores para este recurso.

Identity Manager también avisa a los abastecedores por correo electrónico o con un ticket de Remedy cuando tienen una solicitud pendiente.

Nota – Como en el caso de otros recursos, es posible definir aprobadores para que aprueben o rechacen solicitudes. Aunque debe definir abastecedores, éstos no aprueban ni rechazan solicitudes, sino que completan o no completan las tareas.

---

4 **Pulse Aceptar para regresar a la página Cuentas → Listar cuentas. Observe que junto al nombre del usuario aparece un reloj de arena en el icono de elemento de trabajo para indicar que la solicitud está pendiente.**

▼ Para responder a una solicitud de abastecimiento de recursos externos

Cuando se genera una solicitud de abastecimiento, ésta deja en suspenso el proceso de abastecimiento hasta que uno de los abastecedores definidos completa el abastecimiento manual o marca la solicitud como completada, o bien se agota el tiempo de espera de la solicitud. Identity Manager audita estas respuestas de abastecimiento.

Como sucede con cualquier otro elemento de trabajo, puede examinar todas las solicitudes de abastecimiento de recursos externos pendientes en la ficha Elementos de trabajo → Solicitudes de abastecimiento.

Debe responder así a las solicitudes de abastecimiento:

1 **Seleccione las fichas Elementos de trabajo > Solicitudes de abastecimiento para abrir la página Esperando abastecimiento.**

FIGURA 5–20 Página Esperando abastecimiento

2 **Busque la solicitud de abastecimiento pendiente y selecciónela.**

3 **También puede abrir la solicitud de abastecimiento por correo electrónico, seleccionar un vínculo que hay definido en la plantilla de solicitud de abastecimiento e iniciar la sesión para ver una página con detalles sobre la solicitud de abastecimiento.**

En esa página puede actualizar cualquiera de los atributos solicitados para reflejar con exactitud lo que se ha abastecido al usuario. Por ejemplo, si el usuario había solicitado un portátil Sony, pero ese modelo no estaba disponible, puede actualizar la página con el modelo que en realidad ha abastecido.

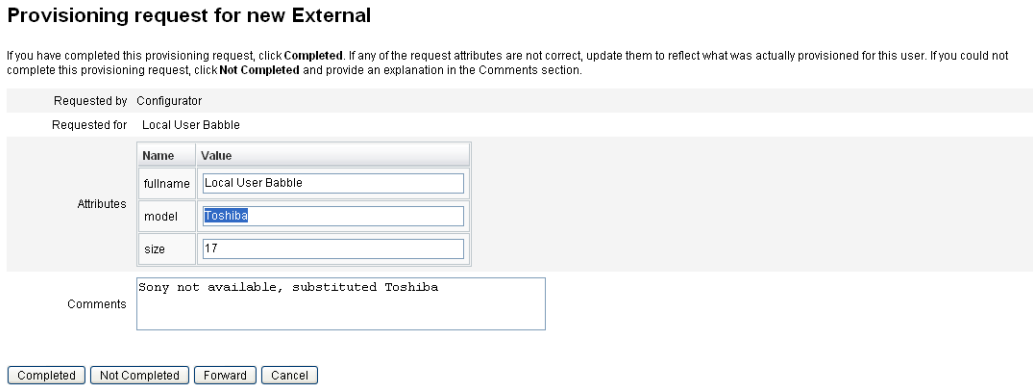


FIGURA 5–21 Solicitud de abastecimiento de un portátil nuevo

4 Pulse uno de los botones siguientes para procesar la solicitud:

- Si puede abastecer el recurso, elija Completada.

  Identity Manager actualiza los atributos de cuenta del recurso externo del usuario para reflejar lo que se ha abastecido realmente, suprime la marca de estado de abastecimiento pendiente y completa el elemento de trabajo de solicitud de abastecimiento que se está actualizando.

  Si así se configura, Identity Manager también notifica al abastecedor que la solicitud de abastecimiento se ha completado utilizando para ello la plantilla de correo electrónico definida al respecto.

- Si no es posible abastecer el recurso, indique el motivo y seleccione No completada.

  Cuando una solicitud se marca como No completada:

  - El usuario no se abastece con el recurso externo.
  - El recurso externo permanece asignado al usuario.
  - Junto al nombre del usuario aparece un icono amarillo para indicar que es preciso actualizar el usuario.

    Si se edita este usuario, aparece un mensaje de error para advertir que el usuario puede encontrarse en el recurso externo.

  - Si así se configura, Identity Manager también notifica al solicitante mediante la plantilla de correo electrónico definida al respecto.

- Si no es posible abastecer el recurso, también puede pulsar Reenviar para trasladar la solicitud a otra persona.

Cuando el elemento de trabajo de solicitud de abastecimiento se ha completado o no, Identity Manager desactiva el estado pendiente del recurso externo asignado al usuario y no se produce ninguna actualización en el almacén de datos de recursos externos.

El recurso aparece en la lista de recursos asignados al usuario y en la de cuentas de recursos vigentes, incluyendo el ID de cuenta del usuario en ese recurso.

Nota – Si el abastecedor asignado no responde a una solicitud de abastecimiento antes de que transcurra el tiempo de espera especificado, Identity Manager cancela el elemento de trabajo de solicitud de abastecimiento asociado.

Más información

Escalada de solicitudes de abastecimiento

- Si especificó un tiempo de espera al configurar la página de notificaciones a abastecedores y una solicitud de abastecimiento supera dicho periodo, Identity Manager realiza una de las siguientes acciones:
  - Si había especificado una regla de escalada a abastecedor, Identity Manager la aplica para establecer el próximo abastecedor y le traslada la solicitud.
  - Si no había seleccionado una regla de escalada a abastecedor, Identity Manager escalará la solicitud al configurador. Si no hay configurador, la solicitud se clasificará como no completada una vez caducado el tiempo de espera.
- Si dejó vació el campo de tiempo de espera de escalada o introdujo cero, Identity Manager nunca escala la solicitud.

Delegación de solicitudes de abastecimiento

Los elementos de trabajo de solicitud de abastecimiento de recursos externos se pueden delegar igual que cualquier otra solicitud de abastecimiento. Encontrará más información e instrucciones en "Delegación de elementos de trabajo" en la página 234.

Anulación de asignación y desvinculación de recursos externos

Como cualquier otro recurso, la asignación de recursos externos a un usuario se puede anular o desvincular en la ficha General. Consulte las instrucciones en "Creación de usuarios y trabajo con cuentas de usuario" en la página 58

Nota – Al anular la asignación y desvincular recursos externos de un usuario no se crea una solicitud de abastecimiento ni un elemento de trabajo. Cuando se anula la asignación o se desvincula un recurso externo, Identity Manager no desabastece ni elimina la cuenta de recursos, por lo que no es necesario que haga nada.

Solución de problemas de recursos externos

No es posible eliminar los usuarios que aún tienen asignados recursos externos. Primero debe desabastecer o eliminar esos recursos externos para poder eliminar los usuarios.

Identity Manager le ofrece diversos métodos para depurar y rastrear los recursos externos:

- Puede efectuar un seguimiento del adaptador de recursos externos.
  - Si utiliza un almacén de datos de tipo base de datos, rastree los nombres de clase `com.waveset.adapter.ScriptedJdbcResourceAdapter` y `com.waveset.adapter.JdbcResourceAdapter` .
  - Si utiliza un almacén de datos de directorio, rastree el nombre de clase `com.waveset.adapter.LDAPResourceAdapter`.
- Puede utilizar seguimiento de flujo de trabajo para rastrear otros flujos de datos y de trabajo, así como utilizar el complemento NetBeans o Eclipse Identity Manager IDE para depurar.
- Dado que usted configura y controla el almacén de datos, puede inspeccionarlo para asegurarse de que contenga la información correcta.
- Identity Manager graba registros de auditoría de todas las actividades que ocurren.

Para obtener más información sobre seguimiento y solución de problemas, consulte *Sun Identity Manager 8.1 System Administrator's Guide* .

◆ ◆ ◆ CAPÍTULO 6

Administración

En este capítulo se incluye información y procedimientos para realizar gran variedad de tareas administrativas en el sistema Identity Manager, como crear y gestionar administradores y organizaciones de Identity Manager. También se explica cómo utilizar los roles, las capacidades y los roles administrativos en Identity Manager.

Esta información se ha dividido en los temas siguientes:

Conceptos de administración de Identity Manager

Los administradores de Identity Manager son usuarios con privilegios extendidos de Identity Manager.

Los administradores de Identity Manager gestionan:

- Cuentas de usuario
- Objetos del sistema, como roles y recursos
- Organizaciones

A diferencia de los usuarios, los administradores de Identity Manager tienen asignadas capacidades y organizaciones controladas, que se definen así:

- **Capacidades**. Un conjunto de permisos que conceden derechos de acceso a usuarios, organizaciones, roles y recursos de Identity Manager.
- **Organizaciones controladas**. Una vez que tiene asignado el control de una organización, el administrador puede gestionar los objetos de dicha organización y de todas las organizaciones jerárquicamente descendentes de ella.

Administración delegada

En la mayoría de las empresas, los empleados que realizan tareas administrativas asumen responsabilidades específicas. En consecuencia, las tareas de administración de cuentas que pueden desempeñar estos administradores tienen un ámbito limitado.

Por ejemplo, un administrador puede encargarse únicamente de crear cuentas de usuario de Identity Manager. Con este ámbito de responsabilidad limitado, es improbable que el administrador necesite información específica sobre los recursos donde se crean las cuentas de usuario o sobre los roles u organizaciones que existen dentro del sistema.

Identity Manager también puede restringir los administradores a determinadas tareas dentro de un ámbito específico definido.

Identity Manager permite separar las responsabilidades y utilizar un modelo de administración delegada así:

- Las **capacidades** asignadas limitan a los administradores a tareas de trabajo específicas.
- Las **organizaciones controladas** asignadas restringen a los administradores a controlar sólo determinadas organizaciones (y los objetos que hay en ellas).
- Las vistas filtradas de las páginas Crear usuario y Editar usuario impiden que los administradores vean la información no relevante para sus tareas de trabajo.

Es posible especificar las delegaciones de un usuario en la página Crear usuario al configurar una cuenta de usuario nueva o al editar una existente.

En la ficha Elementos de trabajo también se pueden delegar elementos de trabajo, como solicitudes de aprobación. Para obtener más información sobre las delegaciones, consulte "Delegación de elementos de trabajo" en la página 234.

Creación y gestión de administradores

Esta sección consta de los temas siguientes:

▼ Creación de un administrador

Para crear un administrador, asigne una o más capacidades a un usuario y designe las organizaciones a las que se deben aplicar las capacidades.

1 **En la interfaz de administración, seleccione Cuentas en la barra de menús.**

Aparece la página Lista de usuarios.

2 **Para conceder privilegios administrativos a un usuario existente, haga clic en el nombre de usuario (se abrirá la página Editar usuario) y después en la ficha Seguridad.**

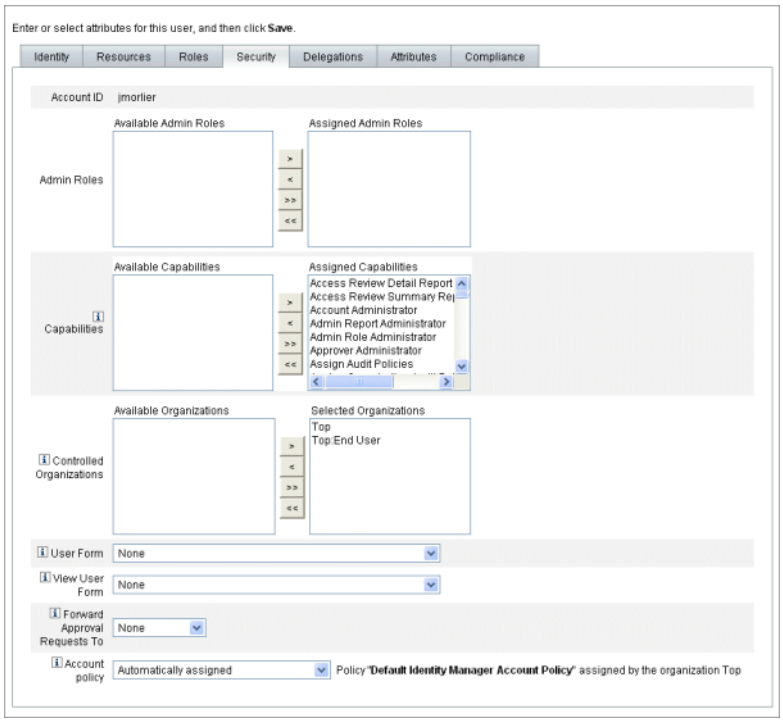
Si hace falta crear una cuenta de usuario nueva, consulte "Creación de usuarios y trabajo con cuentas de usuario" en la página 58.

3 **Especifique atributos para establecer el control administrativo.**

Los atributos disponibles incluyen:

- **Capacidades**. Seleccione una o más capacidades que deben asignarse a este administrador. Esta información es necesaria. Para obtener más información, consulte "Conceptos y administración de capacidades" en la página 216.
- **Organizaciones controladas**. Seleccione una o más organizaciones que deben asignarse a este administrador. El administrador controla los objetos en la organización asignada y en todas aquéllas que se encuentren por debajo de ella en la jerarquía. Esta información es necesaria. Para obtener más información, consulte "Qué son las organizaciones en Identity Manager" en la página 209.
- **Formulario de usuario**. Seleccione el formulario de usuario que debe utilizar este administrador al crear y editar usuarios de Identity Manager (si tiene asignada esta capacidad). Si no asigna directamente un formulario de usuario, el administrador heredará el formulario de usuario asignado a la organización a la que pertenece. El formulario que se seleccione aquí sustituirá cualquier formulario seleccionado dentro de la organización del administrador.

- **Reenviar las solicitudes de aprobación a**. Seleccione un usuario para reenviarle todas las solicitudes de aprobación que hay pendientes. Esta configuración de administrador puede ser también establecida desde la página de aprobaciones.
- **Delegar elementos de trabajo a**. Si esta opción se encuentra disponible, úsela para especificar las delegaciones de esta cuenta de usuario. Puede especificar el gestor del administrador, uno o varios usuarios seleccionados, o utilizar una regla de aprobadores delegados.



Filtración de vistas de administrador

Al asignar formularios de usuario a organizaciones y administradores, establece vistas de administrador específicas de las información de usuario.

El acceso a la información de usuario se configura en dos niveles:

- **Organización**. Cuando se crea una organización, se asigna el formulario de usuario que todos los administradores de la misma utilizarán al crear y editar usuarios de Identity Manager. Cualquier formulario configurado en el nivel de administrador sustituye al formulario configurado aquí. Si no se selecciona ningún formulario para el administrador o la organización, Identity Manager hereda el formulario seleccionado para la organización principal. Si no se configura aquí ningún formulario, Identity Manager utiliza el formulario predeterminado definido en la configuración del sistema.
- **Administrador**. Cuando se asignan capacidades administrativas a un usuario, se puede asignar directamente un formulario de usuario al administrador. Si no se asigna ningún formulario, el administrador hereda el formulario asignado a esta organización (o el formulario predeterminado definido en la configuración del sistema en caso de que no haya ningún formulario asignado a la organización).

"Conceptos y administración de capacidades" en la página 216 describe las capacidades integradas de Identity Manager que se pueden asignar.

Cambio de contraseñas de administrador

Las contraseñas de administrador pueden ser cambiadas por un administrador que tenga asignadas capacidades para cambiar las contraseñas administrativas o por el propietario-administrador.

Los administradores pueden cambiar las contraseñas de otros administradores mediante los formularios siguientes:

- **Formulario Modificar contraseña de usuario** Este formulario puede abrirse de dos formas:
  - Al hacer clic en Cuentas dentro del menú. Aparece la Lista de usuarios. Seleccione un administrador y después elija Cambiar contraseña en la lista Acciones de Usuario. Aparece la página Modificar contraseña de usuario.
  - Al hacer clic en Contraseñas dentro del menú. Aparece la página Modificar contraseña de usuario.
- **Formulario de usuario con fichas**. Al hacer clic en Cuentas dentro del menú. Aparece la Lista de usuarios. Seleccione un administrador y después elija Editar en el menú Acciones de Usuario. Aparece la página "Editar usuario" (formulario de usuario con fichas). En la ficha Identidad del formulario, escriba una contraseña nueva dentro de los campos Contraseña y Confirmar contraseña.

Un administrador puede cambiar su propia contraseña en el área Contraseñas. Haga clic en Contraseñas dentro del menú y después elija Cambiar mi contraseña.

Nota – La directiva de cuentas de Identity Manager que se aplica a la cuenta determina las limitaciones de las contraseñas, como su caducidad, las opciones de reinicialización y las selecciones de notificación. Es posible definir otras limitaciones para las contraseñas mediante las directivas de contraseñas configuradas en los recursos del administrador.

Acciones de desafío del administrador

Es posible configurar Identity Manager para que solicite una contraseña a los administradores antes de procesar ciertas modificaciones de las cuentas. Si falla la autenticación, se cancelarán las modificaciones de la cuenta.

Los administradores pueden cambiar las contraseñas de los usuarios con tres formularios: el formulario de usuario con fichas, el de cambio de contraseña de usuario y el de reinicialización de contraseña de usuario. No olvide actualizar los tres formularios para asegurarse de que se solicite a los administradores la introducción de sus contraseñas antes de que Identity Manager procese las modificaciones de las cuentas de usuario.

▼ Habilitación de la opción de desafío para los formularios de usuario con fichas

Para exigir un desafío de contraseña en el formulario de usuario con fichas, siga estos pasos.

1. **En la interfaz de administración, abra la página de depuración de Identity Manager ("Página de depuración de Identity Manager" en la página 45) introduciendo la URL siguiente en el navegador. (Para abrir esta página debe tener capacidad de depuración.)**

   `http://<`*AppServerHost*`>:<` *Port*`>/idm/debug/session.jsp`

   Aparece la página de configuración del sistema (página de depuración de Identity Manager).

2. **Busque el botón List Objects, elija UserForm en el menú desplegable y haga clic en el botón ListObjects.**

   Aparece la página List Objects of type: UserForm.

3. **Busque la copia del formulario de usuario con fichas que tenga en producción y haga clic en Edit. (El formulario de usuario con fichas distribuido con Identity Manager es una plantilla que no debe modificarse.)**

4. **Agregue el fragmento de código siguiente dentro del elemento `<Form>`:**

```
<Properties>
  <Property name='RequiresChallenge'>
    <List>
      <String>password</String>
```

```
      <String>email</String>
      <String>fullname</String>
    </List>
  </Property>
</Properties>
```

El valor de property es una lista que puede contener uno o más de los siguientes nombres de atributo de vista de usuario:

- `applications`
- `adminRoles`
- `assignedLhPolicy`
- `capabilities`
- `controlledOrganizations`
- `email`
- `firstname`
- `fullname`
- `lastname`
- `organization`
- `password`
- `resources`
- `roles`

5 Guarde las modificaciones.

▼ Habilitación de la opción de desafío para los formularios de cambio de contraseña de usuario y de reinicialización de contraseña de usuario

Para exigir un desafío de contraseña en los formularios de cambio de contraseña de usuario y de reinicialización de contraseña de usuario, siga estos pasos:

1 En la interfaz de administración, abra la página de depuración de Identity Manager ("Página de depuración de Identity Manager" en la página 45) introduciendo la URL siguiente en el navegador. (Para abrir esta página debe tener capacidad de depuración.)

`http://<`*AppServerHost*`>:<` *Port*`>/idm/debug/session.jsp`

Aparece la página de configuración del sistema (página de depuración de Identity Manager).

2 Busque el botón List Objects, elija UserForm en el menú desplegable y haga clic en el botón ListObjects.

Aparece la página List Objects of type: UserForm.

3 Busque la copia del formulario de cambio de contraseña de usuario que tenga en producción y haga clic en Edit. (El formulario de cambio de contraseña de usuario distribuido con Identity Manager es una plantilla que no debe modificarse.)

4 **Busque el elemento** `<Form>` **y después vaya al elemento** `<Properties>`**.**

5 **Agregue la línea siguiente dentro del elemento** `<Properties>` **y guarde las modificaciones.**

```
<Property name='RequiresChallenge' value='true'/>
```

6 **Repita los pasos 3 - 5, pero editando la copia del fromulario de reinicialización de contraseña de usuario que tenga en producción.**

Cambio de respuestas a preguntas de autenticación

Si desea cambiar las respuestas que hay definidas para las preguntas de autenticación de cuentas, use el área Contraseñas. En la barra de menús, seleccione Contraseñas y después Modificar mis respuestas.

Para obtener más información sobre autenticación, consulte la sección "Autenticación de usuarios" en la página 91 en el Capítulo 3, "Administración de usuarios y de cuentas".

Personalización de la visualización del nombre del administrador en la interfaz de administración

En algunas páginas y áreas de la interfaz de administración de Identity Manager se puede visualizar el administrador de Identity Manager por atributo (por ejemplo, `email` o `fullname`) en lugar de por el ID de cuenta.

Por ejemplo, es posible ver los administradores de Identity Manager por atributo en estas áreas:

- Editar usuario (lista de selección de envío de aprobaciones)
- Tabla de roles
- Crear/Editar rol
- Crear/Editar recurso
- Crear/Editar unión de directorios
- Aprobaciones

Si desea configurar Identity Manager para que use un nombre de visualización, agregue lo siguiente al objeto `UserUIConfig` :

```
<AdminDisplayAttribute>
  <String>attribute_name</String>
</AdminDisplayAttribute>
```

Por ejemplo, para usar el atributo email como nombre de visualización, agregue el siguiente nombre de atributo a `UserUIconfig`:

```
<AdminDisplayAttribute>
  <String>email</String>
</AdminDisplayAttribute>
```

Qué son las organizaciones en Identity Manager

Las organizaciones le permiten:

- Gestionar administradores y cuentas de usuario de una manera lógica y segura.
- Limitar el acceso a los recursos, aplicaciones, roles y otros objetos de Identity Manager.

Al crear organizaciones y asignar usuarios a diversas ubicaciones en una jerarquía organizativa, se configura la fase de administración delegada. Las organizaciones que a su vez contienen a otras organizaciones se denominan *organizaciones principales*.

Todos los usuarios de Identity Manager (incluidos los administradores) se *asignan estáticamente* a una organización. Los usuarios también se pueden *asignar dinámicamente* a otras organizaciones.

Los administradores de Identity Manager se asignan además para *controlar* organizaciones.

Creación de organizaciones

▼ Para crear una organización

Las organizaciones se crean en el área Cuentas de Identity Manager.

1 **En la interfaz de administración, seleccione Cuentas en la barra de menús.**

Aparece la página Lista de usuarios.

2 **En el menú Nuevas acciones, seleccione Nueva organización.**

Consejo – Para crear una organización en una ubicación específica de la jerarquía organizativa, seleccione una organización en la lista y después elija Nueva organización en el menú Nuevas acciones.

La Figura 6–1 ilustra la página Crear organización.

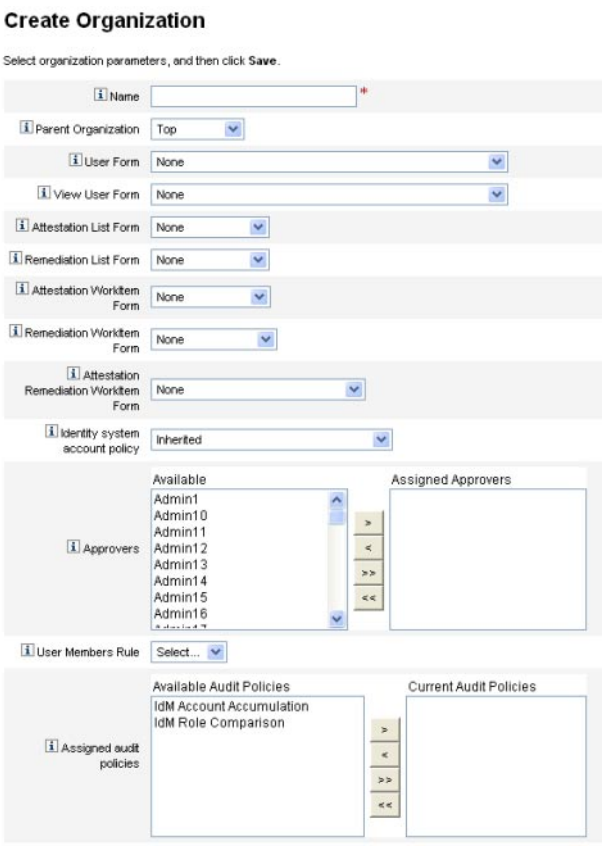


FIGURA 6–1 Página Crear organización

Asignación de usuarios a organizaciones

Cada usuario es un afiliado estático de una sola organización, pero puede ser un afiliado dinámico de varias.

Las afiliaciones organizativas se definen con uno de estos métodos:

- **Asignación directa (estática)**. Seleccione la ficha Identidad en la página Crear usuario o Editar usuario para asignar usuarios directamente a una organización. Un usuario se debe asignar directamente a una organización.
- **Asignación basada en reglas (dinámica)**. Utilice una regla de usuarios afiliados que esté asignada a una organización para asignar usuarios a dicha organización. Cuando se evalúa la regla, devuelve un conjunto de usuarios afiliados.

Identity Manager evalúa la regla de usuarios afiliados cuando:

- Se listan los usuarios de una organización.
- Se buscan usuarios (a través de la página Buscar usuarios), incluidos los afiliados a una organización con una regla de usuarios afiliados.
- Se solicita acceso a un usuario, siempre que el administrador actual controle una organización con una regla de usuarios afiliados.

Nota – Para obtener más información sobre la creación y el uso de reglas en Identity Manager, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.

Seleccione una regla de usuarios afiliados en el menú Regla de usuarios afiliados de la página Crear organización. La figura siguiente muestra un ejemplo de regla de usuarios afiliados.

A continuación se incluye un ejemplo de sintaxis de regla de usuarios afiliados que se utiliza para controlar dinámicamente la afiliación de usuarios a una organización.

Nota –

Antes de crear una regla de usuarios afiliados, debe recordar lo siguiente:

- Para que una regla aparezca en la casilla Regla de usuarios afiliados, su `authType` debe configurarse en `authType='UserMembersRule'` .
- El contexto es la sesión de usuario de Identity Manager actualmente autenticada.
- La variable definida `(defvar) Team players` obtiene el nombre distinguido (dn) para cada usuario afiliado a la unidad organizativa (ou) `Pro Ball Team` de Windows Active Directory.
- Para cada usuario encontrado, la lógica de append concatenará el dn de cada usuario afiliado a la ou `Pro Ball Team` con el nombre del recurso de Identity Manager precedido de dos puntos (como `:smith-AD`).

- Como resultados se devolverá una lista de nombres distinguidos concatenados con el nombre del recurso de Identity Manager en el formato *dn* `:smith-AD`.

EJEMPLO 6–1 Ejemplo de regla de usuarios afiliados

```
<Rule name='Get Team Players' authType='UserMembersRule'>
  <defvar name='Team players'>
    <block>
      <defvar name='player names'>
        <list/>
      </defvar>
  <dolist name='users'>
    <invoke class='com.waveset.ui.FormUtil' name='getResourceObjects'>
      <ref>context</ref>
      <s>User</s>
      <s>singleton-AD</s>
      <map>
        <s>searchContext</s>
        <s>OU=Pro Ball Team,DC=dev-ad,DC=waveset,DC=com</s>
        <s>searchScope</s>
        <s>subtree</s>
        <s>searchAttrsToGet</s>
        <list>
          <s>distinguishedName</s>
        </list>
      </map>
    </invoke>
    <append name='player names'>
    <concat>
      <get>
        <ref>users</ref>
        <s>distinguishedName</s>
      </get>
        <s>:sampson-AD</s>
    </concat>
    </append>
  </dolist>
    <ref>player names</ref>
  </block>
   </defvar>
    <ref>Team players</ref>
</Rule>
```

Nota – Puede configurar diversas propiedades en `Waveset.` para controlar la memoria caché de la lista Usuarios afiliados basada en reglas. Encontrará información en "Tracing Rule-Driven Members Caches" de *Sun Identity Manager 8.1 System Administrator's Guide*.

Asignación de control de organizaciones

En las páginas Crear usuario y Editar usuario se asigna el control administrativo de una o varias organizaciones. Seleccione la ficha de formulario Seguridad para ver el campo Organizaciones controladas.

También es posible asignar el control administrativo de las organizaciones asignando uno o más roles de administrador mediante el campo Roles de administrador (Admin).

Uniones de directorios y organizaciones virtuales

Una *unión de directorios* es un conjunto de organizaciones relacionadas jerárquicamente que refleja el conjunto real de contenedores jerárquicos de recursos de directorio. Un *recurso de directorio* es aquél que utiliza un espacio de nombre jerárquico mediante contenedores jerárquicos. Entre los ejemplos de recursos de directorio tenemos los servidores LDAP y los recursos de Windows Active Directory.

Cada organización de una unión de directorios constituye una *organización virtual*. La organización virtual que ocupa la cima de una unión de directorios refleja el contenedor que representa el contexto base definido en el recurso. Las demás organizaciones virtuales de una unión de directorios son organizaciones secundarias *directas* o *indirectas* de la organización virtual principal y también reflejan uno de los contenedores de recurso de directorio que son secundarios respecto al contenedor del contexto base del recurso definido. Esta estructura se ilustra en la Figura 6–2.

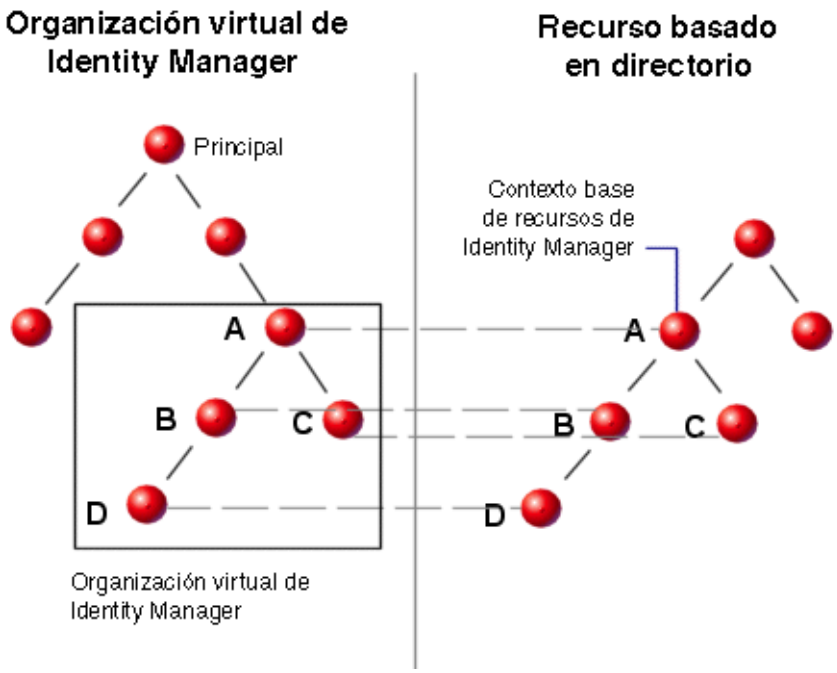


FIGURA 6–2 Organización virtual de Identity Manager

La uniones de directorios se pueden acoplar a cualquier punto de la estructura organizativa existente de Identity Manager. Sin embargo, no es posible acoplar uniones de directorios dentro o debajo de una unión de directorios existente.

Una vez incorporada una unión de directorios al árbol organizativo de Identity Manager, puede crear o eliminar organizaciones virtuales en el contexto de la unión de directorios. Asimismo, en cualquier momento puede actualizar el conjunto de organizaciones virtuales que forman una unión de directorios para asegurarse de que permanezcan sincronizadas con los contenedores de recursos de directorio. No es posible crear una organización no virtual dentro de una unión de directorios.

Puede afiliar objetos de Identity Manager (como usuarios, recursos y roles) a una organización virtual y ponerlos a su disposición igual que si fuera una organización física de Identity Manager.

Configuración de uniones de directorios

A continuación se explica cómo configurar las uniones de directorios.

▼ Para configurar una unión de directorios

1. **En la interfaz de administración, seleccione Cuentas en la barra de menús.**

   Aparece la página Lista de usuarios.

2. **Seleccione una organización de Identity Manager en la lista Cuentas.**

   La organización que seleccione constituirá la organización principal de la organización virtual que configure.

3. **En el menú Nuevas acciones, seleccione Nueva Unión de directorios.**

   Identity Manager abre la página Crear unión de directorios.

4. **Utilice las opciones de la página Crear unión de directorios para configurar la organización virtual.**

   Las opciones incluyen:

   - **Organización principal**. Este campo contiene la organización que ha seleccionado en la lista Cuentas, pero puede elegir otra organización principal en la lista.
   - **Recurso de directorio**. Seleccione el recurso de directorio que gestiona el directorio existente cuya estructura desea reflejar en la organización virtual.
   - **Formulario de usuario**. Seleccione un formulario de usuario para que se aplique a los administradores de esta organización.
   - **Directiva de cuentas de Identity Manager**. Seleccione una directiva o bien la opción predeterminada (heredada) para adoptar la directiva de la organización principal.
   - **Aprobadores**. Seleccione los administradores que pueden aprobar solicitudes relacionadas con esta organización.

Actualización de organizaciones virtuales

Mediante este proceso se actualiza y resincroniza la organización virtual con el recurso de directorio asociado, a partir de la organización seleccionada en sentido descendente. Elija la organización virtual en la lista y seleccione Actualizar organización en la lista Acciones de organización.

Eliminación de organizaciones virtuales

Hay dos opciones al eliminar organizaciones virtuales:

- **Eliminar sólo la organización de Identity Manager**. Elimina únicamente la unión de directorios de Identity Manager.
- **Eliminar la organización de Identity Manager y el contenedor de recursos**. Eliminar la unión de directorios de Identity Manager y la organización correspondiente en el recurso nativo.

Seleccione una opción y haga clic en Eliminar.

Conceptos y administración de capacidades

Las capacidades son grupos de derechos en el sistema Identity Manager. Representan responsabilidades de tareas administrativas, como reinicialización de contraseñas o administración de cuentas de usuario. A cada usuario administrativo de Identity Manager se le asignan una o más capacidades, que le proporcionan una serie de privilegios sin riesgo para la seguridad de los datos.

No es preciso asignar capacidades a todos los usuarios de Identity Manager. Sólo las necesitan los usuarios que vayan a desempeñar una o varias acciones administrativas con Identity Manager. Por ejemplo, no hace falta tener una capacidad asignada para permitir que un usuario cambie su contraseña, pero sí para cambiar la contraseña de otro usuario.

Las capacidades asignadas determinan las áreas de la interfaz de administración de Identity Manager a las que se tiene acceso.

Todos los usuarios administrativos de Identity Manager pueden acceder a ciertas áreas de Identity Manager, que incluyen:

- Fichas **Página de inicio** y **Ayuda**
- Ficha **Contraseñas** (sólo fichas secundarias Cambiar mi contraseña y Modificar mis respuestas)
- **Informes** (limitados a los tipos correspondientes a las responsabilidades concretas del administrador)

Nota – Encontrará una lista de las capacidades funcionales (con definiciones) y basadas en tareas predeterminadas de Identity Manager en el Apéndice D, “Definiciones de capacidades”. En este apéndice también se indican las fichas y fichas secundarias accesibles con cada capacidad basada en tareas.

Categorías de capacidades

Las capacidades de Identity Manager se definen así:

- **Basadas en tareas**. Son las capacidades en el nivel de tareas más simple.
- **Funcionales**. Las capacidades funcionales contienen a su vez otra u otras capacidades funcionales o basadas en tareas.

Las capacidades internas (las que se incluyen con el sistema Identity Manager) están *protegidas*, lo que significa que no son editables. Sin embargo, sí las puede utilizar con las capacidades que usted cree.

Las capacidades protegidas (internas) se señalan en la lista con el icono de una llave roja (o una llave roja y una carpeta). Las capacidades que usted crea y edita se señalan en la lista de capacidades con el icono de una llave verde (o una llave verde y una carpeta).

Operaciones con capacidades

En esta sección se explica cómo crear, editar, asignar y cambiar de nombre las capacidades. Estas operaciones se realizan en la página Capacidades.

Acceso a la página Capacidades

La página Capacidades se encuentra en la ficha Seguridad.

▼ Para abrir la página Capacidades

1. **En la interfaz de administración, seleccione Seguridad en el menú principal.**
2. **Elija Capacidades en el menú secundario.**

   Se abre la página Capacidades con una lista de las capacidades de Identity Manager.

Creación de capacidades

Siga el procedimiento indicado a continuación para crear una capacidad. Para *clonar* una capacidad, consulte "Guardar y cambiar de nombre una capacidad" en la página 219.

▼ Para crear una capacidad

1. **En la interfaz de administración, seleccione Seguridad en el menú principal.**
2. **Elija Capacidades en el menú secundario.**

   Se abre la página Capacidades con una lista de las capacidades de Identity Manager.

3 **Pulse Nuevo.**

Aparece la página Crear Capacidad.

4 **Rellene el formulario así:**

a. **Introduzca un nombre para la nueva capacidad.**

b. **Use los botones de flecha en el área Capacidades para trasladar al cuadro Capacidades asignadas las capacidades que desea asignar a los usuarios.**

c. **En el cuadro Asignadores, seleccione uno o varios usuarios que estarán autorizados para asignar esta capacidad a los demás usuarios.**

- Si no se selecciona ningún usuario, el único usuario que podrá asignar esta capacidad será el que creó la capacidad.
- Si el usuario que creó la capacidad no tiene asignada la capacidad Asignar capacidad de usuario, deberá seleccionar uno o varios usuarios para garantizar que al menos un usuario pueda asignar la capacidad a otro usuario.

d. **En el cuadro Organizaciones, seleccione al menos una organización para la que estará disponible esta capacidad.**

e. **Pulse Guardar.**

Nota – El conjunto de usuarios seleccionables incluye los que tienen asignado el derecho de asignar capacidades.

Edición de capacidades

Puede editar las capacidades no protegidas.

▼ Para editar una capacidad no protegidas

1 **En la interfaz de administración, seleccione Seguridad en el menú principal.**

2 **Elija Capacidades en el menú secundario.**

Se abre la página Capacidades con una lista de las capacidades de Identity Manager.

3 **Haga clic con el botón secundario sobre la capacidad en la lista y seleccione Editar. Aparece la página Editar Capacidad.**

4 **Introduzca las modificaciones y pulse Guardar.**

Las capacidades internas no se pueden editar, pero sí puede guardarlas con otros nombres para crear sus propias capacidades. También puede utilizar las capacidades internas en las capacidades que usted cree.

Guardar y cambiar de nombre una capacidad

Para crear un capacidad nueva, puede guardar con otro nombre una capacidad que ya exista. Este proceso se denomina *clonar* la capacidad.

▼ Para clonar una capacidad

1 **En la interfaz de administración, seleccione Seguridad en el menú principal.**

2 **Elija Capacidades en el menú secundario.**

Se abre la página Capacidades con una lista de las capacidades de Identity Manager.

3 **Haga clic con el botón secundario sobre la capacidad en la lista y seleccione Guardar como.**

Aparece un cuadro de diálogo donde debe escribir un nombre para la nueva capacidad.

4 **Escriba el nombre y pulse Aceptar.**

Ahora puede editar la nueva capacidad.

Asignación de capacidades a usuarios

Para asignar capacidades a los usuarios, utilice las páginas Crear usuario("Creación de usuarios y trabajo con cuentas de usuario" en la página 58) o Editar usuario ("Edición de usuarios" en la página 63). También se pueden asignar capacidades a los usuarios asignando roles de administrador, que se configuran en el área Seguridad de la interfaz. Encontrará más información en "Conceptos y administración de roles de admin" en la página 220.

Nota – Encontrará una lista de las capacidades funcionales (con definiciones) y basadas en tareas predeterminadas de Identity Manager en el Apéndice D, "Definiciones de capacidades". En este apéndice también se indican las fichas y fichas secundarias accesibles con cada capacidad basada en tareas.

Conceptos y administración de roles de admin

Los *roles de administrador* definen dos aspectos: un conjunto de capacidades y un ámbito de control. (El término "ámbito de control" se refiere a una o más organizaciones administradas.) Una vez definidos, los roles de administrador pueden asignarse a uno o varios administradores.

Nota – No hay que confundir los *roles* y los *roles de administrador*. Los roles sirven para administrar el acceso de los usuarios finales a los recursos externos, mientras que los roles de administrador se utilizan sobre todo para gestionar el acceso del administrador a los objetos de Identity Manager.

En esta sección nos limitamos a los roles de administración. Para obtener información sobre los roles, consulte "Conceptos y administración de roles" en la página 121.

Es posible asignar varios roles de administrador a un único administrador. Ello permite que un administrador tenga un conjunto de capacidades en un ámbito de control y otro distinto en otro ámbito de control. Por ejemplo, un rol de administrador puede conceder al administrador el derecho a crear y editar usuarios para las organizaciones controladas especificadas en ese rol de administrador. Sin embargo, un segundo rol de administrador asignado al mismo administrador podría garantizar únicamente el derecho a cambiar las contraseñas de los usuarios en un conjunto distinto de organizaciones controladas definidas en el rol de administrador.

Los roles de administrador permiten reutilizar las parejas de capacidades y ámbito de control. También simplifican la gestión de los privilegios de administrador con cifras de usuarios muy elevadas. En lugar de asignar directamente capacidades y organizaciones controladas a los usuarios, conviene utilizar roles de administrador para otorgar privilegios de administrador.

La asignación de capacidades, organizaciones o ambas a un rol de administrador puede ser directa o dinámica (indirecta).

- **Directo**. Con este método, las capacidades y/u organizaciones controladas se asignan explícitamente al rol de administrador. Por ejemplo, a un rol de administrador se le podría asignar la capacidad Administrador de informes de usuario y la organización controlada superior.
- **Dinámico** (*indirecto*). Este método aplica reglas para asignar capacidades y organizaciones controladas. Las reglas se evalúan cada vez que inicia la sesión un administrador que tiene asignado el rol de administrador. Una vez autenticado un administrador, las reglas determinan dinámicamente qué conjunto de capacidades y/u organizaciones controladas se asigna.

  Por ejemplo, cuando un usuario inicia la sesión:

  - Si su cargo de usuario de Active Directory (AD) es *administrador*, la regla de capacidades podría devolver Administrador de cuentas como capacidad para ser asignada.

- Si su departamento de usuario de Active Directory (AD) es *marketing*, la regla de organizaciones controladas podría devolver Marketing como organización controlada para ser asignada.

La asignación dinámica de roles de administrador a los usuarios se puede habilitar o inhabilitar para cada interfaz de inicio de sesión (por ejemplo, interfaz de usuario o de administración). Para ello, defina el siguiente atributo de configuración del sistema en `true` o `false`:

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.logininterface`

El valor predeterminado para todas las interfaces es `false`.

Encontrará instrucciones para editar el objeto de configuración del sistema en "Edición de objetos de configuración de Identity Manager" en la página 118.

Reglas de roles de administrador

Identity Manager incluye reglas de ejemplo que puede aprovechar para crear reglas de roles de administrador. Estas reglas se encuentran en el directorio de instalación de Identity Manager dentro del archivo `sample/adminRoleRules.xml`.

La Tabla 6–1 contiene los nombres de regla y el tipo de autorización (`authType`) que debe especificar con cada una.

TABLA 6–1 Ejemplos de reglas de roles de administrador

Nombre de regla	`authType`
Regla de organizaciones controladas	`ControlledOrganizationsRule`
Regla de capacidades	`CapabilitiesRule`
Regla de usuario con rol de administrador asignado	`UserIsAssignedAdminRoleRule`

Nota – Encontrará información sobre las reglas de ejemplo suministradas para los roles de administración de usuarios de proveedores de servicios dentro de "Administración delegada para usuarios de Service Provider" en la página 545 en el Capítulo 17, "Administración de Service Provider".

El rol de administrador de usuarios

Identity Manager incluye un rol de administrador interno: el rol de administrador de usuarios. Carece de asignaciones predeterminadas de capacidades y organizaciones controladas. No se

puede eliminar. Este rol de administrador se asigna implícitamente a todos los usuarios (usuarios finales y administradores) al iniciar la sesión, con independencia de la interfaz donde la inicien (por ejemplo, usuario, administración, consola o Identity Manager IDE).

Nota – Encontrará información sobre la creación de roles de administrador para los usuarios de proveedores de servicios dentro de "Administración delegada para usuarios de Service Provider" en la página 545 en el Capítulo 17, "Administración de Service Provider".

El rol de administrador de usuarios se puede editar en la interfaz de administración (seleccione Seguridad y después Roles de administrador (Admin).

Como las capacidades u organizaciones controladas asignadas estáticamente mediante este rol de administrador se asignan a todos los usuarios, se recomienda utilizar reglas para asignar capacidades y organizaciones controladas. Así será posible que distintos usuarios tengan distintas (o ninguna) capacidades, mientras que el ámbito de las asignaciones dependerá de factores como quiénes son, en qué departamento trabajan o si son directivos, lo que puede consultarse en el contexto de las reglas.

El rol de administrador de usuarios no impide ni sustituye el uso de la marca `authorized=true` en los flujos de trabajo. Esta marca sigue siendo apropiada cuando el usuario no debería tener acceso a los objetos a los que se accede en el flujo de trabajo, excepto cuando se está ejecutando el flujo de trabajo. Básicamente, esto permite al usuario introducir un modo de *ejecución como superusuario*.

No obstante, a veces interesa que un usuario tenga acceso específico a uno o más objetos fuera (y potencialmente dentro) de los flujos de trabajo. En estos casos, el uso de reglas para asignar dinámicamente capacidades y organizaciones controladas permite la autorización minuciosa de dichos objetos.

Creación y edición de roles de administrador

Para crear o editar un rol de administrador, debe tener asignada la capacidad Administrador de roles de Admin.

Para acceder a los roles de administrador en la interfaz de administración, seleccione Seguridad y después la ficha Roles de administrador (Admin). La lista de la página Roles de administrador (Admin) sirve para crear, editar y eliminar roles de administrador para los usuarios de Identity Manager y los usuarios de proveedores de servicios.

Para editar un rol de administrador existente, haga clic en un nombre de la lista. Pulse Nuevo para crear un rol de administrador. Identity Manager muestra las opciones de la vista Crear rol de administrador (Admin) (ilustrada en la Figura 6–3). La vista Crear rol de administrador (Admin) ofrece cuatro fichas que sirven para especificar los atributos, las capacidades y el ámbito genéricos del nuevo rol de administración, así como asignaciones del rol a los usuarios.

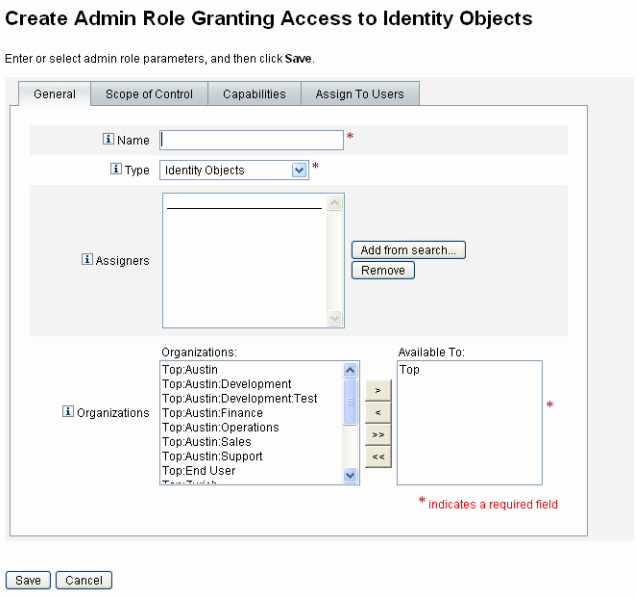


FIGURA 6–3 Página Crear rol de administrador (Admin): ficha General

Ficha General

En la ficha General de la vista de creación o edición de rol de administrador se especifican las siguientes características básicas del rol de administrador:

- **Nombre**. Un nombre único para este rol de administrador.

  Por ejemplo, podría crear el rol de administrador financiero para los usuarios que vayan a tener capacidades administrativas en el departamento (u organización) financiero.

- **Tipo**. Elija Objetos de Identity o Usuarios de Service Provider como tipo. Este campo es necesario.

  Seleccione Objetos de Identity si va a crear un rol de administrador para usuarios (u objetos) de Identity Manager. Seleccione Usuarios de Service Provider si va a crear el rol de administrador para conceder acceso a usuarios de proveedores de servicios.

Nota – Encontrará información sobre la creación de roles de administrador para otorgar acceso a los usuarios de proveedores de servicios dentro de "Administración delegada para usuarios de Service Provider" en la página 545 en el Capítulo 17, "Administración de Service Provider".

- **Asignadores**. Seleccione o busque los usuarios que estarán autorizados a asignar este rol de administrador a otros usuarios. El conjunto de usuarios seleccionables incluye los que tienen asignado el derecho de asignar capacidades.

  Si no se selecciona ningún usuario, el único que podrá asignar el rol de administrador será el que lo haya creado. Si el usuario que creó el rol de administrador no tiene asignada la capacidad Asignar capacidades de usuario, seleccione uno o varios usuarios como Asignadores para garantizar que al menos un usuario pueda asignar el rol de administrador a otro usuario.
- **Organizaciones**. Seleccione una o varias organizaciones para las que estará disponible este rol de administrador. Este campo es necesario.

  El administrador puede administrar objetos en la organización asignada y en cualquier organización que pertenezca a ella en la jerarquía.

Ámbito de control

Identity Manager permite controlar qué usuarios quedan dentro del ámbito de control de un usuario final.

Use la ficha Ámbito de control (Figura 6–4) para especificar las organizaciones que pueden administrar los afiliados a esta organización, o la regla determinante de las organizaciones que deben administrar los usuarios con rol de administrador, así como para seleccionar el formulario de usuario para el rol de administrador.

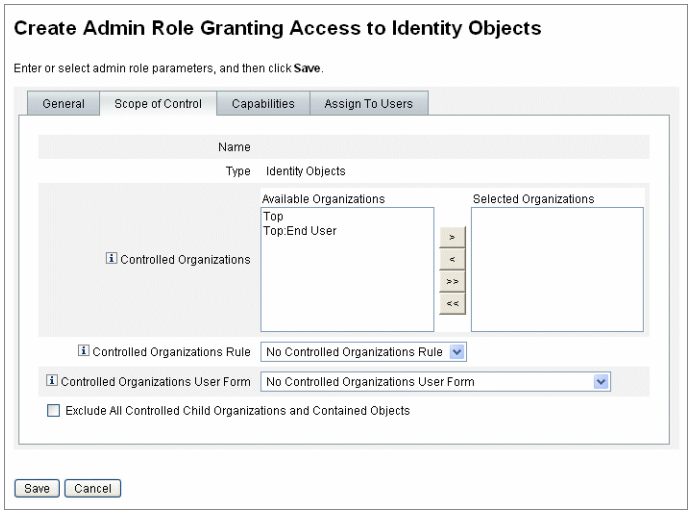


FIGURA 6–4 Crear rol de administrador (Admin): Ámbito de control

- **Organizaciones controladas**. En la lista Organizaciones disponibles, seleccione las organizaciones que este rol de administrador tiene derecho a gestionar.
- **Regla de organizaciones controladas**. Seleccione una regla que, al iniciar la sesión, evaluará las organizaciones que deben ser controladas por el usuario al que se le asigne este rol de administrador. La regla seleccionada debe tener el tipo de autenticación `ControlledOrganizationsRule`. De manera predeterminada no se selecciona ninguna regla de organización controlada.

  Puede aplicar la regla `EndUserControlledOrganizations` para establecer la lógica necesaria para asegurar que el conjunto adecuado de usuarios esté disponible para delegar, de acuerdo con sus necesidades organizativas.

  Si prefiere que la lista de usuarios del ámbito sea igual para los administradores, ya utilicen la interfaz de administración o de usuario final, debe cambiar la regla `EndUserControlledOrganizations.`

  Modifique la regla para comprobar primero si el usuario autenticador es un administrador y después configure lo siguiente:

  - Si el usuario no es un administrador, devolver el conjunto de organizaciones que debe controlar un usuario final, como su propia organización (por ejemplo, `waveset.organization`).
  - Si el usuario es un administrador, no devolver ninguna organización, de manera que el usuario sólo controle las organizaciones que se le asignen por ser administrador.

    Por ejemplo:

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'>
  <Comments>
    If the user logging in is not an Idm administrator,
    then return the organization that they are a member of.
    Otherwise, return null.
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>
```

- Si el usuario o administrador pertenecen a una organización dinámica, no se devuelven en los resultados de búsqueda.

  Sin embargo, es posible crear una regla para devolver usuarios en organizaciones dinámicas. Cambie la regla de ejemplo siguiente añadiendo un atributo nuevo a la definición de esquema de usuario de Identity Manager incluida en el objeto `Idm Schema Configuration`, importe dicho objeto y después reinicie el servidor de Identity Manager.

```
        <IDMAttributeConfigurations>
            ...
            <IDMAttributeConfiguration name='region'
                                       syntax='STRING'
                                       description='region of the country'/>
        </IDMAttributeConfigurations>

        <IDMObjectClassConfigurations>
            ...
            <IDMObjectClassConfiguration name='User'
                                         extends='Principal'
                                           description='User description'>
                ...
                <IDMObjectClassAttributeConfiguration name='region'
                                                      queryable='true'/>
            </IDMObjectClassConfiguration>
        </IDMObjectClassConfigurations>

Next, import the following Identity Manager objects:
```

```
<!-- User member rule that will include all users whose region attribute
matches the region organization display name -->

<Rule name="Region User Member Rule" authType="UserMembersRule">
  <Description>User Member Rule</Description>
  <list>
    <new class='com.waveset.object.AttributeCondition'>
      <s>region</s>
      <s>equals</s>
      <ref>userMemberRuleOrganizationDisplayName</ref>
    </new>
  </list>
  <MemberObjectGroups>
    <ObjectRef type="ObjectGroup" id="#ID#All" name="All"/>
  </MemberObjectGroups>
</Rule>

<!-- North & South Region organizations with user member rule assigned -->

<ObjectGroup id='#ID#North Region' name='North Region'
displayName='North Region'> <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<ObjectGroup id='#ID#South Region' name='South Region'
displayName='South Region'>  <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- Organization containing all employees -->

<ObjectGroup id='#ID#Employees' name='Employees' displayName='Employees'>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- End user controlled organization rule that give each user control
of the regional organization they are a member of -->
```

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'
      primaryObjectClass='Rule'>
  <switch>
    <ref>waveset.attributes.region</ref>
    <case>
      <s>North Region</s>
      <s>North Region</s>
    </case>
    <case>
      <s>South Region</s>
      <s>South Region</s>
    </case>
    <case>
      <s>East Region</s>
      <s>East Region</s>
    </case>
    <case>
      <s>West Region</s>
      <s>West Region</s>
    </case>
  </switch>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>

<!-- 4 employees (2 in North and 2 in South region) -->

<User name='emp1' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee One'/>
  <Attribute name='lastname' type='string' value='One'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp2' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Two'/>
  <Attribute name='lastname' type='string' value='Two'/>
  <Attribute name='region' type='string' value='North Region'/>
```

```
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp4' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Four'/>
  <Attribute name='lastname' type='string' value='Four'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp5' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Five'/>
  <Attribute name='lastname' type='string' value='Five'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>
```

A continuación, inicie la sesión en la interfaz de usuario final de Identity Manager como `emp1` , que se halla al norte del país. Seleccione Delegaciones → Nuevo. Cambie el criterio de búsqueda a **`Comienza con`** y el valor a **`emp`**, después elija Buscar. Con este método se debería devolver `emp2` en la lista de usuarios disponibles.

- **Formulario de usuario de organizaciones controladas**. Seleccione el formulario de usuario que utilizará un usuario que tenga asignado este rol de administrador cuando cree o edite usuarios afiliados a estas organizaciones controladas del rol de administrador. De manera predeterminada no se selecciona ningún formulario de usuario regla de organizaciones controladas.

  Un formulario de usuario asignado mediante un rol de administrador sustituye a cualquier formulario de usuario heredado de la organización a la que pertenece el administrador. No sustituye a los formularios de usuario asignados directamente al administrador.

Asignación de capacidades al rol de administrador

Las capacidades asignadas al rol de administrador determinan los derechos administrativos que tienen los usuarios asignados al rol de administrador. Por ejemplo, este rol de administrador

podría restringirse a la creación de usuarios exclusivamente para las organizaciones controladas especificadas del rol de administrador. En tal caso, deberá asignar la capacidad Crear usuario.

En la ficha Capacidades, seleccione las opciones siguientes.

- **Capacidades**. Son capacidades (derechos administrativos) específicos que los usuarios del rol de administrador tendrán para sus organizaciones controladas. Elija una o más capacidades en la lista de capacidades disponibles y trasládelas a la lista Capacidades asignadas.
- **Regla de capacidades**. Seleccione una regla de manera que, cuando se evalúe al iniciar la sesión el usuario, determine la lista de cero o más capacidades otorgadas a los usuarios que tienen el rol de administrador. La regla seleccionada debe tener el tipo de autenticación `CapabilitiesRule`.

Asignación de formularios de usuario a un rol de administrador

Puede especificar un formulario de usuario para quienes tienen un rol de administrador. Use la ficha Asignar a usuarios de la vista de creación o edición de rol de administrador para especificar las asignaciones.

El administrador que tiene asignado el rol de administrador utilizará este formulario al crear o editar usuarios en las organizaciones controladas por dicho rol. Un formulario de usuario asignado mediante un rol de administrador sustituye a cualquier formulario de usuario heredado de la organización a la que pertenece el administrador. Este formulario no sustituye a los formularios de usuario asignados directamente al administrador.

El formulario de usuario empleado para editar un usuario se determina por este orden de prioridad:

- Si hay un formulario de usuario asignado directamente al administrador, es ése el que se utiliza.
- Si no hay ningún formulario de usuario asignado directamente al administrador, pero éste tiene asignado un rol de administrador que controla la organización al que pertenece el usuario que se crea o edita y se especifica un formulario de usuario, es ése el que se utiliza.
- Si no hay ningún formulario de usuario asignado directamente al administrador, o asignado indirectamente mediante un rol de administrador, se utiliza el formulario asignado a las organizaciones del administrador (empezando justo después de la `Superior`).
- Sin ninguna de las organizaciones del administrador tiene asignado un formulario, se utiliza el formulario de usuario predeterminado.

Si un administrador tiene asignados varios roles de administrador que controlan la misma organización pero especifican distintos formularios de usuario, aparece un error cuando intenta

crear o editar un usuario de dicha organización. Si un administrador intenta asignar dos o más roles de administrador que controlan la misma organización pero especifican distintos formularios de usuario, también aparece un error. Los cambios no pueden guardarse hasta que se resuelve el conflicto.

La organización de usuario final

La organización de usuario final brinda a los administradores un medio práctico para poner a disposición de los usuarios finales determinados objetos, como recursos y roles. Los usuarios finales pueden ver y potencialmente asignarse objetos designados a sí mismos (pendientes de proceso de aprobación) a través de la interfaz de usuario final ("Inicio de sesión en la interfaz de usuario final de Identity Manager" en la página 43).

Nota – La organización de usuario final se introdujo en la versión 7.1.1 de Identity Manager.

Para poder conceder a los usuarios finales acceso a los objetos de configuración de Identity Manager (como roles, recursos, tareas y demás), antes los administradores tenían que editar los objetos de configuración y utilizar tareas de usuario final, recursos de usuario final y tipos de autenticación de usuario final.

Para seguir avanzando, Sun recomienda utilizar la organización de usuario final para conceder a los usuarios finales acceso a los objetos de configuración de Identity Manager.

La organización de usuario final es controlada implícitamente por todos los usuarios y les permite visualizar varios tipos de objetos, incluyendo tareas, reglas, roles y recursos. Sin embargo, la organización carece inicialmente de objetos.

La organización de usuario final pertenece a la `superior` y no puede tener organizaciones secundarias. Además, la organización de usuario final no aparece en la lista de la página Cuentas. A pesar de esto, cuando se modifican objetos (como roles, roles de administración, recursos, directivas, tareas, etc.) puede utilizar la interfaz de usuario de administración con el fin de que cualquier objeto esté disponible para la organización de usuario final.

Cuando los usuarios finales inician la sesión en la interfaz de usuario final, ocurre lo siguiente:

- Los usuarios finales reciben el control de la organización de `usuario final` (`ObjectGroup`).
- Identity Manager evalúa la regla interna de organización controlada de usuario final, que automáticamente otorga al usuario el control de todos los nombres de organización que devuelve la regla. (Esta regla se incorporó en la versión 7.1.1 de Identity Manager. Encontrará más información en la sección "La regla de organización controlada de usuario final" en la página 232.)
- Los usuarios finales reciben derechos sobre los tipos de objeto especificados en la capacidad `EndUser`.

La regla de organización controlada de usuario final

El argumento de entrada para la regla de organización controlada de usuario final es la vista del usuario que se autentica. Identity Manager espera que la regla devuelva una o varias organizaciones que serán controladas por el usuario que inicia la sesión en la interfaz de usuario final. Identity Manager espera que la regla devuelva una cadena (para una sola organización) o una lista (para varias organizaciones).

Para gestionar estos objetos, los usuarios necesitan la capacidad Administrador de usuario final. Los usuarios que tienen asignada la capacidad Administrador de usuario final pueden ver y modificar el contenido de la regla de organización controlada de usuario final. Estos usuarios también pueden ver y modificar los tipos de objeto especificados en la capacidad de usuario final (EndUser).

La capacidad Administrador de usuario final se asigna de forma predeterminada al usuario Configurator. Los usuarios que han iniciado la sesión no pueden ver de forma dinámica los cambios que se producen en la lista o en las organizaciones que se devuelven al evaluar la regla de organización controlada de usuario final. Para ver los cambios tienen que cerrar la sesión y volver a iniciarla.

Si la regla de organización controlada de usuario final devuelve una organización no válida (por ejemplo, una inexistente en Identity Manager), el problema se incluye en el registro del sistema. Para solucionarlo, inicie la sesión en la interfaz de administración y corrija la regla.

Administración de elementos de trabajo

Algunos procesos de flujo de trabajo generados por tareas en Identity Manager crean elementos de acción o *elementos de trabajo*. Estos elementos de trabajo pueden ser solicitudes de aprobación u otra solicitud de acción asignada a una cuenta de Identity Manager.

Identity Manager agrupa todos los elementos de trabajo en el área Elementos de trabajo de la interfaz, lo que permite ver y responder a todas las solicitudes pendientes desde una única ubicación.

Tipos de elementos de trabajo

Los elementos de trabajo pueden ser de los siguientes tipos:

- **Aprobaciones**. Solicitudes de aprobaciones de nuevas cuentas o modificaciones de cuentas.
- **Autenticaciones**. Solicitudes para revisar y aprobar derechos de usuario.
- **Remediaciones**. Solicitudes para remediar o mitigar infracciones de directiva de auditoría de cuentas de usuario.
- **Otros**. Solicitudes de elementos de acción de cualquier otro tipo. Pueden ser solicitudes de acción generadas por un flujo de trabajo personalizado.

Para ver los elementos de trabajo pendientes de cada tipo, seleccione Elementos de trabajo en el menú.

Nota – Si posee elementos de trabajo pendientes (o delegados), cuando inicie la sesión en la interfaz de usuario de Identity Manager aparecerá su lista de Elementos de trabajo.

Manipulación de solicitudes de elementos de trabajo pendientes

Para responder a una solicitud de elemento de trabajo, haga clic en uno de los tipos de elementos de trabajo dentro del área Elementos de trabajo de la interfaz. Seleccione elementos de la lista de solicitudes y después pulse uno de los botones disponibles para indicar la acción que desear realizar. Las opciones de los elementos de trabajo varían según su tipo.

Encontrará más información para responder a las solicitudes en los temas siguientes:

- "Aprobación de cuentas de usuario" en la página 237
- "Administración de tareas de autenticación" en la página 495
- "Remediación y mitigación de infracciones del cumplimiento" en la página 470

Visualización del historial de elementos de trabajo

La ficha Historial del área Elementos de trabajo muestra los resultados de las acciones de elementos de trabajo anteriores.

La Figura 6–5 muestra una vista de ejemplo del historial de elementos de trabajo.

FIGURA 6–5 Vista del historial de elementos de trabajo

Delegación de elementos de trabajo

Los propietarios de elementos de trabajo pueden manejar las cargas de trabajo delegando elementos de trabajo en otros usuarios durante un periodo concreto. La página Elementos de trabajo → Delegar mis elementos de trabajo del menú principal sirve para delegar futuros elementos de trabajo (como solicitudes de aprobación) en uno o más usuarios (delegados). No es necesario que los usuarios dispongan de capacidades de aprobador para ser delegados.

Nota – La función de delegación se aplica únicamente a elementos de trabajo futuros. Los elementos existentes (los indicados en Mis elementos de trabajo) se deben remitir selectivamente mediante la función de reenvío.

También se pueden delegar elementos de trabajo desde otras páginas:

- En las páginas Crear usuario y Editar usuario de la interfaz de administración ("Páginas de usuario (Crear/Editar/Ver)" en la página 54). Haga clic en la ficha Delegaciones.
- En la interfaz de usuario final ("Interfaz de usuario final de Identity Manager" en la página 40), los usuarios pueden seleccionar la opción de menú Delegaciones.

Los delegados pueden aprobar elementos de trabajo en nombre de los propietarios de dichos elementos durante el periodo de delegación efectivo. Los elementos de trabajo delegados incluyen el nombre del delegado.

Cualquier usuario puede crear una o más delegaciones para sus elementos de trabajo futuros. Los administradores que pueden editar un usuario también pueden crear una delegación en nombre de dicho usuario. Sin embargo, un administrador no puede delegar en alguien en quien no pueda delegar el usuario. (En lo que respecta a las delegaciones, el ámbito de control del administrador es igual que el del usuario en cuyo nombre se delega.)

Entradas del registro de auditoría

Las entradas del registro de auditoría muestran el nombre del delegador cuando se aprueban o rechazan elementos de trabajo delegados. Los cambios realizados en la información del aprobador delegado de un usuario se registran en la sección de cambios detallados de la entrada de registro de auditoría cuando se crea o se modifica un usuario.

Visualización de las delegaciones actuales

Las delegaciones se ven en la página Delegaciones actuales.

▼ Para ver las delegaciones actuales

1. **En la interfaz de administración, seleccione Elementos de trabajo en el menú principal.**
2. **Elija Delegar mis elementos de trabajo en el menú secundario.**

   Identity Manager muestra la página Delegaciones actuales, donde puede ver y editar las delegaciones vigentes.

Visualización de delegaciones anteriores

Las delegaciones anteriores se ven en la página Delegaciones anteriores.

▼ Para ver las delegaciones anteriores

1. **En la interfaz de administración, seleccione Elementos de trabajo en el menú principal.**
2. **Elija Delegar mis elementos de trabajo en el menú secundario.**

   Aparece la página Delegaciones actuales.
3. **Haga clic en Anterior.**

   Aparece la página Delegaciones anteriores. Los elementos de trabajo delegados con anterioridad se pueden aprovechar para configurar nuevas delegaciones.

Creación de delegaciones

Las delegaciones se crean en la página Nueva delegación.

▼ Para crear una delegación

1. **En la interfaz de administración, seleccione Elementos de trabajo en el menú principal.**
2. **Seleccione Delegar mis elementos de trabajo.**

   Aparece la página Delegaciones actuales.

3 **Pulse Nuevo.**

Aparece la página Nueva delegación.

4 **Rellene el formulario así:**

a. **Seleccione un tipo de elemento de trabajo en la lista Seleccionar tipo de elemento de trabajo para delegar. Para delegar todos sus elementos de trabajo, seleccione Todos los tipos de elementos de trabajo.**

Si va a delegar un elemento de trabajo de tipo de rol, organización o recurso, especifique los roles, organizaciones o recursos concretos que deben definir esta delegación utilizando las flechas para trasladarlos de la columna Disponible a la columna Seleccionado.

b. **Delegar elementos de trabajo a.**

Seleccione una de estas opciones:

- **Usuarios seleccionados**. Le sirve para buscar usuarios de su ámbito de control (por nombre) para convertirlos en delegados. Si alguno de los delegados seleccionados ha delegado también sus elementos de trabajo, las solicitudes de elementos de trabajo futuras se delegarán a los delegados de ese delegado.
- **Seleccione uno o más usuarios en el área Usuarios seleccionados**. Otra posibilidad es elegir Agregar de búsqueda para abrir la función de búsqueda y buscar usuarios. Pulse Agregar para agregar un usuario encontrado a la lista. Para eliminar un delegado de la lista, selecciónelo y, a continuación, haga clic en Eliminar.
  - **Mi administrador**. Esta opción delega los elementos de trabajo en su administrador (si está asignado).
  - **Regla de elementos de trabajo delegados**. Seleccione una regla que devuelva una lista de nombres de usuario de Identity Manager en quienes pueda delegar el tipo de elemento de trabajo seleccionado.

c. **Fecha de inicio. Seleccione la fecha en la que debe comenzar la delegación del elemento de trabajo. De forma predeterminada, el día seleccionado comienza a las 12:01 a.m.**

d. **Fecha final. Seleccione la fecha en la que debe terminar la delegación del elemento de trabajo. De forma predeterminada, el día seleccionado finaliza a las 11:59 p.m.**

Nota – Puede elegir la misma fecha inicial y final para delegar elementos de trabajo sólo durante un día.

---

e. **Pulse Aceptar para guardar las selecciones y regresar a la lista de elementos de trabajo en espera de aprobación.**

Nota – Una vez configurada la delegación, todos los elementos de trabajo que se creen durante el periodo efectivo de delegación se añadirán a la lista del delegado. Si el usuario termina una delegación o el periodo de delegación caduca, los elementos de trabajo delegados se devuelven a su lista. En consecuencia, pueden duplicarse elementos de trabajo en la lista. No obstante, Al aprobar o rechazar un elemento, su duplicado se suprime automáticamente de la lista.

Delegaciones a usuarios eliminados

Cuando se elimina un usuario que es propietario de elementos de trabajo pendientes, Identity Manager actúa así:

- Si los elementos de trabajo pendientes se han delegado y el delegador no se ha eliminado, dichos elementos se devuelven al delegador.
- Si los elementos de trabajo pendientes no se han delegado, o se han delegado y el delegador se ha eliminado, el intento de eliminación no tendrá efecto hasta que los elementos de trabajo pendientes se hayan resuelto o remitido a otro usuario.

Terminación de delegaciones

Las delegaciones se terminan en la página Delegaciones actuales.

▼ Para terminar una o más delegaciones

1. **En la interfaz de administración, seleccione Elementos de trabajo en el menú principal.**
2. **Elija Delegar mis elementos de trabajo en el menú secundario.**
   Aparece la página Delegaciones actuales.
3. **Seleccione una o varias delegaciones para terminarlas y después haga clic en Finalizar.**
   Identity Manager suprime las configuraciones de delegación seleccionadas y devuelve a la lista de elementos pendientes todos los elementos de trabajo delegados del tipo elegido.

Aprobación de cuentas de usuario

Cuando se añade un usuario al sistema Identity Manager, los administradores asignados como *aprobadores* de nuevas cuentas deben validar la creación de la cuenta.

Identity Manager ofrece tres categorías de aprobación:

- **Organización**. Hace falta aprobación para añadir la cuenta de usuario a la organización.
- **Rol**. Hace falta aprobación para asignar la cuenta de usuario a un rol.

- **Recurso**. Hace falta aprobación para proporcionar acceso a un recurso a la cuenta de usuario.

Además, si se habilitan las aprobaciones de cambio y se efectúan cambios en un rol, se envía un elemento de trabajo de aprobación de cambio a los propietarios de rol designados.

Identity Manager permite aprobaciones de cambios por *definición de roles*. Si un administrador cambia una definición de rol, se necesita que un propietario del rol apruebe los cambios. Para que el cambio sea efectivo, un propietario del rol debe aprobar el elemento de trabajo.

Nota –

- Identity Manager puede configurarse para aprobaciones por firma digital. Encontrará las instrucciones en "Configuración de aprobaciones y acciones por firma digital" en la página 240.
- Los nuevos administradores de Identity Manager a veces confunden el concepto de aprobación con el de autenticación. Aunque puedan parecer similares, se producen en contextos distintos.

  Las aprobaciones están relacionadas con la validación de nuevas cuentas de usuario. Cuando se añade un usuario a Identity Manager, pueden hacer falta una o más aprobaciones para validar la autorización de la nueva cuenta.

  Las autenticaciones están relacionadas con la verificación de que los usuarios existentes sólo tienen los privilegios adecuados en los recursos adecuados. Dentro de un proceso de revisión de acceso periódico, se puede instar a un usuario de Identity Manager (el autenticador) a que certifique si son válidos y correctos los datos de la cuenta de otro usuario (es decir, los recursos que tiene asignados). Este proceso se denomina autenticación.

Configuración de aprobadores de cuentas

Configurar aprobadores de cuentas para las aprobaciones de organizaciones, roles y recursos es optativo, pero aconsejable. Por cada categoría donde se configuran aprobadores se necesita al menos una aprobación para crear una cuenta. Si un aprobador rechaza una solicitud de aprobación, no se crea la cuenta.

Es posible asignar más de un aprobador a cada categoría. Como sólo se precisa una aprobación dentro de una categoría, es posible configurar diversos aprobadores para contribuir a impedir que el flujo de trabajo se retrase o detenga. Si un aprobador no está disponible, lo estarán otros para gestionar las aprobaciones. La aprobación sólo se aplica a la creación de cuentas. De manera predeterminada, las actualizaciones y eliminaciones de cuentas no requieren aprobación. Sin embargo, es posible personalizar este proceso para que sí la requiera.

Los flujos de trabajo se pueden personalizar aprovechando Identity Manager IDE para cambiar el flujo de aprobaciones, capturar las eliminaciones de cuentas y las actualizaciones.

Encontrará información sobre Identity Manager IDE en `https://identitymanager.dev.java.net`. Para obtener información sobre los flujos de trabajo y consultar un ejemplo ilustrado de su alteración, consulte el Capítulo 1, "Workflow" de *Sun Identity Manager Deployment Reference*.

Los aprobadores de Identity Manager pueden aprobar o rechazar una solicitud de aprobación.

Los administradores pueden ver y gestionar las aprobaciones pendientes desde el área Elementos de trabajo de la interfaz de Identity Manager. En la página Elementos de trabajo, seleccione **Mis elementos de trabajo** para ver las aprobaciones pendientes. Haga clic en la ficha **Aprobaciones** para administrar aprobaciones.

Firma de aprobaciones

Para aprobar un elemento de trabajo mediante una firma digital, primero debe configurarla como se explica en "Configuración de aprobaciones y acciones por firma digital" en la página 240.

▼ Para firmar una aprobación

1. **En la interfaz de administración de Identity Manager, seleccione Elementos de trabajo.**
2. **Haga clic en la ficha Aprobaciones.**
3. **Seleccione una o varias aprobaciones en la lista.**
4. **Introduzca comentarios referentes a la aprobación y haga clic en Aprobar.**

   Identity Manager le preguntará si se debe confiar en el applet.
5. **Haga clic en Siempre.**

   Identity Manager muestra un resumen fechado de la aprobación.
6. **Introduzca o pulse Examinar para buscar la ubicación del almacén de claves. (Esta ubicación se establece al configurar la aprobación mediante firma, como se explica en el paso 10m del procedimiento "Para habilitar la configuración del lado del servidor para aprobaciones firmadas mediante PKCS12" en la página 242.)**
7. **Introduzca la contraseña del almacén de claves, que se establece al configurar la aprobación mediante firma, como se explica en el paso 10l del procedimiento "Para habilitar la configuración del lado del servidor para aprobaciones firmadas mediante PKCS12" en la página 242.**
8. **Haga clic en Firmar para aprobar la solicitud.**

Más información Firma de aprobaciones posteriores

Tras firmar una aprobación, para las acciones de aprobación posteriores sólo se requerirá que introduzca la contraseña del almacén de claves y que después haga clic en **Firmar**. (Identity Manager recuerda la ubicación del almacén de claves desde la aprobación anterior.)

Configuración de aprobaciones y acciones por firma digital

Utilice la información y los procedimientos descritos a continuación para configurar la operación de firma digital. Es posible firmar digitalmente:

- Aprobaciones (incluidas las de cambios)
- Acciones de revisión de acceso
- Remediaciones de infracciones de cumplimiento

En esta sección se explica la configuración del lado del servidor y del lado del cliente necesaria para agregar el certificado y la CRL a Identity Manager para las aprobaciones firmadas.

▼ Para habilitar la configuración del lado del servidor para aprobaciones firmadas

1 **Abra el objeto de configuración del sistema para editarlo y defina**
`security.nonrepudiation.signedApprovals=true`

Encontrará instrucciones para editar el objeto de configuración del sistema en "Edición de objetos de configuración de Identity Manager" en la página 118.

En caso de utilizar PKCS11, también deberá definir
`security.nonrepudiation.defaultKeystoreType=PKCS11`

Si utiliza un proveedor de claves PKCS11 personalizado, también deberá definir
`security.nonrepudiation.defaultPKCS11KeyProvider=` *nombre de su proveedor*

Nota – Para obtener más información acerca de cuándo es necesario incluir un proveedor personalizado, consulte los elementos siguientes en el kit REF.

`com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`
`REF/transactionsigner/SamplePKCS11KeyProvider`

El kit REF (Resource Extension Facility) se encuentra en el directorio `/REF` del CD del producto o en la imagen de instalación.

---

2. **Agregue los certificados de su autoridad de certificación (AC) como certificados de confianza. Para ello debe obtener primero una copia de los certificados.**

   Por ejemplo, si utiliza una autoridad de certificación de Microsoft, siga un procedimiento como éste:

   a. **Vaya a** `http://`*IPAddress*`/certsrv` **e inicie la sesión con privilegios administrativos.**

   b. **Elija recuperar el certificado de AC o la lista de revocación de certificados y pulse Next.**

   c. **Descargue el certificado de AC y guárdelo.**

3. **Agregue el certificado a Identity Manager como un certificado de confianza:**

   a. **En la interfaz de administración, seleccione Seguridad y después Certificados. Identity Manager muestra la página Certificados.**

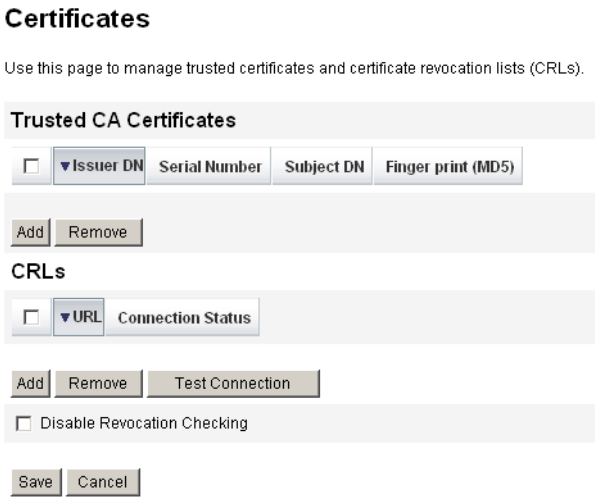


FIGURA 6–6 Página Certificados

   b. **En el área Certificados de CA en los que se confía, haga clic en Añadir. Identity Manager muestra la página Importar certificado.**

   c. **Busque y seleccione el certificado de confianza y haga clic en Importar.**

      Al hacerlo, el certificado aparece en la lista de certificados de confianza.

4 **Agregue la lista de revocación de certificados (CRL) de su AC.**

   a. **En el área CRLs de la página Certificados, pulse Agregar.**

   b. **Especifique la URL de la CRL emitida por la autoridad de certificación (AC).**

   Nota –

   - La lista de revocación de certificados (CRL) es una lista de números de serie de certificados que se han revocado o no son válidos.
   - La URL de la CRL emitida por la autoridad de certificación (AC) puede ser http o LDAP.
   - Cada AC tiene una URL distinta donde se distribuyen las CRL. Puede averiguar cuál es examinando la extensión de puntos de distribución de CRL del certificado.

5 **Haga clic en Conexión de prueba para verificar la URL.**

6 **Haga clic en Guardar.**

7 **Firme los applets**`/ts2.jar`**mediante jarsigner.**

Nota – Encontrará más información en `http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/jarsigner.html`. El archivo `ts2.jar` suministrado con Identity Manager se firma mediante un certificado firmado automáticamente y no debe utilizarse con sistemas de producción. En producción conviene volver a firmar este archivo utilizando un certificado de firma codificada emitido por su AC de confianza.

▼ Para habilitar la configuración del lado del servidor para aprobaciones firmadas mediante PKCS12

La siguiente información de configuración corresponde a aprobaciones firmadas mediante PKCS12. Obtenga un certificado y una clave privada, y después expórtelos a un almacén de claves PKCS#12. Por ejemplo, si utiliza una autoridad de certificación de Microsoft, siga un procedimiento como éste:

Antes de empezar Identity Manager ahora requiere como mínimo JRE 1.5.

1 **Con Internet Explorer, vaya a** `http://`*IPAddress*`/certsrv` **e inicie la sesión con privilegios administrativos.**

2 **Seleccione Request a certificate y pulse Next.**

3 **Seleccione Advanced request y pulse Next.**

4. **Pulse Next.**
5. **Seleccione User for Certificate Template.**
6. **Seleccione estas opciones:**
   a. **Mark keys as exportable.**
   b. **Enable strong key protection.**
   c. **Use local machine store.**
7. **Pulse Submit y después OK.**
8. **Haga clic en Install this certificate.**
9. **Seleccione Run → mmc para iniciar mmc.**
10. **Agregue el componente de certificado:**
    a. **Seleccione Console → Add/Remove Snap-in.**
    b. **Haga clic en Add.**
    c. **Seleccione Computer account.**
    d. **Pulse Next y después Finish.**
    e. **Haga clic en Close.**
    f. **Haga clic en OK.**
    g. **Vaya a Certificates → Personal → Certificates.**
    h. **Haga clic con el botón secundario en Administrator All Tasks → Export.**
    i. **Pulse Siguiente.**
    j. **Pulse Next para confirmar la exportación de la clave privada.**
    k. **Pulse Siguiente.**
    l. **Introduzca una contraseña y pulse Next.**

m. Archivo *CertificateLocation***.**

n. Pulse Next y después Finish. Pulse OK para confirmar.

Nota – Anote la información utilizada en los pasos 10l (contraseña) y 10m (ubicación del certificado) de la configuración del lado del cliente. Necesitará dicha información para firmar aprobaciones.

▼ Para habilitar la configuración del lado del cliente para aprobaciones firmadas mediante PKCS11

Si va a utilizar PKCS11 para las aprobaciones firmadas

- **Consulte los recursos siguientes en el kit REF para obtener información sobre la configuración:**

  `com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`
  `REF/transactionsigner/SamplePKCS11KeyProvider`

  El kit REF (Resource Extension Facility) se encuentra en el directorio `/REF` del CD del producto o en la imagen de instalación.

Visualización de la firma de transacción

A continuación se explica el procedimiento para ver firmas de transacciones en un informe de registro de auditoría de Identity Manager.

▼ Para ver una firma de transacción

1. **En la interfaz de administración de Identity Manager, seleccione Informes.**
2. **En la página Ejecutar informes, elija Informe de AuditLog dentro de la lista de opciones Nuevo.**
3. **En el campo Título del informe, escriba un título (por ejemplo, Aprobaciones).**
4. **En el área de selección Organizaciones, seleccione todas las organizaciones.**
5. **Elija la opción Acciones y después Aprobar.**
6. **Haga clic en Guardar para guardar el informe y volver a la página Ejecutar informes.**
7. **Haga clic en Ejecutar para ejecutar el informe Aprobaciones.**
8. **Seleccione el vínculo de detalles para ver la información de la firma de transacción.**

La información de la firma de transacción puede incluir:

- Emisor
- Asunto
- Número de serie de certificado
- Mensaje firmado
- Firma
- Algoritmo de firma

Configuración de aprobaciones firmadas en formato XMLDSIG

Identity Manager le permite agregar a su proceso de aprobación aprobaciones firmadas en formato XMLDSIG, incluida una marca de fecha y hora digital conforme con RFC. Cuando se configura Identity Manager para utilizar aprobaciones firmadas en formato XMLDSIG, los aprobadores no perciben los cambios a no ser que visualicen la aprobación en el registro de auditoría. Sólo varía el formato de la aprobación firmada que se almacena en el registro de auditoría.

Como en el caso de las anteriores aprobaciones firmadas en Identity Manager, en la máquina cliente se ejecuta un applet y se presenta al aprobador la información de aprobación para que la firme. A continuación, elige un almacén de claves y una clave para firmar la aprobación.

Una vez que el aprobador ha firmado la aprobación, se crea un documento XMLDSIG que contiene los datos de la aprobación. Este documento se devuelve al servidor, que valida el documento firmado en XMLDSIG. Si el resultado es satisfactorio y se han configurado marcas digitales de fecha y hora RFC 3161, también se genera una marca digital de fecha y hora para este documento. La marca de fecha y hora emitida por la autoridad de marca de fecha y hora (TSA) se verifica para detectar posibles errores y se validan sus certificados. Por último, si todo es correcto, Identity Manager genera un registro de auditoría que incluye el objeto de la aprobación firmada en formato XMLDSIG dentro de la columna blob XML.

Formato de datos de aprobación

Éste es el formato de un objeto de aprobación en formato XMLDSIG:

```
<XMLSignedData signedContent="...base64 transaction text ...">
   <XMLSignature>
      <TSATimestamp>
         ...The base64 encoded PKCS7 timestamp token returned by the TSA...
      </TSATimestamp
      <Signature>
        <SignedInfo>...XMLDSIG stuff...</SignedInfo>
        <SignatureValue>...base64 signature value</SignatureValue>
        <KeyInfo>...cert info for signer</KeyInfo>
```

```
      </Signature>
   </XMLSignature>
</XMLSignedData>
```

donde:

- Los datos de aprobación `base64` son el texto de los datos de la aprobación real presentado al aprobador en el applet, codificado en formato `base64`.
- El elemento `<TSATimestamp>` contiene la respuesta de marca de fecha y hora PKCS7 codificada en `base64` procedente de la autoridad de marcas de fecha y hora (TSA).
- El elemento `<Signature>` contiene los datos de la firma en XMLDSIG.

Este documento XMLDSIG se almacena en la columna XML del registro de aprobación del registro de auditoría.

Instalación y configuración

Los requisitos de instalación y configuración para utilizar aprobaciones firmadas en formato XMLDSIG son iguales a los descritos dentro del apartado "Para habilitar la configuración del lado del servidor para aprobaciones firmadas" en la página 240, pero con un paso más. Debe firmar el archivo `xmlsec-1.4.2.jar` además del archivo `ts2.jar`.

Configuración de aprobación

Puede utilizar los atributos de configuración del sistema para:

- Elegir el formato `SignedData` o `XMLSignedData` . Recuerde que sólo puede configurar un único formato simultáneamente, aunque los administradores pueden cambiar este valor según convenga.
- Incluir una marca digital de fecha y hora obtenida de una autoridad de marcas de fecha y hora (TSA) configurada conforme con RFC 3161.
- Especificar una URL, sólo en HTTP, desde la cual obtener esta marca de fecha y hora.

Si desea editar estos atributos, utilice las páginas de depuración de Identity Manager para editar el objeto de configuración del sistema. Todos estos atributos se encuentran dentro de `security.nonrepudiation`, junto con otros atributos de aprobación firmada.

Los atributos XMLDSIG incluyen:

- `security.nonrepudiation.useXmlDigitalSignatures` es un valor booleano que habilita las firmas XMLDSIG.
- `security.nonrepudiation.timestampXmlDigitalSignatures` es un valor booleano que incluye marcas digitales de fecha y hora RFC 3161 en firmas XMLDSIG.
- `security.nonrepudiation.timestampServerURL` es un valor de cadena donde la URL señala a la TSA basada en HTTP de la cual se obtienen marcas de fecha y hora.

Nota –

- Para que cualquiera de los atributos anteriores tenga efecto, antes debe configurar el atributo `useSignedApprovals` existente en **`true`**.
- Identity Manager no admite varias firmas en una única aprobación ni aprobaciones firmadas para solicitudes de abastecimiento más genéricas.

◆ ◆ ◆ CAPÍTULO 7

Carga y sincronización de datos

En este capítulo se incluye información y procedimientos para utilizar las funciones de carga y sincronización de datos de Identity Manager. Aprenderá a usar las herramientas de sincronización de datos de Identity Manager(descubrimiento, reconciliación y sincronización) para mantener actualizados los datos.

La información se ha organizado como sigue:

Encontrará una explicación detallada sobre cómo funcionan la carga y la sincronización de datos en Identity Manager en el Capítulo 3, "Data Loading and Synchronization" de *Sun Identity Manager Deployment Guide*.

Herramientas de sincronización de datos: ¿cuál usar?

Identity Manager ofrece diversas herramientas para importar y sincronizar datos de cuenta. Encontrará ayuda para seleccionar la herramienta correcta con una tarea específica en la Tabla 7–1.

Nota – Encontrará una explicación detallada sobre cómo funcionan la carga y la sincronización de datos en Identity Manager en el Capítulo 3, "Data Loading and Synchronization" de *Sun Identity Manager Deployment Guide*.

TABLA 7–1 Tareas con herramientas de sincronización de datos

Para	Elija esta función
Extraer inicialmente cuentas de recursos en Identity Manager sin verlas antes de cargarlas.	Cargar desde recurso
Extraer inicialmente cuentas de recursos en Identity Manager con la posibilidad de ver y editar los datos antes de cargarlas.	Extraer a archivo, Cargar desde archivo
Extraer periódicamente cuentas de recursos en Identity Manager realizando acciones en cada cuenta según la directiva configurada.	Reconciliar con recursos
Introducir o *extraer* cambios de cuentas de recursos en Identity Manager.	Sincronización con adaptadores Active Sync (múltiples implementaciones de recursos)

Funciones de descubrimiento de cuentas

Las funciones de descubrimiento de cuentas de Identity Manager facilitan la implementación rápida y aceleran las tareas de creación de cuentas.

Estas funciones son:

- **Extraer a archivo**. Extrae a un archivo (en formato CSV o XML) las cuentas de recursos devueltas por un adaptador de recursos. Este archivo se puede manipular antes de importar los datos a Identity Manager.
- **Cargar desde archivo**. Lee las cuentas en un archivo (en formato CSV o XML) y las carga en Identity Manager.
- **Cargar desde recurso**. Combina las otras dos funciones de descubrimiento; extrae las cuentas de un recurso y las carga directamente en Identity Manager.

Estas herramientas le permiten crear nuevos usuarios de Identity Manager o correlacionar cuentas de un recurso con cuentas de usuario de Identity Manager existentes.

Nota – En esta sección se explica el uso de las funciones de descubrimiento de Identity Manager. Para obtener información detallada sobre la carga y la sincronización de datos, consulte el Capítulo 3, "Data Loading and Synchronization" de *Sun Identity Manager Deployment Guide*.

Extraer a archivo

Use esta función para extraer cuentas de recursos desde un recurso a un archivo de texto CSV o XML. Ello le permite ver y modificar los datos extraídos antes de importarlos a Identity Manager.

▼ Para extraer cuentas

1. **En la barra de menús, seleccione Cuentas y después Extraer a archivo.**
2. **Seleccione un recurso desde el que desee extraer las cuentas.**
3. **Seleccione un formato de archivo para la presentación de información de cuenta. Puede extraer datos a un archivo XML o a un archivo de texto con atributos de cuenta con un formato de valores separados por comas (CSV).**
4. **Haga clic en Descargar. Identity Manager muestra un cuadro de diálogo de descarga de archivos donde puede guardar o ver el archivo extraído.**

   Si decide abrir el archivo, quizá tenga que seleccionar un programa para verlo.

Cargar desde archivo

Use esta función para cargar en Identity Manager cuentas de recursos extraídas desde un recurso a través de Identity Manager o desde otro archivo de recursos. Los archivos generados con la función Extraer a archivo de Identity Manager tienen formato XML. Al cargar una lista de nuevos usuarios, el archivo de datos suele tener formato CSV.

Acerca del formato de archivo CSV

Es frecuente que las cuentas que se van a cargar aparezcan en una hoja de cálculo y se guarden en un formato de valores separados por comas (CSV) para cargarlas en Identity Manager.

El contenido del archivo CSV debe respetar estas pautas:

- **Línea 1**. Muestra los encabezados de columna o los atributos de esquema de cada campo, separados por comas.
- **Línea y sucesivas**. Enumeran los valores de cada atributo definido en la línea 1, separados por comas. Si no hay datos para un valor de campo, ese campo debe representarse con comas adyacentes.

  Por ejemplo, las tres primeras líneas de un archivo CVS podrían ser análogas a las entradas de este ejemplo:

  ```
  firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Phone
  John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
  Jane,B,Doe,E1111,E1111,1111,,555-222-4444
  ```

  En este ejemplo, la segunda usuaria, Jane Doe, carece de departamento. El valor que falta aparece representado con comas adyacentes (,,).

▼ Para cargar cuentas

1 **En la interfaz de administración, seleccione Cuentas en el menú y después Cargar desde archivo.**

Identity Manager muestra la página Cargar cuentas desde archivo.

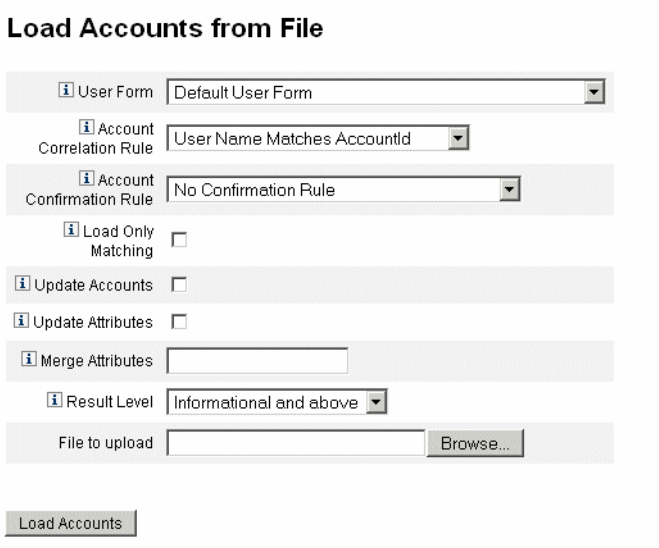


FIGURA 7–1 Cargar desde archivo

2 **Utilice esta página para especificar las opciones de carga de cuentas adecuadas.**

Las opciones incluyen:

- **Formulario de usuario**. Cuando la carga crea un usuario, el formulario de usuario asigna una organización, así como roles, recursos y otros atributos. Seleccione el formulario de usuario que se deba aplicar a cada cuenta de recursos.
- **Regla de correlación de cuentas**. Una regla de correlación de cuentas selecciona los usuarios que pueden poseer las cuentas de recursos sin propietario. Una vez especificados los atributos de una cuenta de recursos sin propietario, la regla de correlación devolverá una lista de nombres o una lista de condiciones de atributo que se utilizará para seleccionar posibles propietarios. Seleccione una regla para buscar usuarios de Identity Manager que puedan ser propietarios de recursos que no sean propiedad de nadie.
- **Regla de confirmación de cuenta**. Una regla de confirmación de cuenta elimina a cualquier usuario que no sea propietario de la lista de propietarios en potencia que selecciona la regla de correlación. Si se proporciona una vista completa del usuario de Identity Manager y de los atributos de una cuenta de recursos que no sea propiedad de nadie, una regla de confirmación devuelve el valor 'true' si el usuario es propietario de la cuenta y 'false' si no lo

es. Seleccione una regla para probar cada propietario en potencia de una cuenta de recursos. Si selecciona Ninguna regla de confirmación, Identity Manager aceptará todos los propietarios potenciales sin necesidad de confirmación.

Nota – Si en el entorno la regla de correlación va a seleccionar como máximo un propietario, no será necesario establecer ninguna regla de confirmación.

- **Cargar sólo coincidencias**. Seleccione esta opción para cargar en Identity Manager sólo aquellas cuentas que coincidan con un usuario existente de Identity Manager. Si esta opción está seleccionada, la carga descartará todas las cuentas de recursos que no tengan coincidencias.
- **Actualizar atributos**. Seleccione esta opción para sustituir los valores de atributos del usuario actual de Identity Manager por los valores de atributos procedentes de la cuenta que se está cargando.
- **Atributos de combinación**. Introduzca uno o más nombres de atributo, separados por comas, para los cuales los valores deberán combinarse (eliminando duplicados) en lugar de ser sobrescritos. Utilice esta opción sólo para atributos tipo lista, tales como grupos y listas de correo. También debe seleccionar la opción Actualizar atributos.
- **Nivel de resultado**. Seleccione un umbral en el que el proceso de carga registrará un resultado concreto para una cuenta:
  - **Errores solamente**. Registre un resultado individual sólo cuando el proceso de carga de la cuenta genere un mensaje de error.
  - **Advertencias y errores**. Registre un resultado concreto cuando el proceso de carga de la cuenta genere un mensaje de error o de advertencia.
  - **De carácter informativo y más**. Registre un resultado concreto para cada cuenta. Esto hace que el proceso de carga se ejecute más lentamente.

3 En el campo Archivo para cargar, especifique un archivo para cargarlo y después elija Cargar cuentas.

Nota –

- Si el archivo de entrada no contiene ninguna columna de usuario, debe seleccionar una regla de confirmación para que la carga se realice correctamente.
- El nombre de instancia de tarea asociado al proceso de carga se basa en el nombre del archivo de entrada; en consecuencia, si vuelve a utilizar un nombre de archivo, la instancia de tarea asociada al último proceso de carga sobrescribirá las instancias de las tareas anteriores.

  En "Acerca del formato de archivo CSV" en la página 251 se describen los campos y opciones disponibles en la pantalla Cargar desde archivo.

Si una cuenta coincide (o está correlacionada) con usuario existente, el proceso de carga combinará la cuenta con el usuario. El proceso creará también un nuevo usuario de Identity Manager a partir de cualquier cuenta de entrada no correlacionada (salvo que se especifique Correlación requerida).

La variable de configuración `bulkAction.maxParseErrors` establece un límite sobre el número de errores que puede haber al cargar un archivo. El límite predeterminado es 10 errores. Si se encuentra el número de errores indicado en `maxParseErrors`,, se detiene el análisis.

Cargar desde recurso

Use esta función para extraer e importar cuentas directamente a Identity Manager con arreglo a las opciones de carga que especifique.

▼ Para importar cuentas

1 **En la interfaz de administración, seleccione Cuentas en el menú y después Cargar desde recurso.**

Aparece la página "Cargar cuentas del recurso".

2 **Especifique las opciones de carga en la página "Cargar cuentas del recurso".**

Las opciones de carga de esta página son iguales a las de la página "Cargar desde archivo" (consulte "Cargar desde archivo" en la página 251).

Reconciliación de cuentas

Use la función de reconciliación para comparar periódicamente cuentas de recursos en Identity Manager con las cuentas que realmente hay en los recursos. La reconciliación correlaciona los datos de cuenta y resalta las diferencias.

Nota – En esta sección se explica cómo realizar tareas de reconciliación con la interfaz de administración. Para obtener información detallada sobre la reconciliación, consulte el Capítulo 3, "Data Loading and Synchronization" de *Sun Identity Manager Deployment Guide*.

Nociones sobre reconciliación

Como la reconciliación está concebida para comparaciones continuas, sus características son:

- Realiza un diagnóstico más específico de la situación de las cuentas y admite un abanico de respuestas más amplio que el proceso de descubrimiento.
- Se puede programar (el descubrimiento no).
- Ofrece un modo incremental (el descubrimiento siempre se efectúa en modo completo).
- Puede detectar cambios nativos (el descubrimiento no).

También es posible configurar la reconciliación para iniciar un flujo de trabajo arbitrario en cada uno de los siguientes puntos del procesamiento de un recurso:

- Antes de reconciliar una cuenta
- Con cada cuenta
- Tras reconciliar todas las cuentas

Se accede a las funciones de reconciliación de Identity Manager desde el área Recursos. La lista Recursos indica cuándo se reconcilió por última vez cada recurso y su estado de reconciliación actual.

Nota – De la reconciliación se encarga el componente reconciliador de Identity Manager. Los valores de configuración del reconciliador se explican en .

Acerca de las directivas de reconciliación

Las directivas de reconciliación le permiten establecer un conjunto de respuestas, por recurso, para cada una de las tareas de reconciliación. En una directiva, puede seleccionar el servidor que ejecutará la reconciliación, determinar cuándo se debe realizar la reconciliación y con qué frecuencia, y definir respuestas para cada situación que se presente durante la reconciliación. También puede configurar la reconciliación para que detecte los cambios realizados de forma nativa (no a través de Identity Manager) en los atributos de cuenta.

Edición de directivas de reconciliación

▼ Para editar una directiva de reconciliación

1 **En la interfaz de administración, seleccione Recursos en el menú.**

2 **Seleccione un recurso de la lista Recursos.**

3 **En la lista Acciones de recurso, elija Editar directiva de reconciliación.**

Identity Manager muestra la página Editar directiva de reconciliación, donde puede seleccionar las siguientes opciones para la directiva:

- **Servidores de reconciliación**. En un entorno de clúster, cada servidor puede ejecutar la reconciliación. Especifique qué servidor de Identity Manager ejecutará la reconciliación con respecto a los recursos de la directiva.
- **Modos de reconciliación**. La reconciliación se puede llevar a cabo en distintos modos, lo que optimiza las diferentes cualidades.
  - **Reconciliación completa**. Optimiza la exactitud del proceso en detrimento de la velocidad.
  - **Reconciliación incremental**. Optimiza la velocidad en detrimento de la exactitud del proceso.

    Seleccione el modo en el que Identity Manager debe ejecutar la reconciliación con respecto a los recursos de la directiva. Seleccione No reconciliar para inhabilitar la reconciliación para los recursos de destino.
- **Programa de reconciliación completa**. Si se habilita el modo de reconciliación completa, la misma se efectuará automáticamente según una programación fija. Especifique cuán frecuentemente deberá ejecutarse la reconciliación completa frente a los recursos de la directiva.
  - Seleccione la opción Heredar directiva predeterminada para heredar la programación indicada desde una directiva de nivel superior.
  - Desactive la opción Heredar directiva predeterminada para especificar un programa. Use los campos suministrados establecer un programa recurrente, o una regla de repetición de programación de tareas para personalizar el programa de reconciliación. Encontrará información para crear una regla de repetición de programación de tarea en "Uso de reglas de repetición de programación de tareas" en la página 264.
- **Programa de reconciliación incremental**. Si se habilita el modo de reconciliación incremental, la misma se efectuará automáticamente según una programación fija.
  - Seleccione la opción Heredar directiva predeterminada para heredar la programación desde una directiva de nivel superior.

- Desactive la opción Heredar directiva predeterminada para especificar un programa. Use los campos suministrados establecer un programa recurrente, o una regla de repetición de programación de tareas para personalizar el programa de reconciliación. Encontrará información para crear una regla de repetición de programación de tarea en "Uso de reglas de repetición de programación de tareas" en la página 264.

Nota – No todos los recursos admiten reconciliación incremental.

- **Reconciliación a nivel de atributos**. Es posible configurar la reconciliación para que detecte los cambios realizados de forma nativa (no a través de Identity Manager) en los atributos de cuenta. Especifique si desea que la reconciliación detecte los cambios nativos realizados en los atributos especificados en Atributos reconciliados de cuenta.
- **Regla de correlación de cuentas**. Una regla de correlación de cuentas selecciona los usuarios que pueden poseer las cuentas de recursos sin propietario. Una vez especificados los atributos de una cuenta de recursos sin propietario, la regla de correlación devolverá una lista de nombres o una lista de condiciones de atributo que se utilizará para seleccionar posibles propietarios. Seleccione una regla para buscar usuarios de Identity Manager que puedan ser propietarios de recursos que no sean propiedad de nadie.
- **Regla de confirmación de cuenta**. Una regla de confirmación de cuenta elimina a cualquier usuario que no sea propietario de la lista de propietarios en potencia que selecciona la regla de correlación. Si se proporciona una vista completa del usuario de Identity Manager y de los atributos de una cuenta de recursos que no sea propiedad de nadie, una regla de confirmación devuelve el valor 'true' si el usuario es propietario de la cuenta y 'false' si no lo es. Seleccione una regla para probar cada propietario en potencia de una cuenta de recursos. Si selecciona Ninguna regla de confirmación, Identity Manager aceptará todos los propietarios potenciales sin necesidad de confirmación.

Nota – Si en el entorno la regla de correlación va a seleccionar como máximo un propietario, no será necesario establecer ninguna regla de confirmación.

- **Administrador de proxy**. Especifique el administrador que utilizar cuando se lleven a cabo respuestas de reconciliación. La reconciliación sólo puede realizar aquellas acciones que le estén permitidas al administrador de proxy designado. La respuesta utilizará el formulario de usuario (si fuese necesario) asociado con este administrador.

  También puede seleccionar la opción No existe administrador del proxy. Cuando está seleccionada esta opción, pueden verse los resultados de la reconciliación pero no se ejecuta ninguna medida de respuesta o flujo de trabajo.
- **Opciones de situación** (y respuesta) La reconciliación reconoce diversos tipos de situaciones, que se describen a continuación. Especifique en la columna Respuesta cualquier acción que deba efectuar la reconciliación.

- **CONFIRMADO**. La cuenta esperada existe.

  Para que se marque como CONFIRMADO, debe cumplirse lo siguiente:

  - Identity Manager espera que la cuenta exista.
  - La cuenta existe en el recurso.

- **COLISIÓN**. Dos o más usuarios de Identity Manager tienen asignada la misma cuenta en un recurso.
- **ELIMINADO**. La cuenta esperada no existe.

  Para que se marque como ELIMINADO, debe cumplirse lo siguiente:

  - Identity Manager espera que la cuenta exista.
  - La cuenta no existe en el recurso.

- **ENCONTRADO**. El proceso de reconciliación ha encontrado una cuenta coincidente en un recurso asignado.

  Para que se marque como ENCONTRADO, debe cumplirse lo siguiente:

  - Identity Manager espera que la cuenta pueda o no existir. (Una cuenta puede existir o no en un recurso si éste se ha asignado al usuario, pero aún no se ha abastecido.)
  - La cuenta existe en el recurso.

- **FALTA**. No existe ninguna cuenta coincidente en un recurso asignado al usuario.

  Para que se marque como FALTA, debe cumplirse lo siguiente:

  - Identity Manager espera que la cuenta pueda o no existir. (Una cuenta puede existir o no en un recurso si éste se ha asignado al usuario, pero aún no se ha abastecido.)
  - La cuenta no existe en el recurso.

- **SIN ASIGNAR**. El proceso de reconciliación ha encontrado una cuenta coincidente en un recurso no asignado al usuario.

  Para que se marque como SIN ASIGNAR, debe cumplirse lo siguiente:

  - Identity Manager no espera que la cuenta exista. (Identity Manager no espera que una cuenta exista si el recurso no está asignado al usuario.)
  - La cuenta existe en el recurso.

- **SIN COINCIDENCIAS**. La cuenta del recurso no coincide con ningún usuario.
- **EN CONFLICTO**. La cuenta del recurso coincide con más de un usuario.

  Seleccione una de las siguientes opciones de respuesta disponibles, que pueden variar según la situación:

  - **Crear un nuevo usuario de Identity Manager basado en la cuenta de recursos**. Ejecuta el formulario del usuario en los atributos de la cuenta de recursos para crear un nuevo usuario. La cuenta de recurso no se actualiza como resultado de los cambios.

- **Crear cuenta de recursos para el usuario de Identity Manager** Vuelve a crear la cuenta de recurso que falta con el formulario de usuario para generar de nuevo los atributos de cuenta de recurso.
- **Eliminar cuenta de recursos e Inhabilitar cuenta de recursos** Elimina/Inhabilita la cuenta en el recurso.
- **Vincular cuenta de recursos con usuario de Identity Manager y Desvincular cuenta de recursos de usuario de Identity Manager**. Añade o quita la asignación de cuenta de recursos al usuario. No se efectúa ningún procesamiento del formulario.
- **No hacer nada**. Elija esta opción si prefiere que la reconciliación no efectúe ninguna reparación.

  Puede reparar manualmente cualquier situación de cuenta descubierta mediante reconciliación. Seleccione Recursos → Examinar índice de cuenta en el menú. Desde aquí puede examinar la situación registrada para todas las cuentas que se han reconciliado. Haga clic con el botón secundario en una cuenta y aparecerá una lista con las opciones de reparación válidas. Para obtener más información, consulte "Examen del índice de cuenta" en la página 263.

- **Flujo de trabajo de pre-reconciliación**. La reconciliación puede ser configurada para ejecutar un flujo de trabajo especificado por el usuario antes de reconciliar un recurso. Especifique el flujo de trabajo que deberá ejecutar la reconciliación. Seleccione No ejecutar flujo de trabajo si no se debe ejecutar ningún flujo de trabajo.
- **Flujo de trabajo por cuenta**. La reconciliación se puede configurar para ejecutar un flujo de trabajo especificado por el usuario después de responder a la situación de una cuenta de recursos. Especifique el flujo de trabajo que deberá ejecutar la reconciliación. Seleccione No ejecutar flujo de trabajo si no se debe ejecutar ningún flujo de trabajo.
- **Flujo de trabajo de post-reconciliación**. La reconciliación se puede configurar para ejecutar un flujo de trabajo especificado por el usuario tras completar la reconciliación de un recurso. Especifique el flujo de trabajo que deberá ejecutar la reconciliación. Seleccione **No ejecutar flujo de trabajo** si no se debe ejecutar ningún flujo de trabajo.
- **Explicar la situación**. Si se habilita, la reconciliación registrará información adicional sobre cómo se clasifican las situaciones de cuentas. Esta opción está inhabilitada de forma predeterminada. El registro de las explicaciones puede hacer que el proceso de reconciliación tarde más tiempo en completarse.
- **Límite de errores**. Si está habilitada esta opción, la reconciliación terminará automáticamente cuando se haya producido el número de errores especificado durante el procesamiento. Un valor de 0 indica que no hay límite de errores. Desactive la opción Heredar directiva predeterminada para ver el campo Máximo de errores permitidos y escribir un valor.
- **Número máximo de cuentas suprimidas nativamente**. Esta opción actúa como protección, porque evalúa el número de cuentas que faltan en el recurso y, si se supera un umbral, impide que el reconciliador desvincule las cuentas.

Para habilitar esta función, desactive la casilla Heredar directiva predeterminada e introduzca un porcentaje en el campo Número máximo de cuentas suprimidas nativamente. El umbral debe configurarse con un porcentaje completo situado entre 0 y 100 (el 0 desactiva la función).

Si el porcentaje de cuentas eliminadas supera el umbral, la reconciliación continúa todo el procesamiento no relacionado con las cuentas que faltan y termina con un error.

Haga clic en Guardar para guardar los cambios de directiva.

Inicio de la reconciliación

A continuación se describen dos opciones para iniciar tareas de reconciliación.

- Reconciliación a intervalos programados
- Reconciliación inmediata

▼ Para ejecutar la reconciliación a intervalos regulares

1. **Abra la página Editar directiva de reconciliación como se explica en "Edición de directivas de reconciliación" en la página 256.**

2. **Especifique los parámetros de programación de la reconciliación.**

   La reconciliación se ejecutará en función de los parámetros definidos en la directiva.

▼ Para ejecutar la reconciliación inmediatamente

1. **En la interfaz de administración, seleccione Recursos en el menú.**

2. **Seleccione un recurso de la lista Recursos.**

3. **Elija una opción en la lista Acciones de recurso.**

   Las opciones incluyen:

   - Reconciliación completa ahora
   - Reconciliación incremental ahora

     La reconciliación se ejecutará en función de los parámetros definidos en la directiva. Si la directiva incluye un programa definido para tareas de reconciliación a intervalos regulares, se seguirá ejecutando tal y como se especificó.

▼ Para cancelar la reconciliación

1. **En la interfaz de administración, seleccione Recursos en el menú.**
2. **Elija en la Lista de recursos el recurso cuya reconciliación desea cancelar.**
3. **Busque la lista Acciones de recurso y elija Cancelar la reconciliación.**

Visualización del estado de la reconciliación

Hay dos formas principales de ver el estado de la reconciliación. Para ver el estado detallado de la reconciliación, abra la página Resultados de resumen de reconciliación para un recurso determinado. La Lista de recursos también ofrece directamente el estado resumido de la reconciliación.

▼ Para ver el estado de la reconciliación

El estado detallado de la reconciliación aparece en la página Resultados de resumen de reconciliación.

1. **En la interfaz de administración, seleccione Recursos en el menú.**
2. **Elija en la Lista de recursos el recurso cuyo estado de reconciliación desea ver.**
3. **Busque la lista Acciones de recurso y elija Ver estado de la reconciliación.**

   Aparece la página Resultados de resumen de reconciliación para el recurso.

▼ Para ver el estado de la reconciliación en la Lista Recursos

También puede ver el estado de la reconciliación en la Lista Recursos.

1. **Abra la interfaz de administración.**
2. **Seleccione Recursos en el menú principal.**

   La columna **Estado** indica las siguientes condiciones de estado de la reconciliación:

   - **desconocido**. No se conoce el estado. Los resultados de la tarea de reconciliación más reciente no están disponibles.
   - **inhabilitado**. La reconciliación está inhabilitada.
   - **fallida**. La última reconciliación no se ha podido completar.
   - **satisfactorio**. La última reconciliación se ha completado satisfactoriamente.
   - **completado con errores**. La última reconciliación se ha completado, pero con errores.

Nota – Para ver los cambios del estado debe actualizar esta página. (La información no se actualiza automáticamente.)

Uso del índice de cuenta

El índice de cuenta registra el último estado conocido para cada cuenta de recurso reconocida por Identity Manager. Se mantiene sobre todo mediante reconciliación, pero otras funciones de Identity Manager también lo actualizan conforme es preciso.

Las herramientas de descubrimiento no actualizan el índice de cuenta.

▼ Para buscar el índice de cuenta

Busque el índice de cuenta para ver el último estado conocido de una cuenta de recurso determinada.

1. **En la interfaz de administración, seleccione Recursos en el menú.**
2. **Elija en la Lista de recursos el recurso cuyo índice de cuenta desea buscar.**
3. **Busque la lista Acciones de recurso y elija Buscar índice de cuenta.**

   Aparece la página Buscar índice de cuenta.
4. **Seleccione un tipo de búsqueda y, a continuación, escriba o seleccione los atributos de búsqueda.**
   - **Nombre de cuenta de recursos**. Seleccione esta opción, elija un modificador ("comienza por", "contiene" o "es") y, a continuación, introduzca el nombre completo de una cuenta o sólo una parte.
   - **El recurso es uno de**. Seleccione esta opción y, a continuación, seleccione uno o varios recursos de la lista para encontrar las cuentas reconciliadas que residen en los recursos especificados.
   - **Propietario**. Seleccione esta opción, elija un modificador ("comienza por", "contiene" o "es") y, a continuación, introduzca el nombre completo de un propietario o sólo una parte. Para buscar cuentas sin propietario, busque cuentas que estén en la situación SIN ASIGNAR o EN TRÁMITE.
   - **La situación es una de**. Seleccione esta opción y, a continuación, seleccione una o varias situaciones de la lista para encontrar las cuentas reconciliadas en las situaciones especificadas.

5 **Haga clic en Buscar para buscar cuentas que se ajusten a los parámetros de la búsqueda. Para limitar los resultados de la búsqueda puede especificar un número en el primer campo "Limitar resultados a". Por defecto, los resultados se limitan a las 1.000 primeras cuentas encontradas.**

Haga clic en Reinicializar consulta para borrar la página y realizar nuevas selecciones.

Examen del índice de cuenta

También es posible ver todas las cuentas de usuario de Identity Manager, con la posibilidad de reconciliarlas por usuario.

▼ Para examinar el índice de cuenta

1 **En la interfaz de administración, seleccione Recursos en el menú.**

2 **Elija Examinar índice de cuenta en el menú secundario.**

Aparece la página Examinar índice de cuenta.

La tabla muestra todas las cuentas de recursos que conoce Identity Manager (pertenezcan o no a usuarios de Identity Manager). Esta información se agrupa por recurso o por organización de Identity Manager. Para cambiar esta vista, elija una opción en la lista Modificar vista del índice.

Operaciones con cuentas

Para trabajar con las cuentas de un recurso, seleccione la vista del índice Agrupar por recursos. Identity Manager muestra carpetas para cada tipo de recurso. Para ir a un recurso concreto, expanda su carpeta. Haga clic en + o - junto al recurso para ver todas las cuentas de recursos que conoce Identity Manager.

No aparecerán las cuentas que se hayan añadido directamente al recurso después de la última reconciliación con él.

Es posible realizar diversas acciones según la situación actual de la cuenta. Haga clic con el botón secundario en una cuenta y aparecerá una lista con las opciones de reparación válidas. También se pueden ver los detalles de la cuenta o elegir reconciliarla individualmente.

Operaciones con usuarios

Para trabajar con usuarios de Identity Manager , seleccione la vista del índice Agrupar por usuarios. En esta vista, los usuarios y las organizaciones de Identity Manager aparecen con una jerarquía similar a la de la página Lista de cuentas. Para ver las cuentas asignadas actualmente a un usuario en Identity Manager, vaya hasta él y haga clic en el indicador adjunto a su nombre. Bajo el nombre del usuario aparecen sus cuentas y el estado actual de las que conoce Identity Manager.

Es posible realizar diversas acciones según la situación actual de la cuenta. También se pueden ver los detalles de la cuenta o elegir reconciliarla individualmente.

Uso de reglas de repetición de programación de tareas

Las reglas de repetición de programación de tareas sirven para ajustar las programaciones de tareas. Por ejemplo, si quiere que las reconciliaciones previstas para el sábado se retrasen hasta el lunes siguiente, aplique una regla de repetición de programación de tareas.

Las reglas de repetición de programación de tareas permiten ajustar la programación tanto de reconciliaciones completas como incrementales.

Encontrará información para seleccionar reglas de repetición de programación de tareas en "Edición de directivas de reconciliación" en la página 256.

Cómo se programan los horarios de reconciliación

Al terminar un trabajo de reconciliación, el componente reconciliador comprueba cuál es su próxima hora de ejecución programada.

Primero la obtiene de la programación predeterminada. Después ejecuta todas las reglas de repetición de programación de tareas aplicables para comprobar si hay que ajustar la programación. Si es preciso ajustar la programación, la programación de las reglas sustituye a la predeterminada para esa reconciliación.

Nota – Las reglas de repetición de programación de tareas no pueden sustituir a la programación predeterminad. Sólo sustituyen las horas de inicio previstas para trabajos concretos.

▼ Para ver la regla de ejemplo Acepta todas las fechas

A continuación se describe la regla de ejemplo interna Acepta todas las fechas.

1. **En un editor de texto, abra el archivo** `ReconRules.xml`**, que se halla en el directorio** `sample` **de Identity Manager.**

2. **Busque la regla** `SCHEDULING_RULE_ACCEPT_ALL_DATES`**.**

   Para que una regla se incluya en la lista del menú desplegable Regla de repetición de TaskSchedule (en la página Editar directiva de reconciliación), el atributo `subtype` de dicha regla debe configurarse en `SUBTYPE_TASKSCHEDULE_REPETITION_RULE:`

   ```
   <Rule subtype='SUBTYPE_TASKSCHEDULE_REPETITION_RULE'
   name='SCHEDULING_RULE_ACCEPT_ALL_DATES'>
   ```

   Como hemos mencionado antes, las reglas de repetición de programación de tareas pueden modificar la programación de reconciliación predeterminada.

La variable `calculatedNextDate` puede aceptar la siguiente fecha, que se calcula de la manera predeterminada, o devolver otra fecha. Como especifica la regla de ejemplo, `calculatedNextDate` acepta incondicionalmente la fecha predeterminada, lo que se aprecia en este extracto:

```
<RuleArgument name='calculatedNextDate'/>
<block>
  <ref>calculatedNextDate</ref>
</block>
```

Para crear una programación personalizada, sustituya la lógica de la regla entre los elementos `<block>`. Por ejemplo, para cambiar la hora de inicio de la reconciliación a las 10:00 AM del sábado, incluya esta secuencia JavaScript entre los elementos `<block>`:

```
<block>
  <script>
     var calculatedNextDate = env.get('calculatedNextDate');

    // Test to see if this task is scheduled for a Saturday
    // (Note that 6 is used to denote Saturday in JavaScript)
    if(calculatedNextDate.getDay() == 6) {
      // If so, set the time to 10:00:00
      calculatedNextDate.setHours(10);
      calculatedNextDate.setMinutes(0);
      calculatedNextDate.setSeconds(0);
    }
    // Return the modified date
    calculatedNextDate;
  </script>
</block>
```

En "Para ver la regla de ejemplo Acepta todas las fechas" en la página 264, `calculatedNextDate` se define inicialmente en la hora de programación predeterminada. Si la siguiente fecha de ejecución programada es un sábado, la regla programa la reconciliación para que empiece a las 10:00. Si la siguiente fecha de ejecución programada no es un sábado, "Para ver la regla de ejemplo Acepta todas las fechas" en la página 264 devuelve `calculatedNextDate` sin realizar ningún cambio y se utiliza la programación predeterminada.

Para obtener más información sobre la creación de reglas personalizadas para usarlas en Identity Manager, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.

Adaptadores Active Sync

La función Activar sincronización de Identity Manager permite sincronizar con los datos de usuario de Identity Manager la información almacenada en un *recurso autorizador externo* (como una aplicación o base de datos). Si se configura la sincronización con un recurso de Identity Manager, éste puede *recibir* o sondear los cambios en el recurso autorizador.

Para configurar como afluyen los cambios de atributos de recursos a Identity Manager, especifique el Formulario de entrada en la directiva de sincronización del recurso (para el tipo de objeto de destino adecuado).

Nota – En este capítulo se explica cómo realizar tareas de activación de la sincronización con la interfaz de administración. Para obtener información detallada sobre la activación de la sincronización, consulte el Capítulo 3, "Data Loading and Synchronization" de *Sun Identity Manager Deployment Guide*.

Configuración de la sincronización

Identity Manager emplea una directiva de sincronización para habilitar la sincronización de los recursos.

▼ Para editar o configurar la sincronización

Cada recurso tiene su propia directiva de sincronización. Siga estos pasos para configurar o editar una directiva de sincronización:

1. **En la interfaz de administración, seleccione Recursos en el menú.**
2. **Elija en la Lista de recursos el recurso para el que desea configurar la sincronización.**
3. **Busque la lista Acciones de recurso y elija Editar directiva de sincronización.**

   Aparece la página Editar directiva de sincronización para el recurso.

   En la página Editar directiva de sincronización, especifique las opciones siguientes para configurar la sincronización:

   - **Tipo de objeto destino**. Seleccione el tipo de usuarios a los que se aplica la directiva, ya sean usuarios de Identity Manager o de un proveedor de servicios.

Nota – En una implementación de Service Provider, debe configurar una directiva de sincronización (especificando el tipo de objeto Usuarios de Service Provider) para habilitar la sincronización de los datos para esos usuarios. Para obtener más información sobre los usuarios de proveedor de servicios, consulte el Capítulo 17, "Administración de Service Provider".

- **Configuración de la programación**. En esta sección se especifica el método de inicio y la programación del sondeo.

  Puede especificar los siguientes tipos de inicio:

  - **Automático con conmutación por errores**. Inicia el origen obligatorio al iniciar Identity System (Sistema de identidad).
  - **Manual**. Es necesario que un administrador inicie el origen obligatorio.
  - **Inhabilitado**. Inhabilita el recurso.

    Use las opciones Fecha de inicio y Hora de inicio para indicar cuándo comienza el sondeo. Para especificar los ciclos de sondeo, seleccione un intervalo e introduzca un valor para el intervalo (segundos, minutos, horas, días, semanas, meses).

    Nota – Si cambia el método de inicio o la programación del sondeo, ha de reiniciar el servidor para que los cambios surtan efecto.

    Si establece la fecha y hora de inicio del sondeo para un momento futuro, se iniciará cuando se haya especificado. Si por el contrario establece la fecha y hora de inicio del sondeo para un momento pasado, Identity Manager determinará cuándo se inicia el sondeo en función de esta información y del intervalo de sondeo.

    Por ejemplo:

    - Supongamos que configura la sincronización activa del recurso para que se realice el 18 de julio de 2005 (martes).
    - Por otro lado, establece que el sondeo se realice semanalmente con fecha de inicio el 4 de julio de 2005 (lunes) a las 9:00 a.m.

  En este caso, el recurso comenzará el sondeo el 25 de julio de 2005 (el lunes siguiente).

  Si no especifica una fecha ni una hora de inicio, el recurso comenzará a realizar el sondeo inmediatamente. Si adopta este enfoque, cada vez que se reinicie el servidor de aplicaciones, todos los recursos configurados para la sincronización activa comenzarán el sondeo de inmediato. Lo habitual es configurar una fecha y hora de inicio.

- **Servidores de sincronización**. En un entorno de clúster, cada servidor puede ejecutar la sincronización. Elija una opción para especificar los servidores que se utilizarán para ejecutar la sincronización del recurso.

- Seleccione Usar cualquier servidor disponible si no importa donde debería ejecutarse la reconciliación. Se elegirá un servidor entre los posibles cuando se inicie la sincronización.
- Seleccione Use los valores de `waveset.properties` para ejecutar la sincronización con los servidores que especifica dicho archivo. (Esta función está desaprobada.)
- Seleccione Usar servidores especificados y después elija uno o varios servidores disponibles en la lista Servidores de sincronización para seleccionar servidores concretos donde ejecutar la sincronización.

- **Configuración específica de los recursos**. En esta sección se especifica cómo la sincronización debe determinar los datos que se procesan para el recurso.
- **Configuración común**. Indique los valores de configuración comunes para las actividades de sincronización de datos.

  Estos valores incluyen:

  - **Administrador de proxy**. Seleccione el administrador que procesará las actualizaciones. Todas las acciones se autorizarán en función de las capacidades asignadas a este administrador. Debe seleccionar un administrador de proxies con un formulario de usuario vacío.
  - **Formulario de entrada**. Seleccione el formulario de entrada que procesará las actualizaciones de datos. Este elemento opcional de configuración permite que los atributos sean transformados antes de ser guardados en las cuentas.
  - **Reglas** (*opcional*). Seleccione las reglas que deben aplicarse durante el proceso de sincronización de datos.

    Puede especificar lo siguiente:

    - **Regla de proceso**. Seleccione esta regla para especificar la ejecución de una regla de proceso para cada cuenta entrante. Esta selección anula todas las demás opciones. Si especifica una regla de proceso, el proceso se ejecutará para cada fila, independientemente de cualquier otro ajuste de este recurso. Puede ser un nombre de proceso o una regla que evalúe un nombre de proceso.
    - **Regla de correlación**. Seleccione una regla de correlación que anule la regla de correlación especificada en la directiva de reconciliación del recurso. Las reglas de correlación correlacionan las cuentas de recursos con las cuentas de Identity System.
    - **Regla de confirmación**. Seleccione una regla de confirmación que anule la regla de correlación especificada en la directiva de confirmación del recurso.
    - **Regla de resolución de procesos**. Seleccione esta regla para especificar el nombre de la definición de tarea que se debe ejecutar cuando haya varias coincidencias para un registro en el suministro. Debe ser un proceso que solicite al administrador que realice una acción manual. Puede ser un nombre de proceso o una regla que evalúe un nombre de proceso.

- **Regla de eliminación**. Seleccione una regla que devuelva el valor "True" (Verdadero) o "False" (Falso) que se evaluará para cada usuario entrante con objeto de determinar si se debe producir una operación de eliminación.

- **Crear cuentas sin asignar**. Cuando esta opción se encuentra habilitada (true), el adaptador intenta crear las cuentas que no encuentra en el sistema Identity Manager. Si está habilitada, el adaptador ejecutará la cuenta durante el proceso devuelto por la regla de resolución de procesos.
- **Configuración de registro**. Especifique un valor para las opciones de registro.

  Las opciones de registro son:

  - **Número máximo de archivos de registro**. Si es mayor que cero, se conserva el último número `N` de archivos de registro. Si es cero, se vuelve a utilizar siempre el mismo archivo de registro. Si es `-1`, nunca se descartan los archivos de registro.
  - **Edad máxima del registro activo**. Después de que haya transcurrido este periodo de tiempo, el registro activo se archivará. Si se establece en 0, no se realizará ninguna operación de archivado basada en tiempo. Si el valor de "Número máximo de archivos de registro" es cero, se trunca el registro activo y se vuelve a utilizar una vez transcurrido este periodo de tiempo. Este criterio de edad se evalúa independientemente del criterio de tiempo especificado en la opción de tamaño máximo de archivo de registro.

    Introduzca un número y, a continuación, seleccione una unidad de tiempo (días, horas, minutos, meses, segundos o semanas). La selección predeterminada está establecida en días.
  - **Ruta de archivo de registro**. Especifique la ruta del directorio en el que se deben crear los archivos de registro activos y archivados. Los nombres de los archivos de registro deben comenzar por el nombre de recurso.
  - **Tamaño máximo del archivo de registro**. Especifique un tamaño máximo en bytes para el archivo de registro activo. El archivo de registro activo se archivará cuando alcance su tamaño máximo. Si el valor de "Número máximo de archivos de registro" es cero, se trunca el registro activo y se vuelve a utilizar una vez transcurrido este periodo de tiempo. Este criterio de tamaño se evalúa independientemente del criterio de edad especificado en la opción de edad máxima del registro activo.
  - **Nivel de registro**. Especifique un nivel de registro.

    Hay disponibles los siguientes niveles de registro:

    - **0**. Sin registro
    - **1**. Error
    - **2**. Información
    - **3**. Detallado
    - **4**. Depurar

4 Haga clic en Guardar para guardar la configuración de la directiva para el recurso.

Edición de Adaptadores Active Sync

Antes de editar un adaptador Active Sync, detenga la sincronización.

▼ Para detener la sincronización

1 **Abra la página Editar directiva de sincronización. (Consulte las instrucciones en "Para editar o configurar la sincronización" en la página 266.)**

2 **Dentro de Configuración de la programación, busque Tipo de inicio y seleccione Inhabilitado.**

Para los usuarios de Service Provider, desactive la opción Habilitar sincronización.

Aparece un mensaje de advertencia para avisar que la sincronización está inhabilitada.

3 **Pulse Guardar.**

Cuando se inhabilita la sincronización de un recurso, se detiene la tarea de sincronización al guardar los cambios.

Ajuste del rendimiento del adaptador Active Sync

Como la sincronización se efectúa en segundo plano, la configuración del adaptador Active Sync puede afectar al rendimiento del servidor.

Para ajustar el rendimiento del adaptador Active Sync se realizan estas tareas:

Los adaptadores Active Sync se gestionan con la lista de recursos. Seleccione un adaptador Active Sync y, a continuación, acceda a las acciones de los controles de inicio, parada y actualización de estado en el área *Sincronización* de la lista Acciones de recurso.

Cambio de los intervalos de sondeo

El intervalo de sondeo determina cuándo el adaptador Active Sync empieza a procesar nuevo información. Los intervalos de sondeo deben basarse en el tipo de actividad realizada. Por ejemplo, si el adaptador lee una lista larga de usuarios en una base de datos y actualiza cada vez todos los usuarios de Identity Manager, le interesa ejecutar este proceso diariamente por la mañana temprano. Algunos adaptadores efectúan una busca rápida de nuevos elementos, lo que permite configurar su ejecución cada minuto.

Especificación del host donde se ejecuta el adaptador

Para especificar el host donde se ejecutarán los adaptadores, debe editar la propiedad `sources.hosts` en el archivo `waveset.properties`.

Especifique uno de estos valores:

- Defina `sources.hosts=`*nombrehost1,nombrehost2,nombrehost3* . Este valor de configuración enumera los nombres de host de las máquinas donde deben ejecutarse los adaptadores Active Sync. El adaptador se ejecutará en el primer host disponible que aparezca en este campo.

  Nota – El *nombrehost* introducido debe coincidir con una entrada de la lista de servidores de Identity Manager. Para ver la lista de servidores, use la ficha Configurar.

- Consulte `sources.hosts=localhost`. Con este valor, el adaptador se ejecutará en el primer servidor de Identity Manager que intente iniciar Active Sync para el recurso.

  Nota – En un clúster hay que utilizar la primera opción cuando es preciso especificar un servidor concreto.

  Este valor de la propiedad sólo se aplica a la sincronización de usuarios de Identity Manager. La configuración de host para sincronizar usuarios de Service Provider la establece la directiva de sincronización.

Los adaptadores Active Sync que requieren más memoria y ciclos de CPU se pueden configurar para ejecutarse en servidores dedicados con el fin de contribuir a equilibrar la carga de los sistemas.

Inicio y detención

Los adaptadores Active Sync se pueden inhabilitar, iniciar a mano o iniciar automáticamente. Para iniciar o detener los adaptadores Active Sync se necesita la capacidad de administrador adecuada para cambiar los recursos de activación de la sincronización. Para obtener información sobre las capacidades de administrador, consulte "Categorías de capacidades" en la página 217.

Si un adaptador se configura para el inicio automático, se reinicia cuando lo hace el servidor de aplicaciones. Cuando se inicia un adaptador, se ejecuta inmediatamente con el intervalo de sondeo especificado. Cuando se detiene un adaptador, se detendrá la próxima vez que verifique la marca de parada.

Registro del adaptador

Los registros de adaptador capturan información sobre el adaptador que está procesándose. El volumen de detalles que captura el registro depende del nivel de registro que se haya configurado. Los registros de adaptador son útiles para depurar problemas y observar el progreso del proceso del adaptador.

Cada adaptador tiene su propio archivo de registro, ruta y nivel de registro. Estos valores se especifican en la sección Registro de la directiva de sincronización para el tipo de usuario apropiado (Identity Manager o Service Provider).

Los registros de adaptador sólo deben eliminarse cuando se haya detenido el adaptador. En la mayoría de los casos, antes de borrar el registro del adaptador conviene realizar una copia para archivarla.

◆ ◆ ◆ CAPÍTULO 8

Informes

Identity Manager informa sobre las actividades automáticas y manuales del sistema. Un potente conjunto de funciones permite capturar y visualizar información de acceso importante sobre los usuarios de Identity Manager en cualquier momento.

En este capítulo conocerá los tipos de informes de Identity Manager, cómo crear, ejecutar y enviar informes por correo electrónico, además de descargar datos sobre ellos.

Este capítulo consta de los temas siguientes:

Uso de informes

En Identity Manager los informes se consideran una categoría de tareas especial. Por eso se trabaja con ellos en dos áreas de la interfaz de administración de Identity Manager:

- **Informes (Ejecutar informes)**. El área Ejecutar informes sirve para definir, ejecutar, eliminar y descargar informes. Sólo los administradores con capacidades suficientes pueden definir, ejecutar, eliminar y descargar informes. Para obtener más información, consulte el Apéndice D, "Definiciones de capacidades".
- **Tareas del servidor**. Tras definir los informes, vaya al área Tareas programadas → Administrar programación para programar y modificar las tareas de informes. Los objetos de definición de tareas (TaskDefinition) deben contener `visibility=schedule` para poder ser programados. Utilice las páginas de depuración para efectuar este cambio. Encontrará más información en "Edición de objetos de configuración de Identity Manager" en la página 118.

Tipos de informe

Los informes se organizan en dos categorías:

- **Informes de Identity Manager**. Son de diversos tipos, incluidos informes en tiempo real, resumen, registro de auditoría, registro del sistema e informes de uso.
- **Informes de Auditor**. Proporcionan información que ayuda a administrar el cumplimiento de los usuarios según los criterios definidos en las directivas de auditoría.

Estas dos categorías contienen a su vez diversos tipos de informe. Los tipos de informes se detallan más adelante en este mismo capítulo. Los informes de Identity Manager se tratan dentro de "Informes de Identity Manager" en la página 280 y los de Auditor en "Informes de Auditor" en la página 288.

Encontrará instrucciones para ver los informes de Identity Manager y de Auditor en "Visualización de informes" en la página 276.

Ejecución de informes

▼ Para ejecutar un informe

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

Aparece la página Ejecutar informes.

2 **Para ver la lista de los informes disponibles en Identity Manager, seleccione Informes de Identity Manager en el menú desplegable Tipo de informe. (Esta opción está seleccionada de forma predeterminada.)**

Para ver la lista de los informes disponibles en Auditor, seleccione Informes de Auditor en el menú desplegable Tipo de informe. Encontrará más información dentro de "Operaciones con Informes de Auditor" en la página 465 en el Capítulo 15, "Auditoría: Cumplimiento de supervisión".

La Figura 8–1 ilustra un ejemplo de la página Ejecutar informes. Los informes de Auditor se seleccionan en el menú desplegable Tipo de informe.

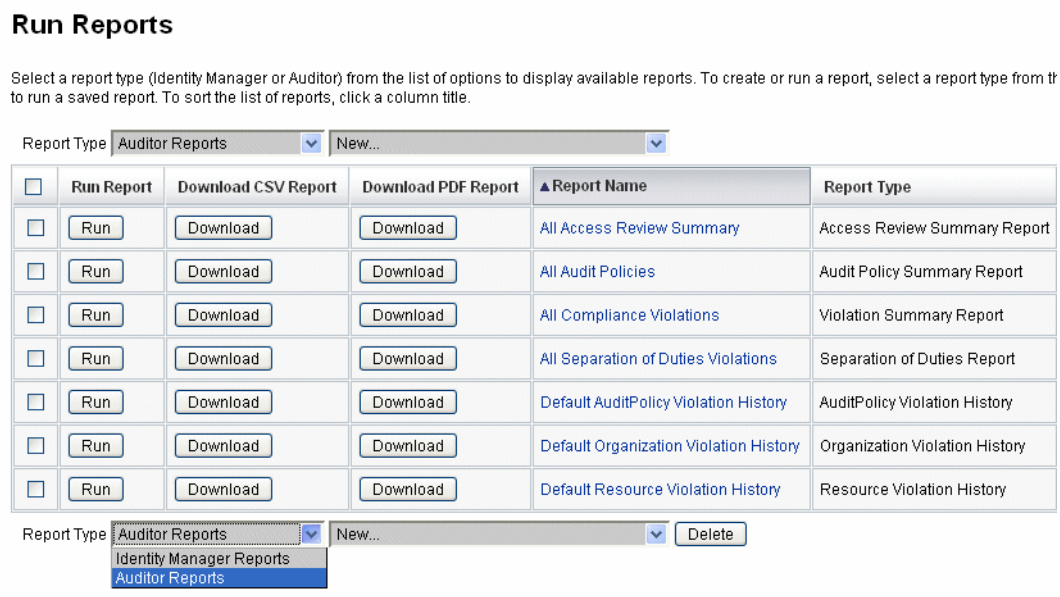


FIGURA 8–1 Selección de Ejecutar informes

3 **Haga clic en Ejecutar para ejecutar un informe.**

Nota – Para poder ejecutar varias instancias simultáneas del mismo informe, edítelo y elija la opción Permitir la ejecución simultánea de informes. Con esta opción habilitada, varios administradores pueden ejecutar el mismo informe a la vez.

Si se ejecutan simultáneamente dos o más instancias del mismo informe, cada informe llevará el ID del administrador seguido de una marca de hora añadida al final del nombre.

Visualización de informes

Tras ejecutar un informe desde la página Ejecutar informes, puede ver la salida de inmediato o más tarde.

▼ Para ver un informe

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

Aparece la página Ejecutar informes.

2 **Haga clic en la ficha Ver informes.**

Aparece la página Ver informes.

3 **Haga clic en un informe para verlo.**

Creación de informes

A continuación se explica cómo crear un informe nuevo de Identity Manager o Identity Auditor sin basarse en otro informe existente.

Nota – Para modificar un informe existente y guardarlo con otro nombre, consulte "Edición y clonación de informes" en la página 277 en la próxima sección.

▼ Para crear un informe nuevo

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

Aparece la página Ejecutar informes.

2 **Seleccione una categoría de informe en el menú desplegable Tipo de informe.**

Hay dos categorías de informes:

- Informes de Identity Manager
- Informes de Auditor

3 **Seleccione el tipo de informe concreto que desea crear en el siguiente menú desplegable (el que indica Nuevo en la parte superior).**

Identity Manager muestra la página Definir un informe, donde se eligen las opciones para crear el informe, ejecutarlo o guardarlo.

Después de escribir y seleccionar el criterio de informe podrá:

- Ejecutar el informe sin guardarlo. Haga clic en Ejecutar para ejecutar el informe. Identity Manager no guarda el informe (si ha definido un nuevo informe) ni los criterios de informe modificados (si ha editado un informe existente).
- Guardar el informe. Haga clic en Guardar para guardar el informe. Tras guardarlo, puede ejecutar el informe desde la página Ejecutar informes (la lista de informes).

Para obtener más información sobre la ejecución de informes, consulte "Ejecución de informes" en la página 274.

Edición y clonación de informes

A continuación se explica cómo modificar o clonar un informe existente y guardarlo con otro nombre.

▼ Para editar o clonar un informe

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

Aparece la página Ejecutar informes.

2 **Seleccione una categoría de informe en el menú desplegable Tipo de informe.**

Hay dos categorías de informes:

- Informes de Identity Manager
- Informes de Auditor

La tabla de informes muestra los informes que hay en la categoría seleccionada.

3 **Haga clic en un informe para editarlo.**

4 **Para editar un informe, ajuste sus parámetros como interese y pulse Guardar.**

Para clonar un informe, introduzca un nombre de informe nuevo. Ajuste los parámetros del informe como interese y pulse Guardar para guardarlo con otro nombre.

Envío de informes por correo electrónico

Cuando cree o edite un informe, puede seleccionar una opción para enviar por correo electrónico el resultado a uno o varios destinatarios. Al seleccionar esta opción, la página se actualiza y solicita las direcciones de los destinatarios. Escriba las direcciones de uno o varios destinatarios separándolas con una coma.

También puede elegir uno de los formatos siguientes para adjuntar el informe por correo electrónico:

- **Adjuntar con formato CSV**. Adjunta los informes con formato de valores separados por comas (CSV).
- **Adjuntar con formato PDF**. Adjunta los informes con formato de documento portátil (PDF).

Programación de informes

Es posible ejecutar de inmediato un informe o programar su ejecución a intervalos regulares mediante una de estas acciones:

- Seleccione **Informe → Ejecutar informe** para ejecutar inmediatamente informes guardados. En la lista de informes, pulsar Ejecutar. Identity Manager ejecuta el informe y muestra los resultados en forma resumida y detallada.
- Seleccionar **Tareas del servidor → Administrar programación** para programar cuándo se ejecutan las tareas de informe. Tras seleccionar una tarea de informe, puede configurar la frecuencia y las opciones del informe. También puede ajustar detalles específicos del informe (por ejemplo, en el área Informes de la página Definir un informe).

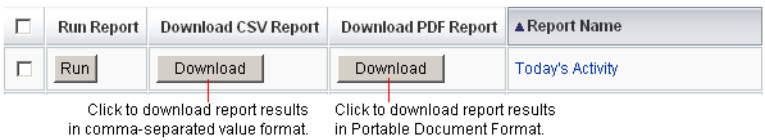
  Para que una definición de tarea aparezca en esta lista, debe definir el atributo `visibility` del objeto TaskDefinition en `schedule`.

Descarga de datos de informe

Desde la página Ejecutar informes puede descargar datos del informe para usarlos en otra aplicación, como Acrobat Reader o StarOffice.

Abra la página Ejecutar informes y pulse Descargar en una de estas columnas:

- **Descargar informe en formato CSV**. Descarga la salida del informe en formato CSV. Tras guardarlo, puede abrir el informe y trabajar con él en otra aplicación, como StarOffice.
- **Descargar informe en formato PDF**. Descarga la salida del informe en formato de documento portátil, que puede verse con Adobe Reader.



Configuración de la salida de los informes

Para configurar la salida de los informes, haga clic en Informes y seleccione Configurar informes.

La página Configurar informes permite realizar las siguientes selecciones:

- **Opciones de informe de PDF**

  Para los informes generados en formato de documento portátil (PDF), puede especificar las fuentes, el tamaño de página y la orientación.

  - **Nombre de fuente de PDF**. Seleccione la fuente que se debe usar al generar informes en PDF. De manera predeterminada sólo se muestran las fuentes disponibles para todos los visores de PDF. Sin embargo, las fuentes adicionales (como las necesarias para idiomas asiáticos) pueden agregarse al sistema copiando archivos de definición de fuente en el directorio `/fonts` del producto y reiniciando el servidor.

    Los formatos de definición de fuente aceptados incluyen `.ttf`, `.ttc`, `.otf` y `.afm`. Si elige una de estas fuentes, deberá estar disponible en el PC donde se visualice el informe. Otras posibilidad es seleccionar la opción Incorporar fuentes en documentos PDF.

  - **Incorporar fuentes en documentos PDF**. Seleccione esta opción para incorporar la definición de fuente en el informe PDF generado. De esta forma, el informe podrá verse en cualquier visor de PDF.

    Nota – Si se incorpora la fuente al documento, puede que éste aumente considerablemente de tamaño.

  - **Tamaño de página**. Para elegir el tamaño de página del PDF, seleccione carta (8 ½ por 11 pulgadas) o legal (8 ½ por 14 pulgadas) en el menú. (El valor predeterminado es *carta*.)

    Nota – A este menú se le pueden agregar otros tamaños con el pdfPageSize del formulario Reports Config Library. pdfPageSize debe adoptar un valor conocido para la clase `com.lowagie.text.Rectangle` en el paquete `itext`.

  - **Orientación**. Para elegir la orientación de página del PDF, seleccione vertical u horizontal en el menú. (El valor predeterminado es *vertical*.)

- **Opciones de informe en CSV**. Seleccione la opción Nombre del juego de caracteres para especificar el juego de caracteres utilizado al generar informes CSV. No todas las aplicaciones que importan archivos CSV admiten la codificación UTF-8 predeterminada. Si es preciso, seleccione otro juego de caracteres.

- **Configuración de eventos objeto de seguimiento**. Seleccione la opción Habilitar colección de eventos para configurar informes que debe supervisar el sistema y no se aplican a formatos personalizados. Para obtener más información, consulte "Configuración de eventos objeto de seguimiento" en la página 297.

Haga clic en Guardar para guardar las opciones de configuración del informe.

Informes de Identity Manager

Los tipos de informes de Identity Manager se agrupan en las siguientes categorías:

Informes de registro de auditoría

Los informes de registro de auditoría se basan en eventos capturados en el registro de auditoría del sistema. Estos informes suministran información acerca de cuentas generadas, solicitudes de aprobación, intentos de acceso fallidos, cambios y reinicializaciones de contraseñas, actividades de autoabastecimiento, infracción de directivas, y usuarios de proveedores de servicios (extranet), entre otros.

Nota – Antes de ejecutar registros de auditoría, debe especificar los tipos de eventos de Identity Manager que desea capturar. Para ello, seleccione Configurar en la barra de menús y después Auditoría. Seleccione uno o más nombres de grupo de auditoría para registrar los eventos correctos y fallidos de cada grupo. Para obtener más información sobre la definición de grupos de auditoría, consulte "Configuración de grupos y eventos de auditoría" en la página 111.

▼ Para definir un informe de registro de auditoría

1 **Siga las instrucciones para crear un informe en "Creación de informes" en la página 276.**

Seleccione Informes de Identity Manager en el primer menú Tipo de informe y después Informe de AuditLog en el segundo menú.

Aparece la página Definir un informe.

2 **Rellene el formulario y pulse Guardar.**

Haga clic en Ayuda si necesita ayuda con el formulario.

Una vez definidos y guardados los parámetros del informe, ejecútelo desde la página Ejecutar informes. Pulse Ejecutar para generar un informe con todos los resultados que cumplen los criterios guardados. El informe incluye la fecha en que se produjo un evento, la acción realizada y su resultado.

Informes de registro de auditoría de usuarios individuales

Igual que sucede con los informes de registro de auditoría, el informe de registro de auditoría de usuario individual se basa en eventos capturados en el registro de auditoría del sistema. Sin embargo, este informe solicita un usuario sobre el que informar, y devuelve una lista de las actividades realizadas por ese usuario. Para optimizar los resultados, este informe busca el nombre de usuario coincidente tanto en el campo `AccountId` como `ObjectDesc` del registro de auditoría.

Este informe puede devolver un conjunto fijo de columnas o bien se puede seleccionar un conjunto personalizado de columnas. Las columnas se definen en `reporttasks.xml` y `defaultreports.xml`. Ambos archivos se hallan en el directorio `sample` (situado en el directorio de instalación de Identity Manager).

▼ Para definir un informe de registro de auditoría de usuario individual

1. **Siga las instrucciones para crear un informe en "Creación de informes" en la página 276.**

   Seleccione Informes de Identity Manager en el primer menú Tipo de informe y después Informe de AuditLog de usuario individual en el segundo menú.

   Aparece la página Definir un informe.

2. **Rellene el formulario y pulse Guardar.**

   Haga clic en Ayuda si necesita ayuda con el formulario.

Informes en tiempo real

Los informes en tiempo real sondean los recursos directamente para comunicar datos en tiempo real.

Los informes en tiempo real incluyen:

- **Informe de grupo de recursos**. Resumen los atributos de grupo, incluidas las afiliaciones de los usuarios.
- **Informe de estado de recurso**. Comprueba el estado de la conexión de los recursos especificados aplicando el método `testConnection` a cada recurso.

- **Informe de usuario de recurso**. Muestra una lista con las cuentas de recursos del usuario y los atributos de las cuentas.

▼ Para definir un informe en tiempo real

1 **Siga las instrucciones para crear un informe en "Creación de informes" en la página 276.**

Seleccione Informes de Identity Manager en el primer menú Tipo de informe y después Informe de grupo de recursos, Informe de estado de recurso o Informe de usuario de recurso en el segundo menú.

Aparece la página Definir un informe.

2 **Rellene el formulario y pulse Guardar.**

Haga clic en Ayuda si necesita ayuda con el formulario.

Una vez definidos y guardados los parámetros del informe, ejecútelo desde la página Ejecutar informes. Pulse Ejecutar para generar un informe con todos los resultados que cumplen los criterios guardados.

Informes de resumen

Los tipos de informe de resumen incluyen los siguientes disponibles en la lista Informes de Identity Manager:

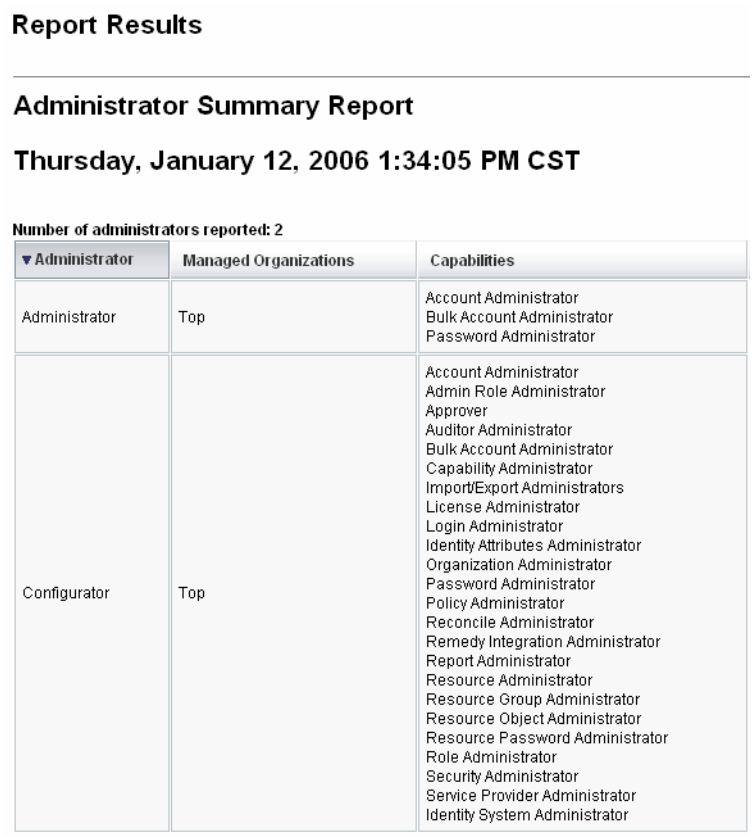
- **Informe de índice de cuenta**. Informa sobre las cuentas de recursos seleccionadas según la situación de reconciliación.
- **Informe de administradores**. Muestra los administradores de Identity Manager, las organizaciones que gestionan y las capacidades asignadas. Al definir un informe de administradores, puede seleccionar qué administradores se incluyen en función de la organización.
- **Informe de roles de administrador (Admin)** . Muestra los usuarios asignados a los roles de administración.
- **Informe de roles**. Informa sobre todos los aspectos de los roles y los recursos asociados.
- **Informe de tareas**. Informa sobre las tareas pendientes y terminadas. Debe establecer la exhaustividad de los datos que se incluyen eligiendo atributos en una lista, como aprobador, descripción, fecha de caducidad, propietario, fecha de inicio y estado.
- **Informe de usuarios**. Muestra los usuarios, los roles a los que se han asignado y los recursos a los que pueden acceder. Al definir un informe de usuarios, puede seleccionar los usuarios que se incluyen por nombre, administrador asignado, rol, organización o asignación de recursos.

- **Informe de preguntas del usuario**. Permite a los administradores localizar a los usuarios que no han contestado al número mínimo de preguntas de autenticación, tal como se especifica en sus requisitos de directiva de cuenta. Los resultados indican el nombre de usuario, la directiva de cuenta, la interfaz asociada a la directiva y el número mínimo de preguntas que se deben contestar.

Nota – De manera predeterminada, los siguientes informes se ejecutan en el conjunto de organizaciones controladas por el administrador que ha iniciado la sesión, salvo que se sustituyan seleccionando una o más organizaciones para ejecutar el informe.

- Resumen de roles de administrador (Admin)
- Resumen de administradores
- Resumen de roles
- Resumen de preguntas del usuario
- Resumen del usuario

Como ilustra la figura siguiente, el informe de administradores muestra los administradores de Identity Manager, las organizaciones que gestionan, y las capacidades y roles de administración que tienen asignados.



Report Results

Administrator Summary Report

Thursday, January 12, 2006 1:34:05 PM CST

Number of administrators reported: 2

▼Administrator	Managed Organizations	Capabilities
Administrator	Top	Account Administrator Bulk Account Administrator Password Administrator
Configurator	Top	Account Administrator Admin Role Administrator Approver Auditor Administrator Bulk Account Administrator Capability Administrator Import/Export Administrators License Administrator Login Administrator Identity Attributes Administrator Organization Administrator Password Administrator Policy Administrator Reconcile Administrator Remedy Integration Administrator Report Administrator Resource Administrator Resource Group Administrator Resource Object Administrator Resource Password Administrator Role Administrator Security Administrator Service Provider Administrator Identity System Administrator

▼ Para definir un informe de resumen

1. **Siga las instrucciones para crear un informe en "Creación de informes" en la página 276.**

   Seleccione uno de los tipos de informe de resumen (según la lista anterior) en el segundo menú.

   Aparece la página Definir un informe.

2. **Rellene el formulario y pulse Guardar.**

   Haga clic en Ayuda si necesita ayuda con el formulario.

Informes de registro del sistema

Un informe de registro del sistema muestra los mensajes y errores del sistema que se registran en el depósito.

Al configurar este informe puede incluir o excluir específicamente los siguientes elementos:

- Componentes del sistema (como abastecedor, programador o servidor)
- Códigos de error
- Niveles de gravedad (error, fatal o advertencia)

También es posible definir el máximo número de registros que se deben mostrar (el valor predeterminado es 3.000), así como si se prefiere ver los registros más antiguos o más recientes cuando los disponibles superan el número máximo especificado.

Al ejecutar un informe de registro del sistema, se pueden recuperar entradas específicas de Syslog indicando el ID de registro del sistema de la entrada de destino. Por ejemplo, para ver entradas concretas en el informe de mensajes recientes del sistema, edítelo y seleccione el campo Evento. Después, introduzca el ID de registro del sistema solicitado y pulse Ejecutar.

Nota – Para extraer registros del registro del sistema también se puede ejecutar el comando `lh syslog`. Las opciones de los comandos se detallan dentro de "Comando `syslog`" en la página 570 en el Apéndice A, "Referencia de `lh`".

▼ Para definir un informe de registro del sistema

1. **Siga las instrucciones para crear un informe en "Creación de informes" en la página 276.**

   Seleccione Informes de Identity Manager en el primer menú Tipo de informe y después Informe de SystemLog en el segundo menú.

   Aparece la página Definir un informe.

2. **Rellene el formulario y pulse Guardar.**

   Haga clic en Ayuda si necesita ayuda con el formulario.

   Una vez definidos y guardados los parámetros del informe, ejecútelo desde la página Ejecutar informes.

Informes de uso

Cree y ejecute informes de uso para ver resúmenes gráficos y/o tabulares de eventos del sistema relacionados con objetos de Identity Manager, como administradores, usuarios, roles o recursos. Los datos de los informes de uso se pueden mostrar con formato de tabla y de gráfico de barras, circular o lineal.

▼ Para definir un informe de uso

1. **Siga las instrucciones para crear un informe en "Creación de informes" en la página 276.**

2 **Seleccione Informes de Identity Manager en el primer menú Tipo de informe y después Informe de uso en el segundo menú.**

Aparece la página Definir un informe.

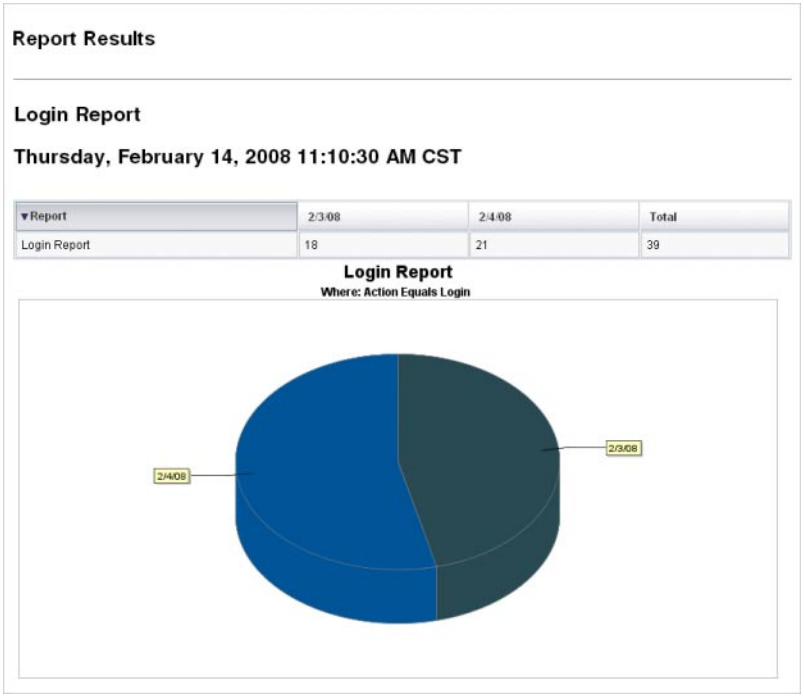
3 **Rellene el formulario y pulse Guardar.**

Haga clic en Ayuda si necesita ayuda con el formulario.

Una vez definidos y guardados los parámetros del informe, ejecútelo desde la página Ejecutar informes.

Ejemplo 8–1 Gráfico de informe de uso (cuentas de usuario generadas)

La figura siguiente muestra un ejemplo de informe de uso. La tabla superior muestra los eventos incluidos en el informe, mientras que el gráfico situado debajo presenta la misma información en formato gráfico.



Informes de flujo de trabajo

Estos informes muestran listas con los flujos de trabajo por nombre y ofrecen los datos siguientes:

- El tiempo medio que ha tardado en realizarse un flujo de trabajo.
- El número de veces que se ha solicitado el flujo de trabajo.
- El número de solicitudes de flujo de trabajo que se han completado.

Además, al hacer clic sobre el nombre del flujo de trabajo aparece una vista detallada del mismo, con cada actividad instrumentada dentro de él y el tiempo medio empleado para su realización.

Los informes de flujo de trabajo resultan especialmente útiles para capturar medidas de rendimiento que ayudan a saber si se están cumpliendo los objetivos del acuerdo de nivel de servicios (SLA).

Se debe configurar Identity Manager para capturar la métrica de temporización del flujo de trabajo como un requisito previo para ejecutar informes de flujo de trabajo. Para obtener más información, consulte la próxima sección.

Configuración de flujos de trabajo para capturar eventos de temporización de auditoría

Para poder ejecutar informes de flujo de trabajo, primero debe activar la auditoría del flujo de trabajo para cada tipo de flujo sobre el que quiera informar.

Nota – El rendimiento baja cuando se realiza una auditoría del flujo de trabajo. Por tanto, sólo debe habilitar la auditoría para aquellos flujos de trabajo que pretenda utilizar con informes de flujo de trabajo.

Para activar la auditoría del flujo de trabajo, proceda así:

- En el caso de los flujos de trabajo que se pueden configurar en la interfaz de administración mediante plantillas de tarea, seleccione la casilla Auditar todo el flujo de trabajo en la ficha Auditoría del formulario de configuración de plantillas de tarea. Consulte las instrucciones en "Configuración de la ficha Auditoría" en la página 329.
- Si se trata de flujos de trabajo carentes de plantillas de tarea, consulte "Modificación de flujos de trabajo para registrar eventos de auditoría de temporización" en la página 343.

Especificación de atributos para almacenar el informe de flujo de trabajo

Aunque no es necesario definir atributos, para aprovechar al máximo los informes de flujo de trabajo conviene almacenar los atributos por los que se pretenda filtrar los informes en el futuro.

Para definir el conjunto de atributos que interesa almacenar para cada tipo de flujo de trabajo, use el formulario con fichas de configuración de plantillas de tarea en la interfaz de administración. La ficha Auditoría contiene una sección Auditar atributos bajo la casilla de verificación Auditar todo el flujo de trabajo. Consulte las instrucciones en "Configuración de la ficha Auditoría" en la página 329.

▼ Para definir un informe de flujo de trabajo

1 **Siga las instrucciones para crear un informe en "Creación de informes" en la página 276.**

Seleccione Informes de Identity Manager en el primer menú Tipo de informe y después Informe de flujo de trabajo en el segundo menú.

Aparece la página Definir un informe.

2 **Rellene el formulario y pulse Guardar. Puede definir parámetros de tiempo y agregar cualquiera de los atributos elegidos para la auditoría. (Consulte "Especificación de atributos para almacenar el informe de flujo de trabajo" en la página 287 en la sección anterior.)**

Para restringir los resultados, especifique un nombre de atributo (por ejemplo, `user.global.state`), seleccione una condición e introduzca un valor de atributo. Puede introducir cuantos atributos necesite.

Haga clic en Ayuda si necesita ayuda con el formulario.

Una vez definidos y guardados los parámetros del informe, ejecútelo desde la página Ejecutar informes. Pulse Ejecutar para generar un informe con todos los resultados que cumplen los criterios guardados.

El informe devolverá los flujos de trabajo por nombre, junto con el tiempo medio que tardan en realizarse, el número de veces que se han solicitado y cuántas de dichas solicitudes se han completado.

Haga clic sobre el nombre del flujo de trabajo para abrir una vista detallada del mismo, con cada actividad instrumentada dentro de él. Como los procesos pueden tener actividades con igual nombre, éstas se acotan por proceso.

Informes de Auditor

Los informes de Auditor proporcionan información que ayuda a administrar el cumplimiento de los usuarios según los criterios definidos en las directivas de auditoría.

Identity Manager ofrece los siguientes informes de auditor:

- Informes de cobertura de revisión de acceso
- Informes de detalle de revisión de acceso
- Informes resumidos de revisión de acceso

- Informes de cobertura de ámbito de usuario de exploración de acceso
- Informes resumidos de directivas de auditoría
- Informes de atributos auditados
- Historial de infracciones de directivas de auditoría
- Informes de acceso de usuario
- Historial de infracciones de la organización
- Historial de infracciones del recurso
- Informes de separación de tareas
- Informes resumidos de infracciones

Para definir un informe de auditor, siga los pasos de "Creación de informes" en la página 276.

Encontrará más información sobre los informes de auditor dentro de "Operaciones con Informes de Auditor" en la página 465 en el Capítulo 15, "Auditoría: Cumplimiento de supervisión".

Uso de gráficos

Puede realizar las siguientes actividades relacionadas con gráficos:

Visualización de gráficos definidos

Identity Manager ofrece gráficos de ejemplo. En unos se utilizan datos de ejemplo y en otro no. Le recomendamos que cree gráficos adicionales para su implementación.

No debe eliminar los gráficos ni los paneles de control de muestra antes de que la implementación pase a producción. Algunos de los gráficos de muestra que no utilizan datos de ejemplo pueden aparecer en blanco si no se han recopilado los datos pertinentes.

▼ Para ver un gráfico definido

1. **En la interfaz de administración, seleccione Informes en el menú principal.**
2. **Elija Gráficos del panel en el menú secundario.**
3. **Seleccione una categoría de gráficos del panel en la lista de opciones Seleccionar tipo de gráfico del panel.**

   Todos los gráficos de la categoría elegida aparecen en la lista de gráficos.

4 **Haga clic en un nombre de gráfico.**

5 **Si lo desea, haga clic en Pausar actualización para interrumpir la actualización del panel de control. Pulse Reanudar para actualizar la vista.**

Nota – En los paneles de control con muchos gráficos, a veces resulta útil pausar la actualización hasta que se hayan cargado inicialmente todos los gráficos.

---

6 **Si lo desea, haga clic en Actualizar ahora para forzar una actualización inmediata.**

7 **Pulse Listo para volver a la página de la lista Gráficos del panel.**

Nota – Si algún gráfico presenta un mensaje de error, abra el objeto de configuración del sistema para editarlo ("Edición de objetos de configuración de Identity Manager" en la página 118) y defina `dashboard.debug=true`. Una vez configurada la propiedad, regrese al gráfico que ha generado el error y use el vínculo Incluya esta secuencia de comandos de textos si desea informar sobre un problema para recuperar la secuencia de comandos de gráfico. Esta secuencia de comandos de gráfico debe incluirse al informar sobre el problema.

▼ Para crear un gráfico del panel de control

1 **En la interfaz de administración, seleccione Informes → Gráficos del panel.**

2 **Seleccione una categoría de gráficos del panel en la lista de opciones Seleccionar tipo de gráfico del panel.**

Todos los gráficos de la categoría elegida aparecen en la lista de gráficos.

3 **Pulse Nuevo para acceder a la página Crear el gráfico del panel de control e introduzca un nombre de gráfico.**

Seleccione un nombre exclusivo y representativo, ya que los gráficos se agregan al panel de control por nombre.

4 **Seleccione un registro: IDM o SAMPLE.**

Los datos de ejemplo se incluyen para que se familiarice con el sistema. Como no hay datos de ejemplo disponibles para todos los eventos con un seguimiento, esta opción es la más útil para demostraciones y experimentar con las diversas opciones de gráficos. Elimine los datos de ejemplo antes de entrar en un entorno de producción.

Nota – El conjunto de eventos objeto de seguimiento que utiliza datos de muestra no coincide con los eventos de los que se realiza realmente un seguimiento.

5 Seleccione un tipo de evento objeto de seguimiento en la lista.

Un evento es una característica del sistema, como el uso de memoria o la adición de eventos objeto de seguimiento, por ejemplo las operaciones con recursos, cuyos valores históricos se registran y se muestran en forma de gráficos o tablas.

Los eventos objeto de seguimiento del registro de IDM son:

- **Recuentos de ejecución de abastecimiento**. Realiza un seguimiento del número de operaciones de abastecimiento que han ocurrido (por tipo de operación).
- **Duración de la ejecución de abastecimiento**. Realiza un seguimiento de las operaciones de cada abastecedor (por tipo de operación).
- **Recuento de operaciones de recurso**. Realiza un seguimiento del número de operaciones de recurso.
- **Duración de la operación de recursos**. Realiza un seguimiento de la duración de una operación de recurso.
- **Duración del flujo de trabajo**. Realiza un seguimiento del tiempo que tarda en ejecutarse un flujo de trabajo.
- **Recuento de ejecución del flujo de trabajo**. Realiza un seguimiento del número de veces que se ha ejecutado cada flujo de trabajo.

6 Seleccione una Escala de tiempo en la lista.

Esta opción controla la frecuencia de adición (por ejemplo, una hora) y de retención de los datos (por ejemplo, un mes). El sistema almacena los datos de eventos objeto de seguimiento para permitir progresivamente escalas de tiempo más amplias y obtener una vista actual y detallada del sistema, así como una comprensión de las tendencias históricas.

7 Seleccione una Medida en la lista.

Se seleccionará una medida (número o media) predeterminada, según el evento objeto de seguimiento seleccionado. Cada gráfico muestra una única medida. Las unidades disponibles dependen del evento objeto de seguimiento seleccionado.

Las medidas posibles son:

- **Número**. Número total de veces que ha ocurrido el evento en el intervalo de tiempo.
- **Media**. La media aritmética de los valores del evento durante el intervalo de tiempo.
- **Máximo**. El valor máximo del evento durante el intervalo de tiempo.
- **Mínimo**. El valor mínimo del evento durante el intervalo de tiempo.
- **Histograma**. Las distintas cifras para los rangos discretos de los valores del evento durante el intervalo de tiempo.

8 **Seleccione Mostrar número como en la lista.**

El número del gráfico se muestra como un total o con distintas escalas de tiempo.

9 **Seleccione un Tipo de gráfico en la lista.**

Esta opción controla la forma en que se muestran los datos de los eventos objeto de seguimiento. Los tipos de gráficos disponibles dependen del evento objeto de seguimiento y pueden incluir gráficos de líneas, de barras o gráficos circulares.

10 **Especifique una dimensión de la base (*opcional*).**

Seleccione en la lista siguiente:

- **Nombre de recurso**. Si se ha seleccionado, se incluirán todos los valores de dimensión en el gráfico. Desactive esta opción para seleccionar valores individuales de la dimensión e incluirlos en el gráfico.
- **Instancia de servidor**. Si se ha seleccionado, se incluirán todos los valores de dimensión en el gráfico. Desactive esta opción para seleccionar valores individuales de la dimensión e incluirlos en el gráfico.
- **Tipo de operación**. Si se ha seleccionado, se incluirán todos los valores de dimensión en el gráfico. Desactive esta opción para seleccionar valores individuales de la dimensión e incluirlos en el gráfico.

  Una vez seleccionada la dimensión, la página se actualiza para mostrar un gráfico.

11 **Introduzca texto en el campo Opciones del gráfico para producir un subtítulo bajo el título principal del gráfico (*opcional*).**

12 **Seleccione Opciones avanzadas del gráfico (*opcional*).**

Use esta opción si quiere especificar lo siguiente:

- **Cuadrícula**
- **Fuente**
- **Paleta de colores**

13 **Haga clic en Guardar para crear el gráfico.**

▼ Para editar un gráfico del panel de control

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

2 **Elija Gráficos del panel en el menú secundario.**

Aparece la página Gráficos del panel de control.

3 **Seleccione una categoría en el menú desplegable Seleccionar tipo de gráfico del panel.**

Aparece una tabla con los gráficos del panel de control.

4 **Haga clic en un nombre de gráfico para editarlo.**

Los atributos del gráfico que se pueden editar varían según el gráfico seleccionado.

Pueden editarse una o varias de las características siguientes:

- **Nombre del gráfico**. Los gráficos se añaden al panel por nombre.
- **Registro**. Especifica la *descripción del evento objeto de seguimiento* definido en el registro. La selección actual incluye: SAMPLE, Service Provider e IDM.
- **Evento objeto de seguimiento**. Una característica del sistema, como el uso de memoria o la adición de eventos objeto de seguimiento, por ejemplo las operaciones con recursos, cuyos valores históricos se registran y se muestran en forma de gráficos o tablas.
- **Escala de tiempo**. Controla la frecuencia de adición y de retención de los datos.
- **Medida**. Cada gráfico muestra una única medida. Las unidades disponibles dependen del evento objeto de seguimiento seleccionado. Puede haber disponible otras opciones para la medida seleccionada.
- **Tipo de gráfico**. Controla el modo en el que se muestran los datos del evento objeto de seguimiento (por ejemplo, gráfico de líneas o de barras).
- **Valores de dimensión incluidos**. Si se ha seleccionado, se incluirán todos los valores de dimensión en el gráfico.
- **Subtítulo del gráfico**. Si lo desea, introduzca un subtítulo bajo el título principal del gráfico.
- **Opciones avanzadas del gráfico**. Sirven para especificar lo siguiente:
  - **Cuadrícula**
  - **Fuente**
  - **Paleta de colores**

5 **Pulse Guardar.**

▼ Para eliminar un gráfico definido

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

2 **Elija Gráficos del panel en el menú secundario.**

3 **Seleccione una categoría de gráficos del panel en la lista de opciones Seleccionar tipo de gráfico del panel.**

Todos los gráficos de la categoría elegida aparecen en la lista de gráficos.

4 **Seleccione los gráficos que desea eliminar mediante las casillas de verificación y después pulse Eliminar.**

Nota – Los gráficos se eliminan de todos los paneles que los contienen sin advertir.

Operaciones con paneles

Un panel o panel de control es un grupo de gráficos relacionados que pueden mostrarse en una misma página. Como sucede con los gráficos, Identity Manager ofrece un conjunto de paneles de ejemplo que a los administradores les conviene personalizar con arreglo a su propia implementación. Consulte las instrucciones en el apartado "Para crear paneles" en la página 294.

▼ Para ver paneles

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

2 **Haga clic en Ver paneles dentro del menú secundario para ver los paneles que hay definidos.**

Aparece la página Paneles de control.

3 **Haga clic en Mostrar junto al panel que desea ver.**

Nota – En los paneles de control con muchos gráficos, a veces resulta útil pausar la actualización hasta que se hayan cargado inicialmente todos los gráficos.

Haga clic en Pausar actualización para interrumpir la actualización del panel o en Actualizar para renovar la vista.

En las secciones siguientes se explican procedimientos para trabajar con los paneles:

- "Para crear paneles" en la página 294
- "Edición de paneles" en la página 295
- "Eliminación de paneles" en la página 296

▼ Para crear paneles

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

2 **Elija Ver paneles en el menú secundario.**

3 **Pulse Nuevo.**

4 **Introduzca un nombre para el nuevo panel.**

5 **Introduzca un resumen descriptivo del nuevo panel.**

6 **Seleccione una frecuencia de actualización de la lista en segundos, minutos u horas.**

Nota – Si configura una frecuencia de actualización inferior a 30 segundos, puede haber problemas con los paneles que contienen varios gráficos.

---

7 **Para asociar un estilo de gráfico al panel, seleccione la entrada correspondiente en la lista.**

Nota – Se puede utilizar un mismo gráfico en varios paneles de control.

---

8 **Para quitar un gráfico de un panel, seleccione la entrada correspondiente en la lista y haga clic en Suprimir gráficos.**

9 **Pulse Guardar.**

Edición de paneles

Para editar un panel, siga el procedimiento descrito en el apartado "Para crear paneles" en la página 294, pero en lugar de seleccionar Nuevo, seleccione el panel que desee modificar y edite estos atributos:

- El nombre del panel.
- El resumen que describe el nuevo panel.
- La frecuencia de actualización de la lista en segundos, minutos u horas.
- Agregue o suprima los gráficos asociados a un panel.

Nota – Cuando se quita un gráfico de un panel no se elimina el gráfico, que aún puede utilizarse en otros paneles de control.

Se puede utilizar un mismo gráfico en varios paneles de control.

La Figura 8–2 ilustra un ejemplo de página de edición de panel.

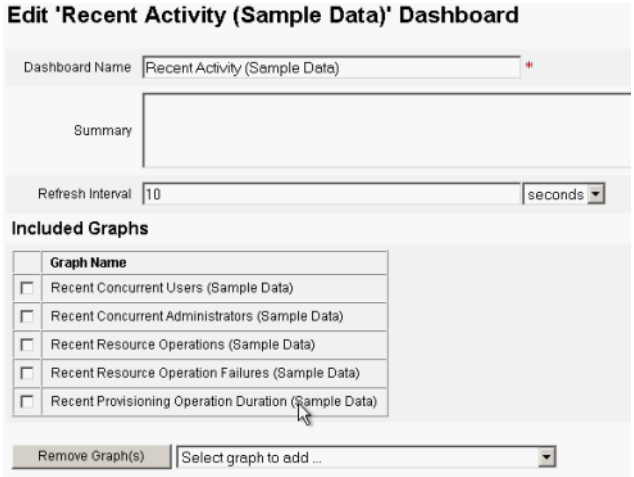


FIGURA 8–2 Edición de paneles

Eliminación de paneles

Para eliminar paneles de Service Provider, haga clic en Administrar panel dentro del área Service Provider, seleccione después el panel adecuado y pulse Eliminar.

Nota – Los gráficos incluidos en el panel no se suprimen con este procedimiento. Para eliminar gráficos, use la página Administrar gráficos del panel (consulte "Para eliminar un gráfico definido" en la página 293).

Supervisión del sistema

Puede configurar Identity Manager para efectuar un seguimiento de los eventos en tiempo real y supervisarlos en gráficos de panel. Los paneles le permiten evaluar rápidamente los recursos del sistema y detectar anomalías, conocer las tendencias históricas de rendimiento (según la hora del día, el día de la semana, etc.) y aislar interactivamente los problemas antes de consultar los registros de auditoría. Aunque no aportan tantos detalles como los registros de auditoría, proporcionan indicios sobre dónde buscar los problemas en los registros.

Puede efectuar visualizaciones de los gráficos en los paneles para rastrear las actividades automáticas y manuales a un nivel superior. Identity Manager ofrece ejemplos de gráficos de panel de *operaciones de recursos*. Los gráficos de panel de *operaciones de recursos* facilitan la supervisión rápida de los recursos del sistema para mantener un nivel de servicio aceptable.

Los datos de ejemplo de estos gráficos se pueden ver en el panel Operaciones de recursos. Para obtener más información sobre el uso de paneles, consulte "Operaciones con paneles" en la página 294.

Se recopilan datos estadísticos que se agregan en varios niveles para presentar una vista en tiempo real basada en sus especificaciones.

Configuración de eventos objeto de seguimiento

En el área Configuración de eventos objeto de seguimiento de la página Configurar informes, puede averiguar si está habilitada la recopilación de datos estadísticos sobre dichos eventos y habilitarla si lo desea. Pulse Habilitar colección de eventos para habilitar la configuración de eventos objeto de seguimiento.

Especifique las siguientes opciones para la colección de eventos:

- **Zona horaria**. Esta opción define la zona horaria que se usa para registrar los eventos objeto de seguimiento. Esta opción determina fundamentalmente los límites diarios.

  Como alternativa, puede configurar la zona horaria en la definida como predeterminada en el servidor.
- **Escalas de tiempo para recopilación**. Esta opción determina los intervalos de tiempo durante los que se agregan datos (es decir, con qué frecuencia se recopilan y persisten). Por ejemplo, si se elige un intervalo de un minuto, los datos se recopilan y persisten cada minuto.

El sistema almacena los datos de eventos objeto de seguimiento para permitir progresivamente escalas de tiempo más amplias y obtener una vista actual y detallada del sistema, así como una comprensión de las tendencias históricas.

Hay disponibles las escalas de tiempo indicadas a continuación, y todos estos intervalos se seleccionan de manera predeterminada. Desactive la selección de los intervalos durante los cuales no desea efectuar la recopilación.

- Intervalos de 10 segundos
- Intervalos de 1 minuto
- Intervalos de 1 hora
- Intervalos de 1 día
- Intervalos de 1 semana
- Intervalos de 1 mes

Tras configurar los eventos objeto de seguimiento, use los paneles para supervisarlos. Cuando haya deslizadores, utilícelos para ampliar una sección del gráfico.

Análisis de riesgo

Las funciones de análisis de riesgo de Identity Manager sirven para informar sobre las cuentas de usuario cuyos perfiles quedan fuera de ciertas restricciones de seguridad. Los informes de análisis de riesgo exploran el recurso físico para reunir datos y mostrar por recurso detalles sobre cuentas inhabilitadas, bloqueadas y sin propietario. También proporcionan detalles acerca de las contraseñas caducadas. Los detalles de los informes varían según el tipo de recurso.

Nota – Hay disponibles informes estándar para recursos de AIX, HP, Solaris, NetWare NDS y Windows Active Directory.

Las páginas de análisis de riesgo se controlan mediante un formulario y se pueden configurar para su entorno. Encontrará una lista de formularios dentro del objeto RiskReportTask en la página `idm\debug` ("Página de depuración de Identity Manager" en la página 45), que puede modificar con Identity Manager IDE. Para obtener más información sobre la configuración de formularios, consulte el Capítulo 2, "Identity Manager Forms" de *Sun Identity Manager Deployment Reference*.

▼ Para crear un informe de análisis de riesgo

1. **En la interfaz de administración, seleccione Informes en el menú principal.**
2. **Elija Ejecutar análisis de riesgo en el menú secundario.**
3. **Seleccione un informe para crear en el menú desplegable Nuevo.**

   Aparece una página Parámetros de informe para análisis de riesgo
4. **Rellene el formulario.**

   Puede restringir el informe para explorar los recursos seleccionados y, según el tipo de recurso, explorar las cuentas que cumplen estos criterios:

   - Cuentas que están inhabilitadas, caducadas, inactivas o bloqueadas.
   - Cuentas que nunca han sido usadas.
   - Cuentas que no tienen nombre completo o contraseña.
   - Cuentas que no necesitan una contraseña.
   - Cuentas con contraseñas que han caducado o no se han cambiado durante un determinado número de días.
5. **Pulse Guardar.**

▼ Para programar un informe de análisis de riesgo

Una vez definido un análisis de riesgo, puede seguir estos pasos para programarlo de modo que se ejecute a intervalos específicos:

1. **En la interfaz de administración, seleccione Tareas de servidor en el menú principal.**
2. **Elija Administrar programación en el menú secundario.**
   Aparece la página Tareas programadas.
3. **Seleccione un informe de análisis de riesgo para programarlo.**
   Aparece la página Crear nueva programación de tareas Análisis de riesgo.
4. **Introduzca un nombre y los datos de programación, y si lo desea, ajuste otras opciones de análisis de riesgo.**
5. **Haga clic en Guardar para guardar la programación.**

◆ ◆ ◆ CAPÍTULO 9

Plantillas de tarea

Las plantillas de tarea de Identity Manager le permiten utilizar la interfaz de administración hasta para configurar determinados funcionamientos del flujo de trabajo como alternativas a los flujos de trabajo personalizados.

El capítulo se divide en las secciones siguientes:

- "Habilitación de las plantillas de tarea" en la página 301. Explica cómo habilitar las plantillas de tarea para poder usarlas en el sistema.
- "Configuración de las plantillas de tarea" en la página 306. Explica cómo utilizar las plantillas de tarea para configurar funcionamientos del flujo de trabajo.

Habilitación de las plantillas de tarea

Identity Manager le ofrece las siguientes plantillas configurables:

- **Plantilla de creación de usuario**. Configura propiedades para la tarea de creación de usuarios.
- **Plantilla de eliminación de usuario**. Configura propiedades para la tarea de eliminación de usuarios.
- **Plantilla de actualización de usuario**. Configura propiedades para la tarea de actualización de usuarios.

Para poder usar estas plantillas de tareas, antes debe asignar sus procesos.

▼ Para asignar tipos de procesos

1 **En la interfaz de administración, seleccione Tareas del servidor en el menú y después Configurar tareas.**

La Figura 9–1 ilustra la página Configurar tareas.

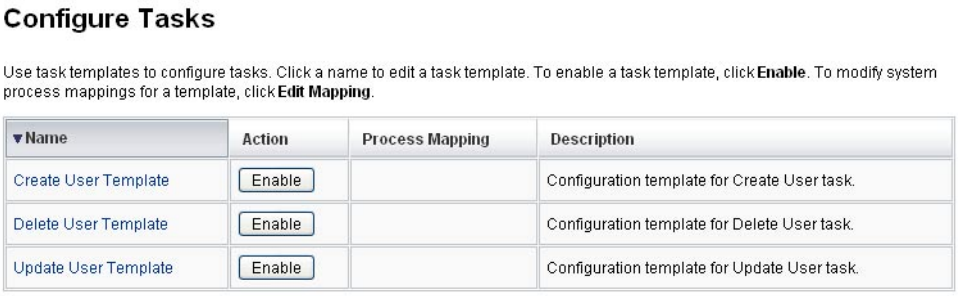


FIGURA 9–1 Página Configurar tareas inicial

La página Configurar tareas contiene una tabla con las siguientes columnas:

- **Nombre**. Ofrece vínculos con las plantillas de creación, eliminación y actualización de usuario.
- **Acción**. Contiene uno de estos botones:
  - **Habilitar**. Aparece cuando aún no se ha habilitado una plantilla.
  - **Editar asignación**. Aparece después de habilitar una plantilla.

    El procedimiento para habilitar y editar asignaciones de procesos es el mismo.
- **Asignación de procesos**. Muestra el tipo de proceso asignado a cada plantilla.
- **Descripción**. Ofrece una breve descripción de cada plantilla.

2 Pulse Habilitar para abrir la página Editar asignaciones de procesos correspondiente a una plantilla.

Por ejemplo, la página siguiente (Figura 9–2) corresponde a la plantilla de creación de usuario.

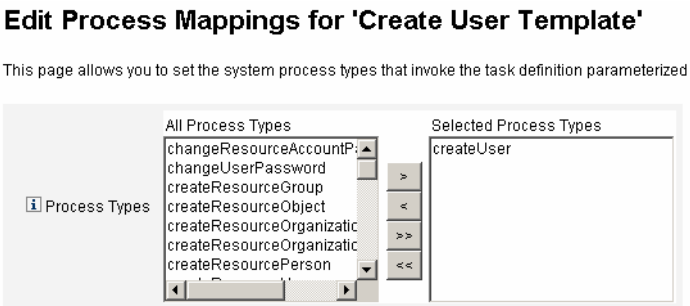
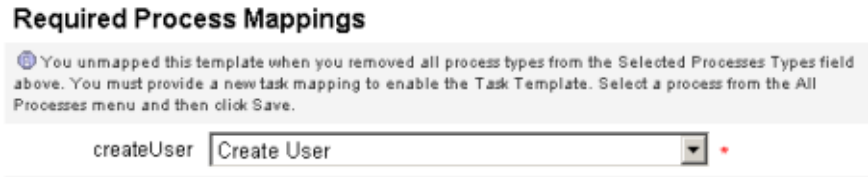


FIGURA 9–2 Página Editar asignaciones de procesos

Nota – El tipo de proceso predeterminado (en este caso, `createUser`) muestra automáticamente la lista Tipos de procesos seleccionados. Si es preciso, seleccione otro tipo de proceso en el menú.

- En general, no se asigna más de un tipo de proceso a cada plantilla.
- Si suprime el tipo de proceso de la lista Tipos de procesos seleccionados y no selecciona un sustituto, aparece una sección Asignaciones de procesos necesarias con instrucciones para elegir una nueva asignación de tarea.



3 **Pulse Guardar para asignar el tipo de proceso seleccionado y regresar a la página Configurar tareas.**

Nota – Cuando vuelve a aparecer la página Configurar tareas, contiene el botón Editar asignación en lugar de Habilitar y el nombre del proceso en la columna Asignaciones de procesos.

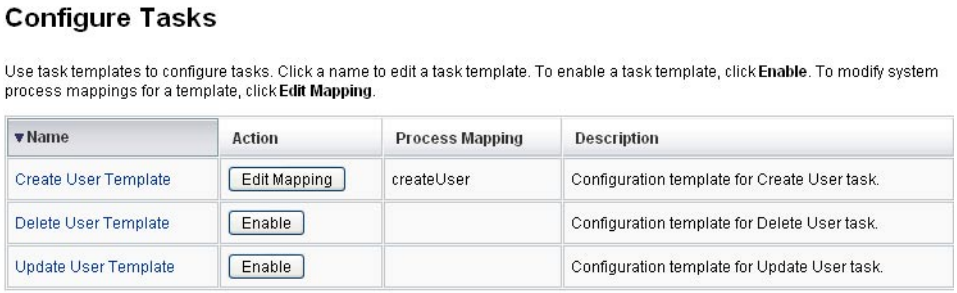


FIGURA 9–3 Tabla Configurar tareas actualizada

4 **Repita el proceso de asignación para cada una de las demás plantillas.**

Más información

Verificación de las asignaciones

- Para verificar las asignaciones, seleccione Configurar → Asignaciones de formularios y procesos. Cuando aparezca la página Configurar asignaciones de formularios y procesos, baje hasta la tabla Asignaciones de procesos y compruebe si los siguientes tipos de procesos están asignados a las entradas de Nombre de proceso asignado a.

Tipo de proceso	Nombre de proceso asignado a
`createUser`	`Plantilla de creación de usuario`
`deleteUser`	`Plantilla de eliminación de usuario`
`updateUser`	`Plantilla de actualización de usuario`

  Si las plantillas se habían habilitado correctamente, todas las entradas de Nombre de proceso asignado a deberían incluir la palabra *Plantilla*.
- También es posible asignar estos tipos de proceso directamente desde la página Asignaciones de formularios y procesos introduciendo **`Plantilla`** en la columna Nombre de proceso asignado a, tal como muestra la tabla.

▼ Para configurar una plantilla de tarea

Tras asignar los tipos de proceso a las plantillas ("Habilitación de las plantillas de tarea" en la página 301), puede configurar las plantillas de tarea.

1. **En la interfaz de administración, seleccione Tareas de servidor en el menú principal y después elija Configurar tareas.**

   Aparece la página Configurar Tareas.

2. **Seleccione un vínculo en la columna Nombre.**

   Aparece una de estas páginas:

   - **Editar plantilla de tarea 'Plantilla de creación de usuario'** . Permite editar la plantilla utilizada para crear una cuenta de usuario nueva.
   - **Editar plantilla de tarea 'Plantilla de eliminación de usuario'** . Permite editar la plantilla utilizada para eliminar o desabastecer la cuenta de un usuario.
   - **Editar plantilla de tarea 'Plantilla de actualización de usuario'** . Permite editar la plantilla utilizada para actualizar la información de un usuario.

     Cada página Editar plantilla de tarea tiene un conjunto de fichas que representan un área de configuración importante para el flujo de trabajo del usuario.

     En la tabla siguiente se describe cada ficha, su función y las plantillas que la utilizan.

Nombre de ficha	Función	Plantilla
General (*ficha predeterminada*)	Permite definir cómo se mostrará el nombre de tarea en las barras de tareas de las páginas de inicio y cuentas, y en la tabla de instancias de tareas de la página de tareas.	Sólo plantillas de tarea Crear usuario y Actualizar usuario
	Puede especificar cómo se eliminan o desabastecen las cuentas de usuario.	Plantilla Eliminar usuario
Notificación	Permite configurar las notificaciones que se envían a los administradores y usuarios por correo electrónico cuando Identity Manager invoca un proceso.	Todas las plantillas
Aprobaciones	Permite habilitar o inhabilitar las aprobaciones por tipo, designar otros aprobadores y especificar atributos a partir de datos de cuenta antes de que Identity Manager ejecute determinadas tareas.	Todas las plantillas
Auditoría	Permite habilitar y configurar la auditoría del flujo de trabajo. Aproveche esta ficha para configurar un flujo de trabajo que capture información para los informes de flujo de trabajo.	Todas las plantillas
Abastecimiento	Permite ejecutar una tarea en segundo plano y dejar a Identity Manager que reintente una tarea si ésta falla.	Sólo plantillas de tarea Crear usuario y Actualizar usuario
Creación y eliminación	Permite suspender una tarea de creación hasta una determinada fecha/hora (creación) o suspender una tarea de eliminación hasta una determinada fecha/hora (eliminación).	Plantilla de tarea Crear usuario
Transformaciones de datos	Permite configurar cómo se transforman los datos de usuario durante el abastecimiento.	Sólo plantillas de tarea Crear usuario y Actualizar usuario

3 Seleccione una de las fichas para configurar las funciones de flujo de trabajo de la plantilla.

Encontrará instrucciones para configurar estas fichas en las secciones:

- "Para asignar tipos de procesos" en la página 301
- "Para configurar una plantilla de tarea" en la página 304

4 Cuando termine de configurar las plantillas, pulse el botón Guardar para guardar los cambios.

Configuración de las plantillas de tarea

Esta sección contiene información e instrucciones para configurar plantillas de tarea. Se divide en estos temas:

Configuración de la ficha General

A continuación se explica cómo configurar la ficha General, disponible dentro del proceso de configuración de plantillas de tarea. Encontrará instrucciones para iniciar el proceso de configuración en "Configuración de las plantillas de tarea" en la página 306.

Nota – En la interfaz de administración, las páginas para editar las plantillas de creación de usuario y de actualización de usuario son idénticas, de ahí que las instrucciones de configuración se unifiquen en una sola sección.

Para las plantillas Crear usuario y Actualizar usuario

Cuando se abre el formulario Editar plantilla de tarea Plantilla de creación de usuario o Editar plantilla de tarea Plantilla de actualización de usuario, de manera predeterminada aparece la ficha General. Esta página consta del campo de texto Nombre de tarea y el menú Insertar un atributo, que se ilustran en la Figura 9–4. Encontrará instrucciones para iniciar el proceso de configuración en la sección "Configuración de las plantillas de tarea" en la página 306.

FIGURA 9–4 Ficha General: Plantilla de creación de usuario

Los nombres de tarea pueden contener texto literal y/o referencias de atributo que se resuelven al ejecutar la tarea.

▼ Para cambiar el nombre predeterminado de la tarea

1. **Escriba un nombre en el campo Nombre de tarea.**

   El nombre predeterminado de la tarea se puede editar o sustituir por completo.

2. **El menú Nombre de tarea proporciona una lista de atributos que están definidos actualmente para la vista asociada a la tarea configurada por esta plantilla. Seleccione un atributo en el menú (*opcional*).**

   Identity Manager añade el nombre de atributo al final de la entrada en el campo Nombre de tarea. Por ejemplo:

   ```
   Create user $(accountId) $(user.global.email)
   ```

3. **Cuando termine, puede:**

   - Seleccionar otra ficha para seguir editando plantillas.
   - Pulsar Guardar para guardar los cambios y regresar a la página Configurar tareas.

     El nuevo nombre de la tarea aparecerá en la barra de tareas de Identity Manager, situada en la parte inferior de las fichas Página de inicio y Cuentas.
   - Pulsar Cancelar para descartar los cambios y regresar a la página Configurar tareas.

Para la plantilla de eliminación de usuario

Cuando se abre la página 'Editar plantilla de tarea Plantilla de eliminación de usuario', de manera predeterminada aparece la ficha General. (Encontrará instrucciones para iniciar el proceso de configuración en "Configuración de las plantillas de tarea" en la página 306.)

▼ Para especificar cómo se eliminan o desabastecen las cuentas de usuario

1. **Use los botones Eliminar cuenta de Identity Manager para especificar si se puede eliminar una cuenta de Identity Manager durante una operación de eliminación.**

   Estos botones incluyen:

   - **Nunca**. Impide la eliminación de las cuentas.
   - **Sólo si el usuario no tiene ninguna cuenta vinculada después del desabastecimiento**. Permite eliminar cuentas de usuario sólo si no quedan cuentas de recursos vinculadas tras desabastecer.
   - **Siempre**. Permite eliminar cuentas de usuario siempre, incluso aunque queden cuentas de recursos asignadas.

2 Use las casillas de Desabastecimiento de cuentas de recursos para controlar el desabastecimiento de *todas* las cuentas de recursos.

Nota – Al anular la asignación y desvincular *recursos* externos de un usuario no se genera una solicitud de abastecimiento ni un elemento de trabajo. Cuando se anula la asignación o se desvincula un recurso externo, Identity Manager no desabastece ni elimina esa cuenta de recursos, por lo que no es necesario que haga nada.

Estas casillas incluyen:

- **Eliminar todo**. Elimina todas las cuentas del usuario en todos los recursos asignados.
- **Anular asignación de todo**. Anula la asignación de todas las cuentas de recursos del usuario. No elimina las cuentas de recursos.
- **Desvincular todo**. Rompe todos los vínculos del sistema Identity Manager con las cuentas de recursos. Los usuarios con cuentas que están asignadas pero no vinculadas se mostrarán con un identificador para indicar que se requiere una actualización.

Estos controles sustituyen los comportamientos de la tabla Desabastecimiento de cuentas de recursos individuales.

3 Utilice las casillas de Desabastecimiento de cuentas de recursos individuales para abordar el desabastecimiento de usuarios de un modo más minucioso que con Desabastecimiento de cuentas de recursos.

Estas casillas incluyen:

- **Eliminar**. Elimina la cuenta que representa al usuario en el recurso.
- **Unassign**. Con esta casilla habilitada, el usuario deja de estar asignado directamente al recurso. No se elimina la cuenta del recurso.
- **Desvincular**. Rompe el vínculo del sistema Identity Manager con las cuentas de recursos. Los usuarios con cuentas que están asignadas pero no vinculadas se mostrarán con un identificador para indicar que se requiere una actualización.

Las opciones de **Desabastecimiento de cuentas de recursos individuales** son útiles para especificar una directiva de desabastecimiento distinta para distintos recursos. Por ejemplo, muchos clientes prefieren no eliminar usuarios de Active Directory porque cada usuario tiene un identificador global que nunca puede volver a crearse después de eliminar. Sin embargo, quizá no le interese usar esta opción en los entornos donde se incorporan nuevos recursos, ya que habría que actualizar la configuración de desabastecimiento cada vez que agregara un nuevo recurso.

Configuración de la ficha Notificación

A continuación se explica cómo configurar la ficha Notificación, disponible dentro del proceso de configuración de plantillas de tarea. Encontrará instrucciones para iniciar el proceso de configuración en "Configuración de las plantillas de tarea" en la página 306.

Todas las plantillas de tarea permiten enviar notificaciones por correo electrónico a administradores y usuarios cuando Identity Manager invoca un proceso (normalmente una vez completado). La ficha Notificación sirve para configurar dichas notificaciones.

Nota – Identity Manager usa plantillas de correo electrónico para suministrar información y solicitudes de acciones a administradores, aprobadores y usuarios. Para obtener más información sobre las plantillas de correo electrónico de Identity Manager, consulte la sección "Personalización de plantillas de correo electrónico" en la página 106 de esta guía.

La Figura 9–5 muestra la página Notificación correspondiente a la plantilla de creación de usuario.

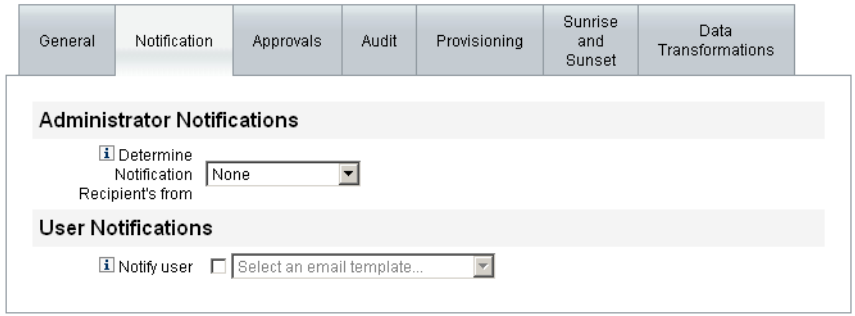


FIGURA 9–5 Ficha Notificación: Plantilla de creación de usuario

Configuración de notificaciones de usuario

Al especificar los usuarios que deben ser notificados, también debe indicar el nombre de una plantilla de correo electrónico para generar el mensaje de correo electrónico de notificación.

Para notificar al usuario que se crea, actualiza o elimina, active la casilla Notificar a usuario y después elija una plantilla de correo electrónico de la lista, como ilustra la Figura 9–6.

FIGURA 9–6 Especificación de una plantilla de correo electrónico

Configuración de notificaciones de administrador

Para especificar cómo determina Identity Manager los destinatarios de las notificaciones de administrador, seleccione una opción en el menú Determinar destinatarios de la notificación desde.

Las opciones disponibles son:

- **Ninguno** (valor predeterminado). No se notifica a ningún administrador.
- **Atributo**. Deriva los ID de cuenta de los destinatarios de la notificación a partir de un atributo especificado en la vista de usuario. Para obtener más información, consulte "Especificación de los destinatarios de las notificaciones de administrador mediante un atributo" en la página 310.
- **Regla**. Los ID de las cuentas de los destinatarios de la notificación se obtienen mediante la evaluación de una regla especificada. Para obtener más información, consulte "Especificación de los destinatarios de las notificaciones de administrador mediante una regla" en la página 311.
- **Consulta**. Los ID de las cuentas de los destinatarios de la notificación se obtienen consultando un recurso concreto. Para obtener más información, consulte "Especificación de los destinatarios de las notificaciones de administrador mediante una consulta" en la página 312.
- **Lista de administradores**. Permite elegir los destinatarios de las notificaciones explícitamente en una lista. Para obtener más información, consulte "Especificación de los destinatarios de las notificaciones de administrador mediante un atributo" en la página 310.

Especificación de los destinatarios de las notificaciones de administrador mediante un atributo

Nota – El atributo debe convertirse en una cadena que represente un único ID de cuenta o en una lista cuyos elementos sean ID de cuenta.

▼ Para derivar los ID de las cuentas de los destinatarios de la notificación mediante un atributo especificado

1 Seleccione Atributo en el menú Determinar destinatarios de la notificación desde y aparecerán las nuevas opciones que muestra la figura siguiente.

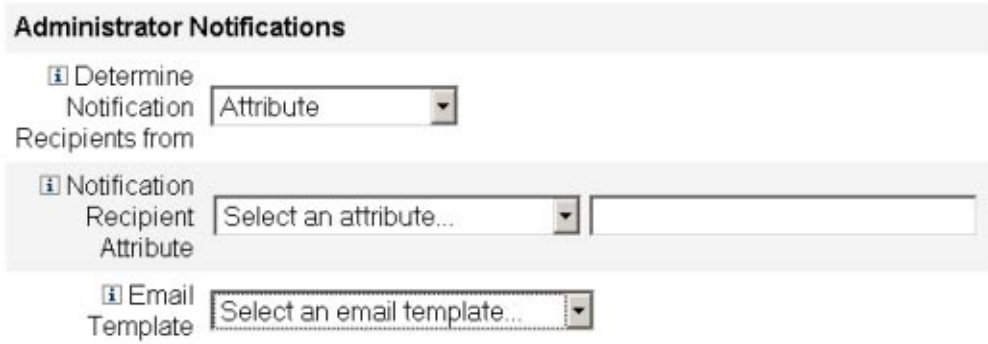


FIGURA 9–7 Notificaciones del administrador: Atributo

Las opciones incluyen:

- **Atributo de destinatario de notificación**. Proporciona una lista de atributos (definidos actualmente para la vista asociada a la tarea configurada por esta plantilla) que se usa para determinar los ID de cuenta de los destinatarios.
- **Plantilla de correo electrónico**. Proporciona una lista de plantillas de correo electrónico.

2 Seleccione un atributo en el menú Atributo de destinatario de notificación.

El nombre de atributo aparece en el campo de texto adyacente al menú.

3 Seleccione una plantilla en el menú Plantilla de correo electrónico para especificar un formato para el correo electrónico de notificación.

Especificación de los destinatarios de las notificaciones de administrador mediante una regla

Nota – Al evaluarla, la regla debe devolver una cadena que represente un único ID de cuenta o una lista cuyos elementos sean ID de cuenta.

▼ Para derivar los ID de las cuentas de los destinatarios de la notificación mediante una regla especificada

1 **Seleccione Regla en el menú Determinar destinatarios de la notificación desde y aparecerán las siguientes opciones nuevas en el formulario Notificación.**

FIGURA 9–8 Notificaciones del administrador: Regla

- **Regla del destinatario de notificación**. Proporciona una lista de reglas (actualmente definidas para el sistema) que, al evaluarlas, devuelven los ID de cuenta de los destinatarios.
- **Plantilla de correo electrónico**. Proporciona una lista de plantillas de correo electrónico.

2 **Seleccione una regla en el menú Regla del destinatario de notificación.**

3 **Seleccione una plantilla en el menú Plantilla de correo electrónico para especificar un formato para el correo electrónico de notificación del administrador.**

Especificación de los destinatarios de las notificaciones de administrador mediante una consulta

Nota – Actualmente sólo se admiten consultas de recursos de LDAP y Active Directory.

▼ Para derivar los ID de las cuentas de los destinatarios de la notificación consultando un recurso concreto

1 **Seleccione Consulta en el menú Determinar destinatarios de la notificación desde y en el formulario Notificación aparecerán las nuevas opciones que muestra la Figura 9–9.**

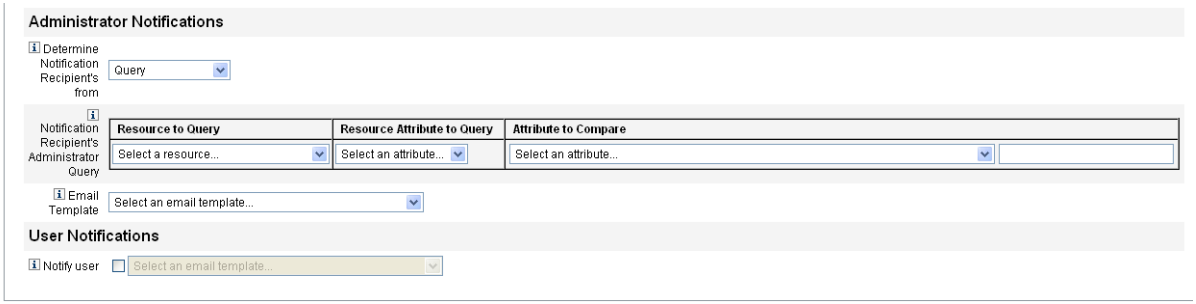


FIGURA 9–9 Notificaciones del administrador: Consulta

La tabla Consulta del administrador del destinatario de notificación tiene los siguientes menús, que puede utilizar para crear una consulta:

- **Recurso de consulta**. Proporciona una lista con los recursos que están actualmente definidos para el sistema.
- **Atributo de recurso de consulta**. Proporciona una lista con los atributos de recursos que están actualmente definidos para el sistema.
- **Atributo de comparación**. Proporciona una lista con los atributos que están actualmente definidos para el sistema.
- **Plantilla de correo electrónico**. Proporciona una lista de plantillas de correo electrónico.

2 Para crear una consulta, seleccione en los menús un recurso, un atributo de recurso y un atributo para comparar.

3 Seleccione una plantilla en el menú Plantilla de correo electrónico para especificar un formato para el correo electrónico de notificación del administrador.

▼ Para especificar destinatarios de notificación de administrador mediante la lista de administradores

1 Seleccione Lista de administradores en el menú Determinar destinatarios de la notificación desde y en el formulario Notificación aparecerán las nuevas opciones que muestra la figura siguiente.

FIGURA 9–10 Notificaciones del administrador: Lista de administradores

Las opciones incluyen:

- **Administradores destinatarios de la notificación**. Proporciona una herramienta de selección con una lista de los administradores que están disponibles.
- **Plantilla de correo electrónico**. Proporciona una lista de plantillas de correo electrónico.

2 Seleccione uno o varios administradores en la lista Administradores disponibles y trasládelos a la lista Administradores seleccionados.

3 Seleccione una plantilla en el menú Plantilla de correo electrónico para especificar un formato para el correo electrónico de notificación del administrador.

Configuración de la ficha Aprobaciones

A continuación se explica cómo configurar la ficha Aprobaciones, disponible dentro del proceso de configuración de plantillas de tarea. Encontrará instrucciones para iniciar el proceso de configuración en la sección "Configuración de las plantillas de tarea" en la página 306.

Puede utilizar la ficha Aprobaciones para designar otros aprobadores y especificar atributos en el formulario de aprobación de tareas antes de que Identity Manager ejecute las tareas de creación, eliminación o actualización de usuarios.

Tradicionalmente, los administradores asociados a una organización, un recurso o un rol concreto deben aprobar ciertas tareas antes de su ejecución. Identity Manager también le permite designar *aprobadores adicionales*, que son otros administradores a los que se les pedirá que aprueben la tarea.

Nota – Si configura aprobadores adicionales para un flujo de trabajo, significará que exige la aprobación por parte de los aprobadores tradicionales *y* de los aprobadores adicionales especificados en la plantilla.

La Figura 9–11 muestra la interfaz de administración de la página Aprobaciones inicial.

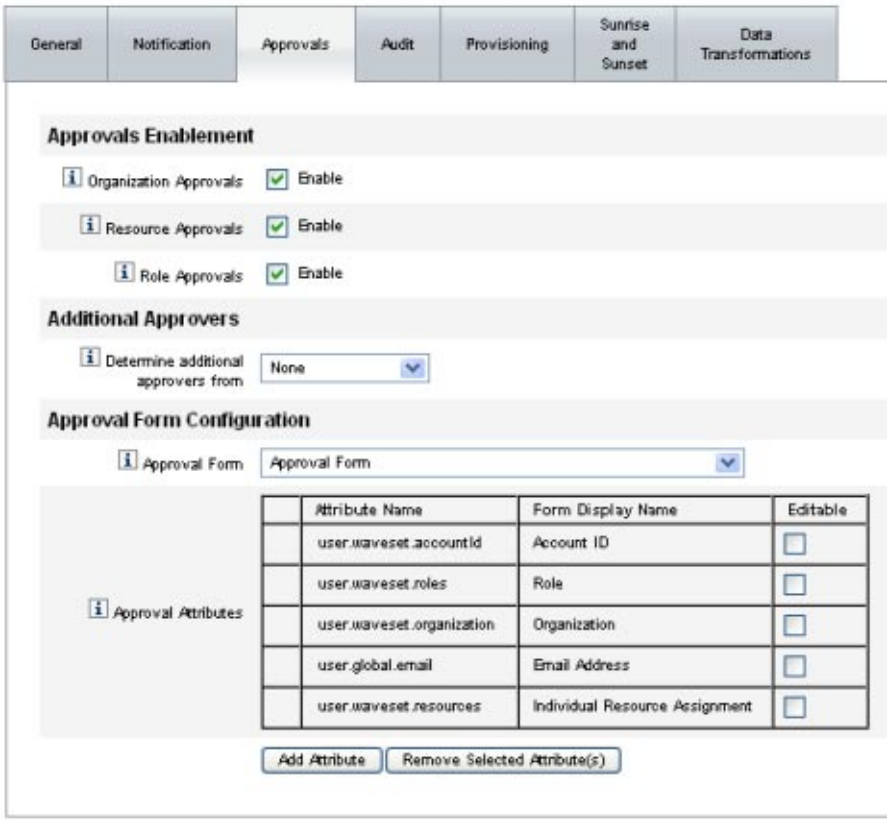


FIGURA 9–11 Ficha Aprobaciones: Plantilla de creación de usuario

▼ Para configurar aprobaciones

1 **Rellene la sección Habilitación de aprobaciones (consulte"Habilitación de aprobaciones (ficha Aprobaciones, sección Habilitación de aprobaciones)" en la página 316).**

2 **Rellene la sección Aprobadores adicionales (consulte "Especificación de aprobadores adicionales (ficha Aprobaciones, sección Aprobadores adicionales)" en la página 316).**

3 **Rellene la sección Configuración del formulario de aprobación sólo en las plantillas Crear usuario y Actualizar usuario (consulte "Configuración del formulario de aprobación (ficha Aprobaciones, sección Configuración del formulario de aprobación)" en la página 326).**

4 **Cuando termine de configurar la ficha Aprobaciones, puede:**

- Seleccionar otra ficha para seguir editando plantillas.
- Pulsar Guardar para guardar los cambios y regresar a la página Configurar tareas.
- Pulsar Cancelar para descartar los cambios y regresar a la página Configurar tareas.

Habilitación de aprobaciones (ficha Aprobaciones, sección Habilitación de aprobaciones)

Use las siguientes casillas de verificación de Habilitación de aprobaciones para exigir aprobaciones previas a la ejecución de tareas de creación, eliminación o actualización de usuarios.

Nota – De manera predeterminada, estas casillas están activadas para las plantillas Crear usuario y Actualizar usuario, pero *desactivadas* para la plantilla Eliminar usuario.

- **Aprobaciones de la organización**. Marque esta casilla para exigir aprobaciones a todos los aprobadores de organización configurados.
- **Aprobaciones de recursos**. Marque esta casilla para exigir aprobaciones a todos los aprobadores de recursos configurados.
- **Aprobaciones de roles**. Marque esta casilla para exigir aprobaciones a todos los aprobadores de roles configurados.

Especificación de aprobadores adicionales (ficha Aprobaciones, sección Aprobadores adicionales)

Use el menú Determinar aprobadores adicionales desde para especificar cómo debe determinar Identity Manager otros aprobadores de las tareas de creación, eliminación o actualización de usuarios.

Las opciones de este menú se describen en la Tabla 9–1.

TABLA 9–1 Opciones del menú Determinar aprobadores adicionales desde

Opción	Descripción
Ninguno (valor predeterminado)	No se requieren aprobadores adicionales para la ejecución de la tarea.
Atributo	Los ID de cuenta de los aprobadores se derivan a partir de un atributo especificado en la vista del usuario.
Regla	Los ID de cuenta de los aprobadores se obtienen mediante la evaluación de una regla especificada.
Consulta	Los ID de cuenta de los aprobadores se obtienen consultando un recurso concreto.
Lista de administradores	Los aprobadores se eligen explícitamente en una lista.

Cuando se selecciona cualquiera de estas opciones (excepto *Ninguno*), aparecen otras opciones en la interfaz de administración.

Siga las instrucciones de las próximas secciones para especificar un método de determinación de aprobadores adicionales.

▼ Para determinar aprobadores adicionales a partir de un atributo

Siga los pasos indicados a continuación para determinar aprobadores adicionales a partir de un atributo.

1 Seleccione Atributo en el menú Determinar aprobadores adicionales desde.

Nota – El atributo debe convertirse en una cadena que represente un único ID de cuenta o en una lista cuyos elementos sean ID de cuenta.

Aparecen nuevas opciones, como ilustra la figura siguiente.

FIGURA 9–12 Aprobadores adicionales: Atributo

- **Atributo de aprobadores**. Proporciona una lista de atributos (definidos actualmente para la vista asociada a la tarea configurada por esta plantilla) que se usa para determinar los ID de cuenta de los aprobadores.
- **Tiempo de espera de la aprobación**. Proporciona un método para especificar cuándo se agota el tiempo de espera de la aprobación.

  El valor de Tiempo de espera de la aprobación afecta a las aprobaciones internas y escaladas.

2 Seleccione un atributo en el menú Atributo de aprobadores.

El atributo seleccionado aparece en el campo de texto adyacente.

3 Indique si desea que la solicitud de aprobación expire cuando transcurra un tiempo de espera determinado.

- Si quiere especificar un tiempo de espera concreto, siga las instrucciones de "Para configurar tiempos de espera de aprobación" en la página 322.
- Si prefiere no especificar ningún tiempo de espera, puede continuar en "Configuración del formulario de aprobación (ficha Aprobaciones, sección Configuración del formulario de aprobación)" en la página 326 o guardar los cambios y proceder a configurar otra ficha.

▼ Para determinar aprobadores adicionales a partir de una regla

Siga los pasos indicados a continuación para derivar las ID de cuenta de los aprobadores a partir de una regla.

1 Seleccione Regla en el menú Determinar aprobadores adicionales desde.

Nota – Al evaluarla, la regla debe devolver una cadena que represente un único ID de cuenta o una lista cuyos elementos sean ID de cuenta.

Aparecen nuevas opciones, como ilustra la figura siguiente.

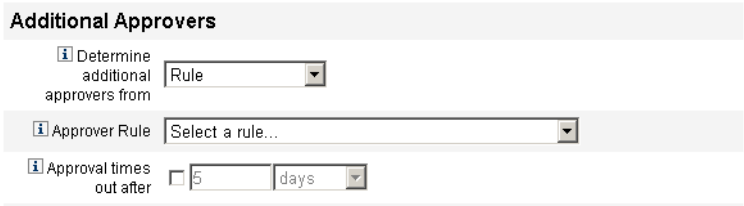


FIGURA 9–13 Aprobadores adicionales: Regla

- **Regla de aprobadores**. Proporciona una lista de reglas (actualmente definidas para el sistema) que, al evaluarlas, devuelven los ID de cuenta de los destinatarios.
- **Tiempo de espera de la aprobación**. Proporciona un método para especificar cuándo se agota el tiempo de espera de la aprobación.

  El valor de Tiempo de espera de la aprobación afecta a las aprobaciones internas y escaladas.

2 **Seleccione una regla en el menú Regla de aprobadores.**

3 **Indique si desea que la solicitud de aprobación expire cuando transcurra un tiempo de espera determinado.**

- Si quiere especificar un tiempo de espera concreto, siga las instrucciones de "Para configurar tiempos de espera de aprobación" en la página 322.
- Si prefiere no especificar ningún tiempo de espera, puede continuar en "Configuración del formulario de aprobación (ficha Aprobaciones, sección Configuración del formulario de aprobación)" en la página 326 o guardar los cambios y proceder a configurar otra ficha.

▼ Para determinar aprobadores adicionales a partir de una consulta

Siga los pasos indicados a continuación para derivar ID de cuenta de aprobadores a partir de un recurso especificado.

Nota – Actualmente sólo se admiten consultas de recursos de LDAP y Active Directory.

---

1 **Seleccione Consulta en el menú Determinar aprobadores adicionales desde y aparecerán las nuevas opciones que muestra la figura siguiente.**

FIGURA 9–14 Aprobadores adicionales: consulta

- **Consulta del administrador de aprobaciones**. Proporciona una tabla con los siguientes menús, que puede utilizar para crear una consulta:
  - **Recurso de consulta**. Proporciona una lista con los recursos que están actualmente definidos para el sistema.
  - **Atributo de recurso de consulta**. Proporciona una lista con los atributos de recursos que están actualmente definidos para el sistema.
  - **Atributo de comparación**. Proporciona una lista con los atributos que están actualmente definidos para el sistema.
- **Tiempo de espera de la aprobación**. Proporciona un método para especificar cuándo se agota el tiempo de espera de la aprobación.

Nota – El valor de Tiempo de espera de la aprobación afecta a las aprobaciones internas y escaladas.

---

2 Cree una consulta así:

a. Seleccione un recurso en el menú Recurso de consulta.

b. Seleccione atributos en los menús Atributo de recurso de consulta y Atributo de comparación.

3 Indique si desea que la solicitud de aprobación expire cuando transcurra un tiempo de espera determinado.

- Si quiere especificar un tiempo de espera concreto, siga las instrucciones de "Para configurar tiempos de espera de aprobación" en la página 322.
- Si prefiere no especificar ningún tiempo de espera, puede continuar en "Configuración del formulario de aprobación (ficha Aprobaciones, sección Configuración del formulario de aprobación)" en la página 326 o guardar los cambios y proceder a configurar otra ficha.

▼ Para determinar aprobadores adicionales a partir de la lista de administradores

Siga los pasos indicados a continuación para elegir aprobadores adicionales explícitamente en la lista de administradores.

1 Seleccione Lista de administradores en el menú Determinar aprobadores adicionales desde y aparecerán las nuevas opciones que muestra la figura siguiente.

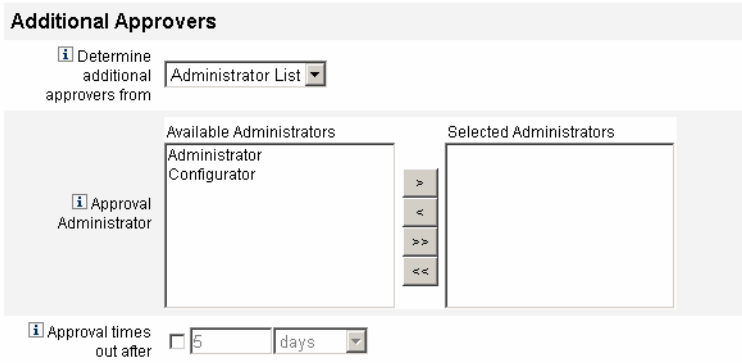


FIGURA 9–15 Aprobadores adicionales: Lista de administradores

- **Administradores destinatarios de la notificación**. Proporciona una herramienta de selección con una lista de los administradores que están disponibles.
- **Formulario de aprobación**. Proporciona una lista de formularios de usuario que los aprobadores adicionales pueden utilizar para aprobar o rechazar solicitudes de aprobación.
- **Tiempo de espera de la aprobación**. Proporciona un método para especificar cuándo se agota el tiempo de espera de la aprobación.

Tiempo de espera de la aprobación afecta a las aprobaciones iniciales y escaladas.

2 Seleccione uno o varios administradores en la lista Administradores disponibles y trasládelos a la lista Administradores seleccionados.

3 Indique si desea que la solicitud de aprobación expire cuando transcurra un tiempo de espera determinado.

- Si quiere especificar un tiempo de espera concreto, siga las instrucciones de "Para configurar tiempos de espera de aprobación" en la página 322.
- Si prefiere no especificar ningún tiempo de espera, puede continuar en "Configuración del formulario de aprobación (ficha Aprobaciones, sección Configuración del formulario de aprobación)" en la página 326.

▼ Para configurar tiempos de espera de aprobación

Siga los pasos indicados a continuación para configurar tiempos de espera de aprobación en la sección Tiempo de espera de la aprobación.

1 **Marque la casilla de verificación Tiempo de espera de la aprobación.**

El campo de texto y el menú adyacentes se activan, y aparecen las opciones de Acción de tiempo de espera, ilustradas en la figura siguiente.

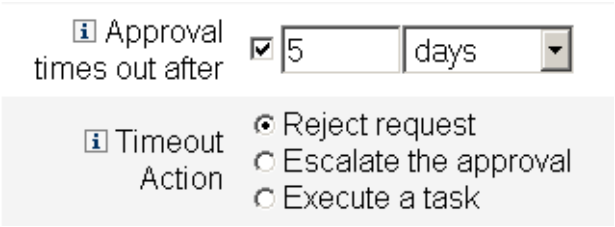


FIGURA 9–16 Opciones de Tiempo de espera de la aprobación

2 **En el campo de texto y el menú de Tiempo de espera de la aprobación, especifique el tiempo de espera así:**

a. **Seleccione segundos, minutos, horas o días en el menú.**

b. **Escriba un número en el campo de texto para indicar cuántos segundos, minutos, horas o días dura el tiempo de espera.**

Nota – El valor de Tiempo de espera de la aprobación afecta a las aprobaciones internas y escaladas.

---

3 **Use los botones de Acción de tiempo de espera para especificar lo que sucede cuando se agotan los tiempos de espera de las solicitudes de aprobación.**

Pulse uno de los siguientes:

- **Rechazar solicitud**. Identity Manager rechaza automáticamente la solicitud si no se aprueba antes de que transcurra el tiempo de espera especificado.
- **Escalar la aprobación**. Identity Manager escala automáticamente la solicitud a otro aprobador si no se aprueba antes de que transcurra el tiempo de espera especificado.

  Al activar este botón, aparecen nuevas opciones para que especifique cómo debe determinar Identity Manager los aprobadores de una aprobación escalada. Siga las instrucciones del apartado "Para configurar la sección Determinar aprobadores para escalar desde" en la página 323.

- **Ejecutar una tarea**. Identity Manager ejecuta automáticamente una tarea alternativa si la solicitud de aprobación no se aprueba antes de que transcurra el tiempo de espera especificado.

  Al activar este botón, aparece el menú Tarea de tiempo de espera de aprobación, donde puede especificar una tarea para que se ejecute cuando se agote el tiempo de espera de la solicitud de aprobación. Siga las instrucciones del apartado "Para configurar la sección Tarea de tiempo de espera de aprobación" en la página 325.

▼ Para configurar la sección Determinar aprobadores para escalar desde

Cuando se selecciona Escalar la aprobación en la sección Acción de tiempo de espera ("Para configurar tiempos de espera de aprobación" en la página 322), aparece el menú Determinar aprobadores para escalar desde, ilustrado en la figura siguiente.

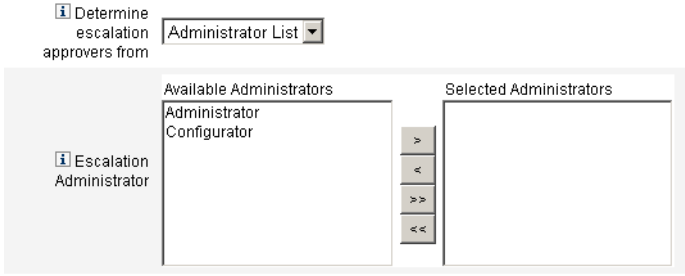
- **Elija una opción en este menú para indicar cómo se determinan los aprobadores de una aprobación escalada.**

  Las opciones incluyen:

  - **Atributo**. Determina los ID de cuenta de los aprobadores a partir de un atributo especificado en la vista del nuevo usuario.

    Nota – El atributo debe convertirse en una cadena que represente un único ID de cuenta o en una lista cuyos elementos sean ID de cuenta.

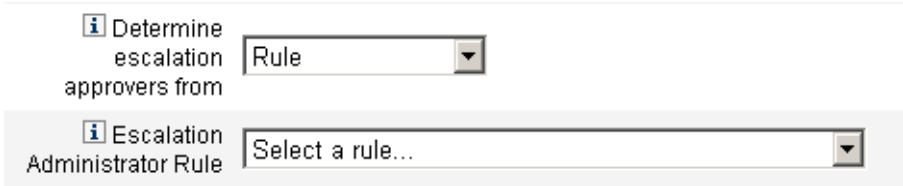
    Cuando se selecciona esta opción, aparece el menú Atributo de administrador para escalar. Seleccione en la lista un atributo, que aparecerá en el campo de texto adyacente, como muestra la figura siguiente.



- **Regla**. Determina los ID de cuenta de los aprobadores mediante la evaluación de una regla especificada.

  Nota – Al evaluarla, la regla debe devolver una cadena que represente un único ID de cuenta o una lista cuyos elementos sean ID de cuenta.

  Cuando se selecciona esta opción, aparece el menú Regla de administrador para escalar, ilustrado en la figura. Seleccione una regla en la lista.

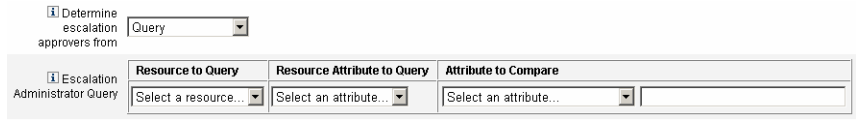


- **Consulta**. Determina los ID de cuenta de los aprobadores consultando un recurso concreto.

  Aparecen los menús de Consulta de administrador para escalar, ilustrados en la figura siguiente.

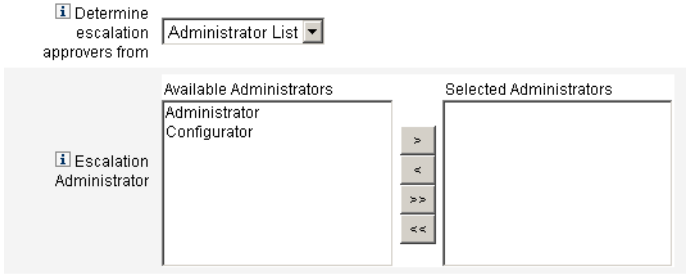
  Cree la consulta así:

  a. Seleccione un recurso en el menú Recurso de consulta.
  b. Seleccione un atributo en el menú Atributo de recurso de consulta.
  c. Seleccione un atributo en el menú Atributo de comparación.



- **Lista de administradores** (*predeterminada*). Los aprobadores se eligen explícitamente en una lista.

  Aparece la herramienta de selección Administrador para escalar, como ilustra la figura siguiente.



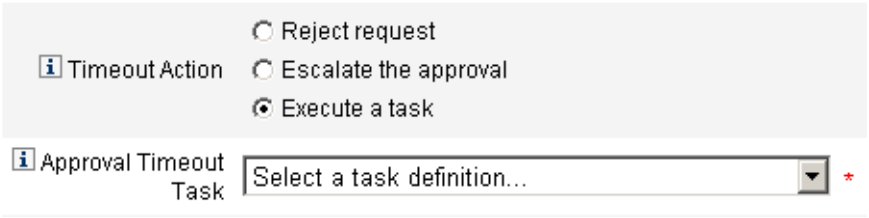
  Seleccione aprobadores así:

  a. Seleccione uno o más nombres de administrador en la lista Administradores disponibles.

  b. Traslade los nombres seleccionados a la lista Administradores seleccionados.

▼ Para configurar la sección Tarea de tiempo de espera de aprobación

Cuando se selecciona la opción Ejecutar una tarea en la sección Acción de tiempo de espera ("Para configurar tiempos de espera de aprobación" en la página 322), aparece el menú Tarea de tiempo de espera de aprobación, ilustrado en la figura siguiente.



- **Elija una definición de tarea para ejecutarla si se agota el tiempo de espera de la solicitud de aprobación.**

  Por ejemplo, puede permitir que el solicitante envíe una solicitud de servicio de asistencia o un informe al administrador.

Configuración del formulario de aprobación (ficha Aprobaciones, sección Configuración del formulario de aprobación)

Nota – La plantilla de eliminación de usuario carece de la sección Configuración del formulario de aprobación. Sólo es posible configurar dicha sección para las plantillas de creación y actualización de usuario.

Las funciones de la sección Configuración del formulario de aprobación sirven para elegir un formulario de aprobación y agregarle (o quitarle) atributos.

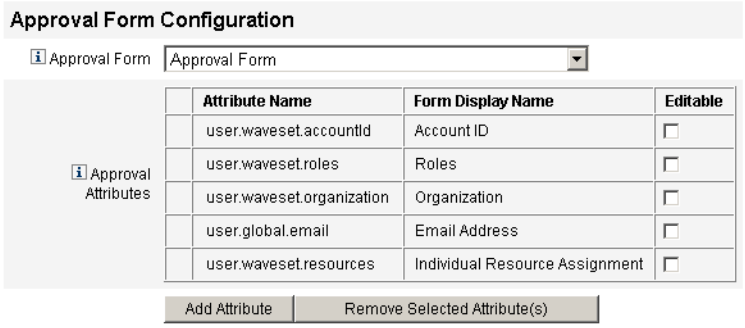


FIGURA 9–17 Configuración del formulario de aprobación

La tabla Atributos de aprobación contiene los siguientes atributos estándar:

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`
- `user.waveset.resources`

Nota – El formulario de aprobación predeterminado está preparado para mostrar los atributos de aprobación. Si va a utilizar otro formulario de aprobación, debe prepararlo para mostrar los atributos de aprobación especificados en la tabla Atributos de aprobación.

▼ Para configurar un formulario de aprobación para aprobadores adicionales

1 **Seleccione un formulario en el menú Formulario de aprobación.**

Los aprobadores utilizarán este formulario para aprobar o rechazar las solicitudes de aprobación.

2 **Marque casillas de verificación en la columna Se puede editar de la tabla Atributos de aprobación para que los aprobadores puedan editar el valor de atributo.**

Por ejemplo, si marca la casilla `user.waveset.accountId`, el aprobador podrá cambiar el ID de la cuenta del usuario.

Nota – Si modifica cualquier valor de atributo específico en el formulario de aprobación, también anulará todos los valores de atributo global que tengan el mismo nombre cuando se efectúe el abastecimiento real del usuario. Por ejemplo, si el recurso `R1` existe en el sistema con un atributo de esquema llamado `description` y usted incluye `user.accounts[R1].description` como atributo editable en el formulario de aprobación, todos los cambios que se realicen en el valor del atributo `description` dentro del formulario de aprobación sustituirán al valor propagado desde `global.description` sólo para el recurso `R1`.

---

3 **Pulse los botones Agregar atributo o *Suprimir atributos seleccionados* para especificar atributos según los datos de la cuenta del nuevo usuario con el fin de que aparezcan en el formulario de aprobación.**

- Para agregar atributos al formulario, consulte "Para agregar atributos al formulario de aprobación" en la página 327.
- Para suprimir atributos del formulario, consulte "Supresión de atributos" en la página 328.

Los atributos predeterminados de un formulario de aprobación no se pueden eliminar a menos que modifique el archivo XML.

▼ Para agregar atributos al formulario de aprobación

1 **Pulse el botón Agregar atributo situado bajo la tabla Atributos de aprobación.**

El menú con nombre Atributo se activa en la tabla Atributos de aprobación, como ilustra la figura siguiente.

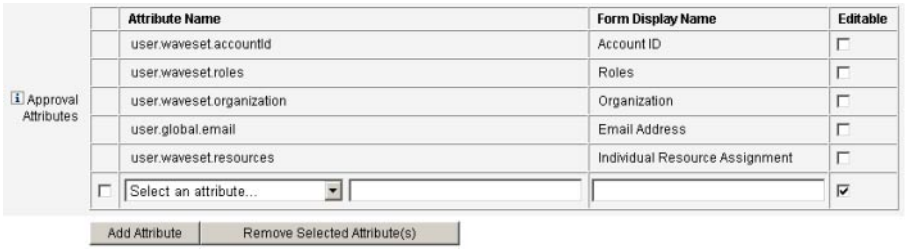


FIGURA 9–18 Inclusión de atributos de aprobación

2 Seleccione un atributo en el menú.

El nombre de atributo seleccionado aparece en el campo de texto adyacente, mientras que el nombre predeterminado del atributo para mostrar aparece en la columna Nombre de visualización del formulario.

Por ejemplo, si selecciona el atributo `user.waveset.organization`, puede:

- Cambiar el nombre de atributo predeterminado o el Nombre de visualización del formulario predeterminado en caso necesario con sólo escribir un nombre nuevo en el campo de texto correspondiente.
- Marque la casilla de verificación Se puede editar para que el aprobador pueda cambiar el valor del atributo.

  Por ejemplo, el aprobador quizá quiera sustituir información como la dirección de correo electrónico del usuario.

3 Repita estos pasos para especificar otros atributos.

Supresión de atributos

Nota – Los atributos predeterminados de un formulario de aprobación no se pueden eliminar a menos que modifique el archivo XML.

▼ Para suprimir atributos del formulario de aprobación

1 Marque una o más casillas de verificación en la columna del extremo izquierdo de la tabla Atributos de aprobación.

2 Pulse el botón Suprimir atributos seleccionados para quitar enseguida los atributos seleccionados de la tabla Atributos de aprobación.

Por ejemplo, `user.global.firstname` y `user.waveset.organization` desaparecerían de la tabla siguiente al pulsar el botón Suprimir atributos seleccionados.

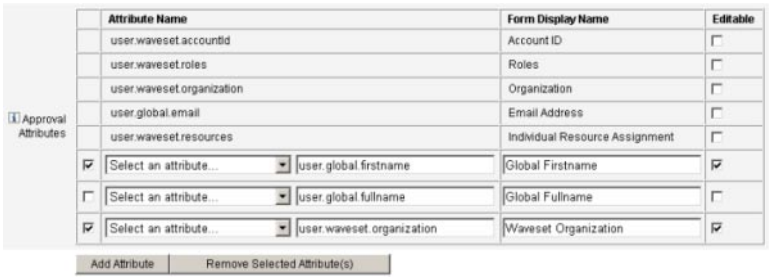


FIGURA 9–19 Supresión de atributos de aprobación

Configuración de la ficha Auditoría

A continuación se explica cómo configurar la ficha Auditoría, disponible dentro del proceso de configuración de plantillas de tarea. Encontrará instrucciones para iniciar el proceso de configuración en "Configuración de las plantillas de tarea" en la página 306.

Todas las plantillas de tarea configurables permiten configurar flujos de trabajo para auditar ciertas tareas. En concreto, puede configurar la ficha Auditoría para controlar si los eventos de flujo de trabajo se auditan y especificar qué atributos se almacenarán para generar informes.

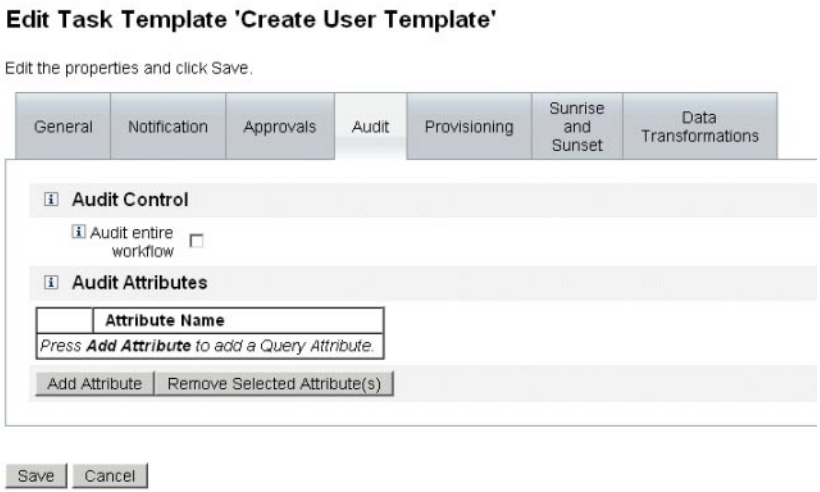


FIGURA 9–20 Auditoría de la plantilla Crear usuario

▼ Para configurar la auditoría

1 **Seleccione la casilla Auditar todo el flujo de trabajo para activar la función de auditoría del flujo de trabajo.**

Encontrará información sobre la auditoría del flujo de trabajo en "Creación de eventos de auditoría a partir de flujos de trabajo" en la página 340. Tenga en cuenta que la auditoría del flujo de trabajo baja el rendimiento.

2 **Pulse el botón Agregar atributo situado en la sección Auditar atributos para seleccionar los atributos que desea auditar a fin de generar informes.**

3 **Cuando el menú Seleccionar un atributo aparezca en la tabla Auditar atributos, elija un atributo en la lista.**

El nombre de atributo seleccionado aparece en el campo de texto adyacente.

FIGURA 9–21 Inclusión de un atributo

▼ Para suprimir atributos

1 **Marque la casilla de verificación adyacente al atributo que desea quitar.**

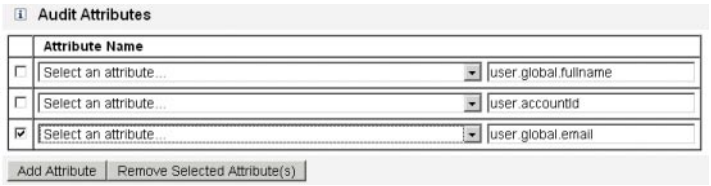


FIGURA 9–22 Supresión del atributo `user.global.email`

2 **Pulse el botón Suprimir atributos seleccionados.**

Configuración de la ficha Abastecimiento

A continuación se explica cómo configurar la ficha Abastecimiento, disponible dentro del proceso de configuración de plantillas de tarea. Encontrará instrucciones para iniciar el proceso de configuración en "Configuración de las plantillas de tarea" en la página 306.

Nota – Esta ficha sólo está disponible para las plantillas de creación y actualización de usuario.

FIGURA 9–23 Ficha Abastecimiento: plantilla de creación de usuario

Puede usar la ficha Abastecimiento para configurar las siguientes opciones relacionadas con el abastecimiento:

- **Abastecimiento en segundo plano**. Marque esta casilla de verificación para ejecutar una tarea de creación, eliminación o actualización en segundo plano, en lugar de ejecutarla de forma sincronizada.

  La posibilidad de ejecutar los procesos de abastecimiento en segundo plano le permite continuar trabajando en Identity Manager mientras se ejecuta la tarea.
- **Agregar vínculo de reintento al resultado de la tarea**. Marque esta casilla de verificación para incluir un vínculo Reintentar en la interfaz de usuario cuando se produzca un error de abastecimiento al ejecutar una tarea. El vínculo Reintentar permite a los usuarios intentar ejecutar de nuevo la tarea en caso de que falle el primer intento.

Configuración de la ficha Creación y eliminación

A continuación se explica cómo configurar la ficha Creación y eliminación, disponible dentro del proceso de configuración de plantillas de tarea. Encontrará instrucciones para iniciar el proceso de configuración en "Configuración de las plantillas de tarea" en la página 306.

Nota – Esta ficha sólo está disponible para la plantilla de creación de usuario.

La ficha Creación y eliminación permite seleccionar un método para determinar la fecha y la hora en que se producen las acciones indicadas a continuación.

- Abastecimiento de un nuevo usuario (*creación*).
- Desabastecimiento de un nuevo usuario (*eliminación*).

Por ejemplo, puede especificar una fecha de eliminación para un trabajador temporal cuyo contrato venza a los seis meses.

La Figura 9–24 ilustra los valores de configuración de la ficha Creación y eliminación.

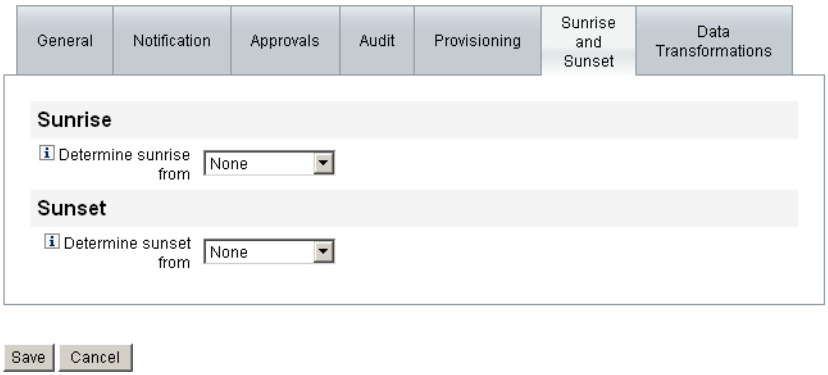


FIGURA 9–24 Ficha Creación y eliminación: Plantilla de creación de usuario

A continuación se explica cómo configurar la ficha Creación y eliminación.

Configuración de creaciones

Los valores de configuración de creación especifican la fecha y la hora en que debe producirse el abastecimiento de un nuevo usuario, así como para indicar a qué usuario pertenece el elemento de trabajo de creación.

▼ Para configurar creaciones

1 Seleccione las siguientes opciones en el menú Determinar creación desde para especificar cómo establece Identity Manager la fecha y hora de abastecimiento.

- **Especificación de la hora**. Retrasa el abastecimiento hasta la hora futura especificada. Encontrará instrucciones al respecto en "Para retrasar el abastecimiento hasta una hora especificada " en la página 333
- **Especificación de la fecha**. Retrasa el abastecimiento hasta la fecha futura especificada. Encontrará instrucciones al respecto en "Para retrasar el abastecimiento hasta una fecha especificada " en la página 334

- **Especificación del atributo**. Retrasa el abastecimiento hasta una determinada fecha y hora en función del valor del atributo que aparece en la vista del usuario. El atributo debe contener una cadena con la fecha y la hora. Al especificar un atributo para que contenga una cadena de fecha/hora, puede elegir el formato de datos que deben adoptar los datos.

  Encontrará instrucciones al respecto en "Para determinar la fecha y la hora de abastecimiento con un atributo" en la página 334.
- **Especificación de una regla**. Retrasa el abastecimiento basándose en una regla que, al evaluarla, genera una cadena de fecha y hora. Al especificar un atributo, puede elegir el formato de datos que deben adoptar los datos.

  Encontrará instrucciones al respecto en "Para determinar la fecha y la hora de abastecimiento evaluando una regla" en la página 335.

El menú Determinar creación desde adopta la opción predeterminada Ninguna, con la que el abastecimiento es inmediato.

2 Seleccione en el menú Propietario del elemento de trabajo el usuario que poseerá el elemento de trabajo para la creación.

Nota – Los elementos de trabajo de creación están disponibles en la ficha Aprobaciones.

Especificación de la hora

Las instrucciones siguientes le ayudarán a retrasar el abastecimiento hasta una hora concreta.

▼ Para retrasar el abastecimiento hasta una hora especificada

1 Seleccione Hora especificada en el menú Determinar creación desde.

2 Cuando aparezcan un nuevo campo de texto y un menú a la derecha del menú Determinar creación desde, escriba un número en el campo de texto vacío y seleccione una unidad de tiempo en el menú.

Por ejemplo, para abastecer un nuevo usuario en dos horas, introduzca los datos que muestra la figura siguiente.

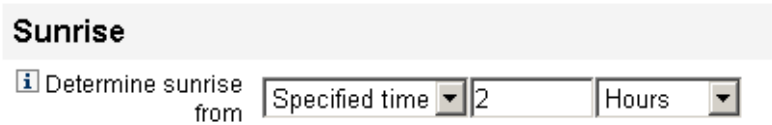


FIGURA 9–25 Abastecimiento de un nuevo usuario en dos horas

▼ Para retrasar el abastecimiento hasta una fecha especificada

Las instrucciones siguientes le ayudarán a retrasar el abastecimiento hasta una fecha concreta.

1 **Seleccione Día especificado en el menú Determinar creación desde.**

2 **Use las opciones de menú que aparecen para indicar la semana del mes, el día de la semana y el mes en que debe producirse el abastecimiento.**

Por ejemplo, para abastecer un nuevo usuario el segundo lunes de septiembre, introduzca los datos siguientes.

FIGURA 9–26 Abastecimiento de un nuevo usuario por fecha

▼ Para determinar la fecha y la hora de abastecimiento con un atributo

Las instrucciones siguientes le ayudarán a determinar una fecha y hora de abastecimiento según los valores de atributo de las cuentas de los usuarios.

1 **Seleccione Atributo en el menú Determinar creación desde.**

Se activan las siguientes opciones:

- **Menú Atributo de creación**. Proporciona una lista de atributos que están definidos actualmente para la vista asociada a la tarea configurada por esta plantilla.
- **Casilla de verificación y menú Formato de fecha específico**. Permiten especificar una cadena de formato de fecha para el valor del atributo (si es preciso).

Si no marca la casilla de verificación Formato de fecha específico, las cadenas de fecha deberán ajustarse a un formato de fecha que sea aceptable para el formato `convertDateToString` del método `FormUtil`. Consulte la documentación del producto para obtener una lista completa de los formatos de fecha admitidos.

2 **Seleccione un atributo en el menú Atributo de creación.**

3 **En caso necesario, marque la casilla de verificación Formato de fecha específico y, cuando se active el campo Formato de fecha específico, escriba una cadena de formato de fecha.**

Por ejemplo, para abastecer un nuevo usuario basándose en el valor del atributo `waveset.accountId` con un formato de día, mes y año, introduzca la información que muestra la figura siguiente.

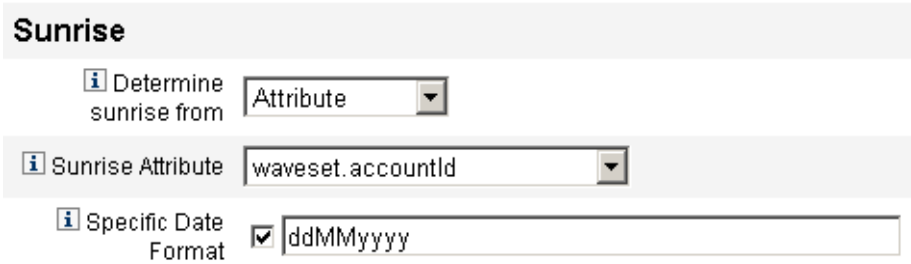


FIGURA 9–27 Abastecimiento de un nuevo usuario por atributo

▼ Para determinar la fecha y la hora de abastecimiento evaluando una regla

Las instrucciones siguientes le ayudarán a establecer la fecha y la hora de abastecimiento evaluando una reglar concreta.

1 **Seleccione Regla en el menú Determinar creación desde.**

Se activan las siguientes opciones:

- **Menú Regla de creación**. Proporciona una lista con las reglas que están actualmente definidas para el sistema.
- Casilla de verificación y menú **Formato de fecha específico**. Permiten especificar una cadena de formato de fecha para el valor devuelto por la regla (si es preciso).

Si no marca la casilla de verificación Formato de fecha específico, las cadenas de fecha deberán ajustarse a un formato de fecha que sea aceptable para el formato `convertDateToString`del método `FormUtil`. Consulte la documentación del producto para obtener una lista completa de los formatos de fecha admitidos.

2 **Seleccione una regla en el menú Regla de creación.**

3 **En caso necesario, marque la casilla de verificación Formato de fecha específico y, cuando se active el campo Formato de fecha específico, escriba una cadena de formato de fecha.**

Por ejemplo, para abastecer un nuevo usuario basándose en la regla de correo electrónico con un formato de año, mes, día, horas, minutos y segundos, introduzca la información que muestra la figura siguiente.

FIGURA 9–28 Abastecimiento de un nuevo usuario con una regla

Configuración de eliminaciones

Las opciones y los procedimientos para configurar las eliminaciones (desabastecimiento) son similares a los de creación (abastecimiento) que se describen en la sección Configuración de creaciones.

La única diferencia es que el área Eliminación contiene un menú Tarea de eliminación, porque debe especificar una tarea para desabastecer al usuario en la fecha y hora indicadas.

▼ Para configurar una eliminación

1 Use el menú Determinar eliminación desde para especificar el método con que se establece cuándo debe producirse el desabastecimiento:

Nota – El menú Determinar eliminación desde adopta la opción predeterminada Ninguna, con la que el desabastecimiento es inmediato.

- **Hora especificada**. Retrasa el desabastecimiento hasta la hora futura especificada. Encontrará instrucciones al respecto en "Para retrasar el abastecimiento hasta una hora especificada " en la página 333
- **Fecha especificada**. Retrasa el desabastecimiento hasta la fecha futura especificada. Encontrará instrucciones al respecto en "Para retrasar el abastecimiento hasta una fecha especificada " en la página 334
- **Atributo**. Retrasa el desabastecimiento hasta una determinada fecha y hora en función del valor del atributo que aparece en la cuenta del usuario. El atributo debe contener una cadena con la fecha y la hora. Al especificar un atributo para que contenga una cadena de fecha/hora, puede elegir el formato de fecha que deben adoptar los datos. Encontrará instrucciones al respecto en "Para determinar la fecha y la hora de abastecimiento con un atributo" en la página 334.
- **Regla**. Retrasa el desabastecimiento basándose en una regla que, al evaluarla, genera una cadena de fecha y hora. Al especificar un atributo, puede elegir el formato de fecha que deben adoptar los datos.

Encontrará instrucciones al respecto en "Para determinar la fecha y la hora de abastecimiento evaluando una regla" en la página 335.

2 **Use el menú Tarea de eliminación para especificar una tarea de desabastecimiento del usuario en la fecha y hora indicadas.**

Configuración de la ficha Transformaciones de datos

A continuación se explica cómo configurar la ficha Transformaciones de datos, disponible dentro del proceso de configuración de plantillas de tarea. Encontrará instrucciones para iniciar el proceso de configuración en "Configuración de las plantillas de tarea" en la página 306.

Nota – Esta ficha sólo está disponible para las plantillas de creación y actualización de usuario.

Si desea alterar datos de cuenta de usuario durante la ejecución del flujo de trabajo, puede usar la ficha Transformaciones de datos para especificar cómo debe transformar Identity Manager los datos durante el abastecimiento.

Por ejemplo, quizá le interese usar formularios o reglas para generar direcciones de correo electrónico conformes con las directivas de la empresa, o tal vez generar fechas de creación o eliminación.

Al seleccionar la ficha Transformaciones de datos, aparece la página siguiente.

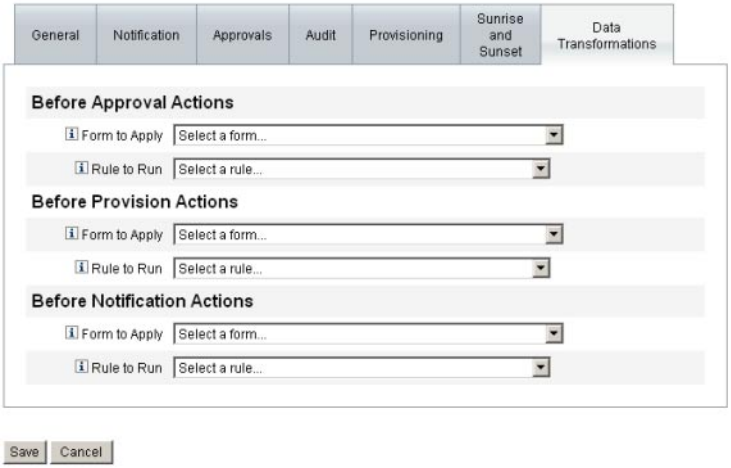


FIGURA 9–29 Ficha Transformaciones de datos: Plantilla de creación de usuario

Esta página contiene las secciones siguientes:

- **Antes de las acciones de aprobación**. Configure las opciones de esta sección para transformar datos de cuenta de usuario antes de enviar solicitudes de aprobación a determinados aprobadores.
- **Antes de las acciones de abastecimiento**. Configure las opciones de esta sección para transformar datos de cuenta de usuario antes de una acción de abastecimiento.
- **Antes de las acciones de notificación**. Configure las opciones de esta sección para transformar datos de cuenta de usuario antes de enviar notificaciones a los destinatarios especificados.

En cada sección se pueden configurar estas opciones:

- Menús **Formulario de aplicación**. Proporciona una lista con los formularios que están actualmente configurados para el sistema. Use estos menús para especificar los formularios que se usarán al transformar los datos de las cuentas de usuario.
- Menú **Regla de ejecución**. Proporciona una lista con las reglas que están actualmente configuradas para el sistema. Use estos menús para especificar las reglas que se usarán al transformar los datos de las cuentas de usuario.

◆ ◆ ◆ CAPÍTULO 10

Registro de auditoría

En este capítulo se explica cómo registra los eventos el sistema de auditoría.

Esta información se ha dividido en los temas siguientes:

El proceso de registro de auditoría

El proceso de auditoría de Identity Manager tiene como finalidad registrar quién ha hecho qué con cuáles objetos de Identity Manager y cuándo lo ha hecho.

Los eventos de auditoría están controlados por uno o varios publicadores. De manera predeterminada, Identity Manager utiliza el publicador del depósito para registrar los eventos de auditoría en el depósito. Con la ayuda de los grupos de auditoría, el filtrado permite al administrador seleccionar un subconjunto de eventos de auditoría para registrarlos. A cada publicador se le puede asignar uno o varios grupos de auditoría que se habilitan inicialmente.

Nota – Encontrará información sobre la supervisión y administración de infracciones de usuario en el Capítulo 13, "Auditoría de identidades: Conceptos básicos".

¿Qué audita Identity Manager?

La mayoría de la auditoría predeterminada la realizan los componentes internos de Identity Manager. Sin embargo, hay interfaces que permiten generar eventos a partir de flujos de trabajo o código Java.

La instrumentación de auditoría de Identity Manager se centra en cuatro áreas principales:

- **Abastecedor**. Un componente interno denominado abastecedor puede generar eventos de auditoría.
- **Controladores de vista**. En la arquitectura de la vista, el controlador de la vista genera registros de auditoría. Un controlador de vista siempre debe auditar cuándo se crean o modifican los objetos.
- **Sesión**. Los métodos de sesión (como `checkinObject`, `createObject`, `runTask`, `login` y `logout`) crean un registro de auditoría tras completar una operación auditable. La mayoría de la instrumentación recae en los controladores de vista.
- **Flujo de trabajo**. De manera predeterminada, sólo los flujos de trabajo de aprobación se instrumentan para generar registros de auditoría. Generan un evento de auditoría cuando se aprueban o rechazan solicitudes. La conexión entre la función del flujo de trabajo y el registrador de auditoría se produce mediante la aplicación `com.waveset.session.WorkflowServices`. Para obtener más información, consulte la próxima sección.

Creación de eventos de auditoría a partir de flujos de trabajo

De manera predeterminada, sólo los flujos de trabajo de aprobación se instrumentan para generar registros de auditoría. En esta sección se explica cómo utilizar la aplicación `com.waveset.session.WorkflowServices` para generar eventos de auditoría adicionales a partir de cualquier proceso de flujo de trabajo.

Quizá necesite más eventos de auditoría si debe producir informes sobre los flujos de trabajo personalizados. En "Modificación de flujos de trabajo para registrar eventos de auditoría estándar" en la página 342 se explica cómo agregar eventos de auditoría a los flujos de trabajo.

También es posible agregar eventos de auditoría especiales a los flujos de trabajo para los informes de flujo de trabajo ("Informes de flujo de trabajo" en la página 287). Los informes de flujo de trabajo indican cuánto tiempo duran los flujos de trabajo completos. Para almacenar los datos que se utilizan en los cálculos de tiempo se necesitan eventos de auditoría especiales. En "Modificación de flujos de trabajo para registrar eventos de auditoría de temporización" en la página 343 se explica cómo agregar eventos de auditoría de temporización a los flujos de trabajo.

La aplicación com.waveset.session.WorkflowServices

La aplicación `com.waveset.session.WorkflowServices` genera eventos de auditoría a partir de cualquier proceso de flujo de trabajo. En la Tabla 10–1 se describen los argumentos disponibles para esta aplicación.

TABLA 10–1 Argumentos para `com.waveset.session.WorkflowServices`

Argumento	Tipo	Descripción
`op`	Cadena	Operación para WorkflowServices. Debe configurarse en `audit` o `auditWorkflow`. Use `audit` para la auditoría de flujos de trabajo estándar. Use `auditWorkflow` para almacenar los eventos de auditoría de temporización que se utilizan en los cálculos de tiempo. Requerido.
`type`	Cadena	Nombre del tipo de objeto que se audita. Los tipos de objeto auditables se indican en la Tabla B–5. Se necesita para registrar eventos de auditoría estándar.
`action`	Cadena	Nombre de la acción realizada. Las acciones auditables se indican en la Tabla B–6. Requerido.
`status`	Cadena	Nombre del estado de la acción especificada. El estado se indica en la Tabla B–7 (dentro de la columna Resultados). Se necesita para registrar eventos de auditoría estándar.
`name`	Cadena	Nombre del objeto al que afecta la acción especificada. Se necesita para registrar eventos de auditoría estándar.
`resource`	Cadena	(*Opcional*) Nombre del recurso donde reside el objeto que se va a modificar.
`accountId`	Cadena	(*Opcional*) ID de cuenta que se va a modificar. Debe ser un nombre de cuenta de recurso nativo.
`error`	Cadena	(*Opcional*) Cadena de error localizada que se adjunta a los fallos.
`reason`	Cadena	(*Opcional*) Nombre del objeto ReasonDenied, que se asigna a un mensaje internacional descriptivo de las causas de fallo habituales.
`attributes`	Asignación	(*Opcional*) Asignación de nombres de atributo y valores que se han añadido o modificado.
`parameters`	Asignación	(*Opcional*) Asigna hasta cinco nombres o valores adicionales relevantes para un evento.

TABLA 10–1 Argumentos para `com.waveset.session.WorkflowServices` *(Continuación)*

Argumento	Tipo	Descripción
`organizations`	Lista	(*Opcional*) Lista de los nombres o ID de las organizaciones donde se situará este evento. Sirve para establecer el ámbito organizativo del registro de auditoría. Si falta, el controlador intenta averiguar la organización basándose en el tipo y el nombre. Si no consigue averiguar la organización, el evento se incluye en la organización superior, que ocupa el máximo nivel de la jerarquía organizativa.
`originalAttributes`	Asignación	(*Opcional*) Asignación de antiguos valores de atributo. Los nombres deben coincidir con los indicados en el argumento attributes. Servirá cualquier valor anterior que quiera guardar en el registro de auditoría.

Modificación de flujos de trabajo para registrar eventos de auditoría estándar

Para crear un evento de auditoría estándar en un flujo de trabajo, agréguele el siguiente elemento `<Activity>`:

```
<Activity name='createEvent'>
```

A continuación, anide en `<Activity>` un elemento `<Action>` que referencie la aplicación `com.waveset.session.WorkflowServices`:

```
<Action class='com.waveset.session.WorkflowServices'>
```

Anide en `<Action>` los elementos `<Argument>` requeridos y opcionales. La Tabla 10–1 contiene la lista de argumentos.

Para registrar eventos de auditoría estándar, el argumento `op` debe configurarse en `audit`.

"Ejemplos de flujo de trabajo" en la página 342 contiene el código mínimo requerido hasta para crear un evento de auditoría.

Ejemplos de flujo de trabajo

El ejemplo siguiente muestra una actividad de flujo de trabajo sencilla y la generación de un evento que generará una actividad de eliminación de recursos denominada `ADSIResource1`, realizada por `ResourceAdministrator`.

EJEMPLO 10–1 Actividad de flujo de trabajo simple

```
<Activity name='createEvent'> <Action class='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='Resource'/>
<Argument name='action' value='Delete'/> <Argument name='status' value='Success'/>
```

EJEMPLO 10–1 Actividad de flujo de trabajo simple *(Continuación)*

```
<Argument name='subject' value='ResourceAdministrator'/>
<Argument name='name' value='ADSIResource1'/> </Action> <Transition to='end'/> </Activity>
```

El siguiente ejemplo muestra cómo agregar atributos específicos a un flujo de trabajo que rastrea los cambios aplicados por cada usuario en un proceso de aprobación hasta un nivel detallado. Esta adición suele seguir a una acción `ManualAction` que solicita entrada al usuario.

`ACTUAL_APPROVER` se configura en el formulario y en el flujo de trabajo (en caso de aprobar desde la tabla de aprobaciones) en función de la persona que realmente ha dado la aprobación. `APPROVER` identifica la persona a la que se había asignado.

EJEMPLO 10–2 Atributos agregados para llevar un seguimiento de los cambios en un proceso de aprobación

```
<Action name='Audit the Approval' application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='User'/>
<Argument name='name' value='$(CUSTOM_DESCRIPTION)'/> <Argument name='action' value='approve'/>
<Argument name='accountId' value='$(accountId)'/> <Argument name='status' value='success'/>
<Argument name='resource' value='$(RESOURCE_IF_APPLICABLE)'/>
<Argument name='loginApplication' value='$(loginApplication)'/>
<Argument name='attributes'> <map>
<s>fullname</s><ref>user.accounts[Lighthouse].fullname</ref>
<s>jobTitle</s><ref>user.accounts[Lighthouse].jobTitle</ref>
<s>location</s><ref>user.accounts[Lighthouse].location</ref>
<s>team</s><ref>user.waveset.organization</ref> <s>agency</s>
<ref>user.accounts[Lighthouse].agency</ref> </map> </Argument>
<Argument name='originalAttributes'> <map> <s>fullname</s> <s>User's previous fullname</s>
<s>jobTitle</s> <s>User's previous job title</s> <s>location</s> <s>User's previous location</s>
<s>team</s> <s>User's previous team</s> <s>agency</s> <s>User's previous agency</s> </map>
</Argument> <Argument name='attributes'> <map> <s>firstname</s> <s>Joe</s> <s>lastname</s>
<s>New</s> </map> </Argument> <Argument name='subject'> <or> <ref>ACTUAL_APPROVER</ref>
<ref>APPROVER</ref> </or>
</Argument> <Argument name='approver' value='$(APPROVER)'/> </Action>
```

Modificación de flujos de trabajo para registrar eventos de auditoría de temporización

Es posible modificar los flujos de trabajo para registrar eventos de temporización que sirvan para los informes de flujo de trabajo ("Informes de flujo de trabajo" en la página 287). Los eventos de auditoría estándar sólo registran que se ha producido un evento, mientras que los eventos de auditoría de temporización registran cuándo ha comenzado y terminado el evento, lo que permite efectuar cálculos de tiempo. Además de los datos del evento de temporización,

también se almacena la mayoría de la información registrada por los eventos de auditoría estándar. Encontrará más información en "¿Qué información almacenan los eventos de auditoría de temporización?" en la página 345.

Nota – Para registrar eventos de auditoría de temporización, antes debe activar la auditoría del flujo de trabajo para cada tipo de flujo sobre el que quiera informar.

- En el caso de los flujos de trabajo que se pueden configurar en la interfaz de administración mediante plantillas de tarea, habilite primero la plantilla de tarea correspondiente al flujo de trabajo que desea auditar. Consulte las instrucciones en "Habilitación de las plantillas de tarea" en la página 301.

  A continuación, active la auditoría del flujo de trabajo marcando la casilla de verificación Auditar todo el flujo de trabajo. Consulte las instrucciones en "Configuración de la ficha Auditoría" en la página 329.
- Si son flujos de trabajo carentes de plantillas de tarea, defina una variable llamada `auditWorkflow` y configure su valor en `true` .

Tenga en cuenta que la auditoría del flujo de trabajo baja el rendimiento.

El Ejemplo 10–3 ilustra el código necesario para crear eventos de auditoría de temporización. Para registrar eventos de auditoría de temporización, el argumento `op` debe configurarse en `auditWorkflow`.

El argumento `action` también es obligatorio y debe definirse en uno de estos valores:

- `StartWorkflow`
- `EndWorkflow`
- `StartProcess`
- `EndProcess`
- `StartActivity`
- `EndActivity`

En el archivo `auditconfig.xml` se pueden definir otros argumentos de acción.

Ejemplos: Comienzo y terminación de eventos de auditoría en un flujo de trabajo

El Ejemplo 10–3 ilustra la habilitación de eventos de auditoría de temporización en un flujo de trabajo. Para instrumentar un flujo de trabajo, se deben agregar eventos `auditWorkflow` al principio y al final de los flujos de trabajo, procesos y actividades.

La operación `auditWorkflow` se define en `com.waveset.session.WorkflowServices` . Consulte "La aplicación `com.waveset.session.WorkflowServices`" en la página 341 para obtener más información.

EJEMPLO 10–3 Comienzo de eventos de auditoría de temporización en un flujo de trabajo

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/>
<Argument name='action' value='StartWorkflow'/>
</Action>
```

Para detener el registro de eventos de auditoría de temporización en un flujo de trabajo, incluya el código del Ejemplo 10–4 en una actividad `pre-end` cerca del final del flujo de trabajo. Observe que, al instrumentar un proceso o flujo de trabajo, no se permite incluir nada en una actividad `end`. Hay que crear una actividad `pre-end` que lleve a cabo el evento `auditWorkflow` final y después realizar una transición incondicional al evento `end`.

EJEMPLO 10–4 Terminación de eventos de auditoría de temporización en un flujo de trabajo

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/> <Argument name='action' value='EndWorkflow'/>
</Action>
```

¿Qué información almacenan los eventos de auditoría de temporización?

De manera predeterminada, los eventos de auditoría de temporización registran la mayoría de la información almacenada por los eventos de auditoría estándar, incluidos los atributos siguientes:

Atributo	Descripción
`WORKFLOW`	Nombre del flujo de trabajo ejecutado.
`PROCESS`	Nombre del proceso actualmente en ejecución.
`INSTANCEID`	ID de instancia único del flujo de trabajo ejecutado.
`ACTIVITY`	Actividad en la que se registra el evento,
`MATCH`	Identificador único dentro de una instancia de flujo de trabajo.

Los atributos anteriores se almacenan en la tabla `logattr` y proceden de `auditableAttributesList`. Identity Manager también verifica si está definido el atributo `workflowAuditAttrConds`.

Es posible llamar algunas actividades varias veces dentro de una misma instancia de un proceso o un flujo de trabajo. Para lograr la coincidencia de los eventos de auditoría en una determinada instancia de actividad, Identity Manager almacena un identificador único dentro de una instancia de flujo de trabajo en la tabla `logattr`.

Si quiere almacenar otros atributos en la tabla `logattr` para un flujo de trabajo, debe definir una lista `workflowAuditAttrConds`, que se considera una lista de objetos genéricos (`GenericObjects`). Si define un atributo `attrName` dentro de la lista `workflowAuditAttrConds` , Identity Manager extrae `attrName` del objeto dentro del código, utilizando primero `attrName` como clave y almacenando después el valor `attrName`. Todas las claves y valores se almacenan como valores en mayúsculas.

Configuración de auditoría

La configuración de auditoría consta de uno o varios publicadores y varios grupos predefinidos.

Un grupo de auditoría define un subconjunto de todos los eventos de auditoría basados en tipos de objeto, acciones y resultados de acción. A cada publicador se le asigna uno o varios grupos de auditoría. El publicador del depósito se asigna de manera predeterminada a todos los grupos de auditoría.

Un publicador de auditoría entrega eventos de auditoría a un destino de auditoría concreto. El publicador del depósito predeterminado escribe registros de auditoría en el depósito. Cada publicador de auditoría puede tener opciones de implementación específicas. A los publicadores de auditoría se les puede asignar un formateador de texto. (Los formateadores de texto aportan una representación textual de los eventos de auditoría.)

El objeto de configuración de auditoría (`#ID#Configuration:AuditConfiguration`) se define en el archivo `sample/auditconfig.xml`. Este objeto de configuración tiene una extensión que es un objeto genérico.

En el nivel superior, este objeto de configuración tiene los siguientes atributos:

- "El atributo `filterConfiguration`" en la página 346
- "El atributo `extendedTypes`" en la página 352
- "El atributo `extendedActions`" en la página 353
- "El atributo `extendedResults`" en la página 354
- "El atributo `publishers`" en la página 355

El atributo `filterConfiguration`

El atributo `filterConfiguration` ofrece una lista de grupos de eventos, que sirven para habilitar la transferencia de uno o más eventos al filtro de eventos. Cada grupo de la lista del atributo `filterConfiguration` contiene los atributos indicados en la Tabla 10–2.

TABLA 10–2 Atributos de `filterConfiguration`

Atributo	Tipo	Descripción
`groupName`	Cadena	Nombre de grupo de eventos
`displayName`	Cadena	Clave del catálogo de mensajes que representa el nombre del grupo.
`enabled`	Cadena	Marca booleana que indica si el grupo completo está habilitado o inhabilitado. Este atributo constituye una optimización para el objeto de filtrado.
`enabledEvents`	Lista	Lista de objetos genéricos que describen los eventos habilitados por un grupo. Para poder registrar un evento, debe estar en la lista. Cada objeto de la lista ha de tener estos atributos: ■ `objectType` (Cadena): Nombre de tipo de objeto (`objectType`). ■ `actions` (Lista): Lista de una o más acciones. ■ `results` (Lista): Lista de uno o más resultados.

El Ejemplo 10–5 ilustra el grupo de administración de recursos predeterminado.

EJEMPLO 10–5 Grupo de administración de recursos predeterminado

```
<Object name='Resource Management'> <Attribute name='enabled' value='true'/>
<Attribute name='displayName' value='UI_RESOURCE_MGMT_GROUP_DISPLAYNAME'/>
<Attribute name='enabledEvents'> <List> <Object> <Attribute name='objectType' value='Resource'/>
<Attribute name='actions' value='ALL'/> <Attribute name='results' value='ALL'/> </Object> <Object>
<Attribute name='objectType' value='ResourceObject'/> <Attribute name='actions' value='ALL'/>
<Attribute name='results' value='ALL'/> </Object> </List> </Attribute> </Object>
```

Identity Manager proporciona grupos de eventos de auditoría predeterminados. Estos grupos y los eventos que habilitan se describen en las próximas secciones:

Puede configurar grupos de eventos de auditoría en la página Configuración de auditoría de la interfaz de administración de Identity Manager (Configurar > Auditoría). Consulte las instrucciones en "Configuración de grupos y eventos de auditoría" en la página 111.

También es posible configurar eventos satisfactorios o fallidos para cada grupo en la página Configuración de auditoría. La interfaz no permite agregar o modificar eventos habilitados para grupos, pero para ello puede utilizar las páginas de depuración de Identity Manager ("Página de depuración de Identity Manager" en la página 45).

Nota – No todas las acciones seleccionables para un grupo de eventos de auditoría producen un registro. Además, la opción con la que se eligen todas las acciones no significa que todas las acciones de la lista estén disponibles o sean factibles para todos los grupos de eventos de auditoría.

Grupo de administración de cuentas

Este grupo está habilitado de manera predeterminada.

TABLA 10–3 Grupos de eventos de administración de cuentas predeterminados

Tipo	Acciones
`Clave de cifrado`	Todas las acciones
`Cuenta de Identity System`	Todas las acciones
`Cuenta de recursos`	Aprobar, Crear, Eliminar, Inhabilitar, Habilitar, Modificar, Rechazar, Cambiar nombre, Desbloquear
`Caso de flujo de trabajo`	Finalizar actividad, Finalizar proceso, Finalizar flujo de trabajo, Iniciar actividad, Iniciar proceso, Iniciar flujo de trabajo
`Usuario`	Aprobar, Crear, Eliminar, Inhabilitar, Habilitar, Modificar, Rechazar, Cambiar nombre

Grupo de cambios fuera de Identity System

Este grupo está inhabilitado de manera predeterminada.

TABLA 10–4 Eventos y grupos de eventos de cambios fuera de Identity Identity Manager

Tipo	Acciones
`Cuenta de recursos`	`Cambio nativo`

Grupo de administración del cumplimiento

Este grupo está habilitado de manera predeterminada.

TABLA 10–5 Eventos del grupo de administración del cumplimiento predeterminado

Tipo	Acciones
`Directiva de auditoría`	Todas las acciones
`Exploración de acceso`	Todas las acciones
`Infracción del cumplimiento`	Todas las acciones
`Exportador de datos`	Todas las acciones
`Derecho de usuario`	Autenticador aprobado, Autenticador rechazado, Remediación solicitada, Nuevo análisis solicitado, Terminar
`Flujo de trabajo de revisión de acceso`	Todas las acciones
`Flujo de trabajo de remediación`	Todas las acciones

Grupo de administración de la configuración

Este grupo está habilitado de manera predeterminada.

TABLA 10–6 Grupos de eventos de administración de la configuración predeterminados

Tipo	Acciones
`Configuración`	Todas las acciones
`Formulario de usuario`	Todas las acciones
`Rule`	Todas las acciones
`Plantilla de correo electrónico`	Todas las acciones
`Configuración de inicio de sesión`	Todas las acciones
`Directiva`	Todas las acciones
`Datos XML`	Importar
`Registro`	Todas las acciones

Grupo de administración de eventos

Este grupo está habilitado de manera predeterminada.

TABLA 10–7 Grupos de eventos de administración de eventos configuración predeterminados

Tipo	Acciones
`Correo electrónico`	Notificar
`Notificación de prueba`	Notificar

Grupo de inicios/cierres de sesión

Este grupo está habilitado de manera predeterminada.

TABLA 10–8 Grupos de eventos de inicio/cierre de sesión de Identity Manager predeterminados

Tipo	Acciones
`Usuario`	Las credenciales caducaron, Bloquear, Iniciar sesión, Cerrar sesión, Desbloquear, Recuperación del nombre de usuario

Grupo de administración de contraseñas

Este grupo está habilitado de manera predeterminada.

TABLA 10–9 Eventos y grupos de eventos de administración de contraseñas predeterminados

Tipo	Acciones
Cuenta de recursos	Cambiar contraseña, Reinicializar contraseña

Grupo de administración de recursos

Este grupo está habilitado de manera predeterminada.

TABLA 10–10 Eventos y grupos de eventos de administración de recursos predeterminados

Tipo	Acciones
`Recurso`	Todas las acciones
`Objeto de recurso`	Todas las acciones
`Formulario de recurso`	Todas las acciones
`Acción de recurso`	Todas las acciones
`Análisis de atributos`	Todas las acciones
`Caso de flujo de trabajo`	Finalizar actividad, Finalizar proceso, Finalizar flujo de trabajo, Iniciar actividad, Iniciar proceso, Iniciar flujo de trabajo

Grupo de administración de roles

Este grupo está inhabilitado de manera predeterminada.

TABLA 10–11 Eventos y grupos de eventos de administración de roles predeterminados

Tipo	Acciones
`Rol`	Todas las acciones

Grupo de administración de la seguridad

Este grupo está habilitado de manera predeterminada.

TABLA 10–12 Eventos y grupos de eventos de administración de la seguridad predeterminados

Tipo	Acciones
`Capacidad`	Todas las acciones
`Clave de cifrado`	Todas las acciones
`Organización`	Todas las acciones
`Rol de administrador`	Todas las acciones

Grupo de Service Provider

Este grupo está habilitado de manera predeterminada.

TABLA 10–13 Eventos y grupos de eventos de de Service Provider

Tipo	Acciones
`Usuario del directorio`	Respuesta de desafío, Crear, Eliminar, Modificar, Llamada posterior a la operación, Llamada previa a la operación, Actualizar respuestas de autenticación, Recuperación del nombre de usuario

Grupo de administración de tareas

Este grupo está inhabilitado de manera predeterminada.

TABLA 10–14 Eventos y grupos de eventos de administración de tareas

Tipo	Acciones
`Instancia de tarea`	Todas las acciones
`Definición de tareas`	Todas las acciones

TABLA 10–14 Eventos y grupos de eventos de administración de tareas *(Continuación)*

Tipo	Acciones
`Programación de tareas`	Todas las acciones
`Resultado de tareas`	Todas las acciones
`Tarea de abastecimiento`	Todas las acciones

El atributo `extendedTypes`

Es posible auditar cada tipo nuevo que se agrega a la clase `com.waveset.object.Type`. A un tipo nuevo se le debe asignar una clave de base de datos única formada por dos caracteres, que se almacena en la base de datos. Todos los tipos nuevos se agregan a las distintas interfaces de informes de auditoría. Cada tipo nuevo que se deba registrar en la base de datos sin filtrar ha de añadirse a un atributo `enabledEvents` de grupos de eventos de auditoría (como se describe con el atributo `enabledEvents`).

A veces interesa auditar algo que no tiene asociada una clase `com.waveset.object.Type`, o representar un tipo existente con más detalles.

Por ejemplo, el objeto `WSUser` almacena toda la información de la cuenta del usuario en el depósito. En lugar de marcar cada evento con el tipo `USER`, el proceso de auditoría divide el objeto `WSUser` en dos tipos de auditoría distintos (cuenta de recursos y cuenta de Identity Manager). Al dividir así el objeto, resulta más fácil buscar información de cuenta específica en el registro de auditoría.

Para agregar tipos de auditoría extendidos, inclúyalos en el atributo . Cada objeto extendido debe tener los atributos indicados en la tabla siguiente.

TABLA 10–15 Atributos de objeto extendidos

Argumento	Tipo	Descripción
`name`	Cadena	El nombre del tipo, que se usa al construir los eventos de auditoría y durante la filtración de eventos.
`displayName`	Cadena	Clave del catálogo de mensajes que representa el nombre del tipo.
`logDbKey`	Cadena	Clave de base de datos formada por dos caracteres que se usa al almacenar el objeto en la tabla de registro. Los valores reservados se indican en "Asignaciones de base de datos de registros de auditoría" en la página 579.

TABLA 10–15 Atributos de objeto extendidos *(Continuación)*

Argumento	Tipo	Descripción
`supportedActions`	Lista	Acciones que admite el tipo de objeto. Este atributo se usa al crear consultas de auditoría desde la interfaz de usuario. Si este valor es nulo, todas las acciones se mostrarán como posibles valores de consulta para este tipo de objeto.
`mapsToType`	Cadena	(Opcional) El nombre de la clase `com.waveset.object.Type` que se asigna a este tipo, si procede. Este atributo se utiliza para intentar resolver la afiliación organizativa de un objeto si aún no está especificada en el evento.
`organizationalMembership`	Lista	(Opcional) Una lista predeterminada de IDs de organización donde deben situarse los eventos de este tipo, si aún no tienen asignada una afiliación organizativa.

Todas las claves específicas del cliente deben empezar por el símbolo # para evitar la duplicación de claves al añadir nuevas claves internas.

El Ejemplo 10–6 ilustra el tipo extendido de cuenta de Identity Manager.

EJEMPLO 10–6 Tipo extendido de cuenta de Identity Manager

```
<Object name='LighthouseAccount'> <Attribute name='displayName' value='LG_LIGHTHOUSE_ACCOUNT'/>
<Attribute name='logDbKey' value='LA'/> <Attribute name='mapsToType' value='User'/>
<Attribute name='supportedActions'> <List> <String>Disable</String> <String>Enable</String>
<String>Create</String> <String>Modify</String> <String>Delete</String> <String>Rename</String>
</List> </Attribute> </Object>
```

El atributo `extendedActions`

Las acciones de auditoría suelen asignarse a objetos `com.waveset.security.Right`. Al agregar nuevos objetos de derechos (Right), debe especificar una clave única `logDbKey` de dos caracteres, que se almacenará en la base de datos. A veces no hay ningún derecho que corresponda a una acción concreta que debe auditarse. Puede extender las acciones incluyéndolas en la lista de objetos del atributo `extendedActions`.

Cada objeto de `extendedActions` debe tener los atributos enumerados en la Tabla 10–16.

TABLA 10–16 Atributos de `extendedAction`

Atributo	Tipo	Descripción
`name`	Cadena	El nombre de la acción, que se usa al construir los eventos de auditoría y durante la filtración de eventos.

TABLA 10–16 Atributos de `extendedAction` *(Continuación)*

Atributo	Tipo	Descripción
`displayName`	Cadena	Clave del catálogo de mensajes que representa el nombre de la acción.
`logDbKey`	Cadena	Clave de base de datos formada por dos caracteres que se usa al almacenar la acción en la tabla de registro. Los valores reservados se indican en "Asignaciones de base de datos de registros de auditoría" en la página 579.

Todas las claves específicas del cliente deben empezar por el símbolo # para evitar la duplicación de claves al añadir nuevas claves internas.

El Tabla 10–16 muestra la inclusión de una acción para el cierre de sesión.

EJEMPLO 10–7 Inclusión de una acción para el cierre de sesión

```
<Object name='Logout'> <Attribute name='displayName' value='LG_LOGOUT'/>
<Attribute name='logDbKey' value='LO'/> </Object>
```

El atributo `extendedResults`

Además de extender tipos y acciones, puede añadir resultados. Hay dos resultados predeterminados: *Satisfactorio* y *No satisfactorio*. Puede extender los resultados incluyéndolos en la lista de objetos del atributo `extendedResults`.

Cada objeto de `extendedResults` debe tener los atributos descritos en la Tabla 10–17.

TABLA 10–17 Atributos de `extendedResults`

Atributo	Tipo	Descripción
`name`	Cadena	El nombre del resultado, que se usa al definir el estado en los eventos de auditoría y durante la filtración de eventos.
`displayName`	Cadena	Clave del catálogo de mensajes que representa el nombre del resultado.
`logDbKey`	Cadena	Clave de base de datos formada por un carácter que se usa al almacenar el resultado en la tabla de registro. Consulte los valores reservados en la sección Claves de base de datos.

Todas las claves específicas del cliente deben tener cifras del 0 al 9 para evitar la duplicación de claves al añadir nuevas claves internas.

El atributo `publishers`

Cada elemento de la lista `publishers` es un objeto genérico. Cada objeto `publishers` tiene los atributos siguientes.

TABLA 10–18 Atributos de `publishers`

Atributo	Tipo	Descripción
`class`	Cadena	El nombre de la clase de publicador.
`displayName`	Cadena	Clave del catálogo de mensajes que representa el nombre del publicador.
`description`	Cadena	Descripción del publicador.
`filters`	Lista	Una lista de grupos de auditoría asignados a este publicador.
`formatter`	Cadena	El nombre del formateador de texto (en su caso).
`options`	Lista	Una lista de opciones del publicador. Estas opciones son específicas del publicador; cada elemento de la lista representa una asignación de `PublisherOption`. Consulte los ejemplos del archivo `sample/auditconfig.xml`.

Esquema de la base de datos

En el depósito de Identity Manager hay dos tablas donde se almacenan los datos de auditoría:

- `waveset.log`: Almacena la mayoría de los detalles de los eventos.
- `waveset.logattr`: Almacena los ID de las organizaciones a las que pertenece cada evento.

Estas tablas se describen a continuación.

Cuando los datos del registro de auditoría exceden los límites de longitud de columna especificados para las tablas anteriores, Identity Manager trunca los datos para que quepan. El truncamiento del registro de auditoría se trata en "Truncamiento del registro de auditoría" en la página 358.

Algunas columnas del registro de auditoría tienen límites de longitud de columna configurables. Encontrará información sobre esas columnas y cómo cambiar sus límites de longitud en "Configuración del registro de auditoría" en la página 358.

La tabla `waveset.log`

A continuación se describen los distintos nombres de columna y tipos de datos de la tabla `waveset.log`. Los tipos de datos proceden de la definición de base de datos de Oracle y varían

ligeramente entre las distintas bases de datos. Encontrará una lista de los valores de esquema de datos para todas las bases de datos compatibles en el Apéndice B, "Esquema de base de datos de registros de auditoría".

Para aprovechar el espacio, algunos valores de columna se almacenan como claves en la base de datos. Las definiciones de las claves se encuentran en la sección "Asignaciones de base de datos de registros de auditoría" en la página 579.

- `objectType CHAR(2)`: Una clave de dos caracteres que representa el tipo de objeto auditado.
- `action CHAR(2)`: Una clave de dos caracteres que representa la acción realizada.
- `actionStatus CHAR(1)`: Una clave de un carácter que representa el resultado de la acción realizada.
- `reason CHAR(2)`: Una clave de base de datos formada por dos caracteres que sirve para describir un objeto `ReasonDenied` en caso de fallo. `ReasonDenied` es una clase que ajusta una entrada del catálogo de mensajes y se utiliza con fallos habituales, como credenciales no válidas o privilegios insuficientes.
- `actionDateTimeVARCHAR(21)`: La fecha y la hora en que se produjo la acción antes indicada. Este valor se almacena en formato horario GMT.
- `objectName VARCHAR(128)`: El nombre del objeto sobre el que se ha actuado durante una operación.
- `resourceName VARCHAR(128)`: El nombre del recurso utilizado durante una operación, si procede. Algunos eventos no referencian recursos, pero a veces se consiguen más detalles registrando el recurso donde se ha efectuado una operación.
- `accountName VARCHAR(255)`: El ID de cuenta sobre el que se actúa, si procede.
- `server VARCHAR(128)`: El servidor donde se ha realizado la acción (lo asigna automáticamente el registrador de eventos).
- `message VARCHAR(255*)` o `CLOB`: Cualquier mensaje localizado asociado a una acción que incluya algo como mensaje de error. El texto se almacena para impedir que se internacionalice. El límite de longitud de esta columna es configurable. El tipo de datos predeterminado es `VARCHAR`, mientras que el límite de tamaño predeterminado es 255. Consulte "Configuración del registro de auditoría" en la página 358 para obtener información sobre cómo ajustar el límite de tamaño.
- `interface VARCHAR(50)`: La interfaz de Identity Manager (por ejemplo, de administración, usuario, IVR o SOAP) desde la que se ha efectuado la operación.
- `acctAttrChanges VARCHAR(4000) to CLOB`: Almacena los atributos de la cuenta que han cambiado durante la creación y la actualización. El campo de los cambios de atributos siempre se rellena al crear o actualizar una cuenta de recursos o un objeto de cuenta de Identity Manager. Todos los atributos modificados durante una acción se almacenan en este campo como una cadena. Los datos adoptan el formato `NOMBRE=VALOR NOMBRE2=VALOR2`. Este campo se puede consultar ejecutando instrucciones SQL "`contains`" en el nombre o el valor.

El siguiente código de ejemplo ilustra un valor de la columna `acctAttrChanges`.

```
COMPANY="COMPANY" DEPARTMENT="DEPT" DESCRIPTION="DSMITH DESCRIPTION"
FAX NUMBER="5122222222" HOME ADDRESS="12282 MOCKINGBIRD LANE" HOME CITY="AUSTIN"
HOME PHONE="5122495555" HOME STATE="TX" HOME ZIP="78729" JOB TITLE="DEVELOPER"
MOBILE PHONE="5125551212" WORK PHONE="5126855555" EMAIL="someone@somecompany.COM"
EXPIREPASSWORD="TRUE" FIRSTNAME="DANIEL" FULLNAME="DANIEL SMITH" LASTNAME="SMITH"
```

Nota – Si su instalación de Identity Manager utiliza un depósito de Oracle y percibe errores de truncamiento en el registro de auditoría, puede convertir el campo `accountAttrChanges` de `VARCHAR(4000)` a `CLOB` en la tabla del registro de auditoría. En el directorio `/web/sample` de Identity Manager hay un ejemplo de secuencia de comandos DDL que convierte `log.acctAttrChanges` de `VARCHAR(4000)` a `CLOB`. La secuencia de comandos `convert_log_acctAttrChangesCHAR2CLOB.oracle.sql` preserva los datos existentes y permite usar más 4.000 caracteres en el campo `accountAttrChanges`.

Esta conversión es opcional y sólo debe realizarse si se aprecian errores de truncamiento. Asimismo, asegúrese de realizar una copia seguridad de las tablas afectadas antes de ejecutar la secuencia de comandos de conversión.

Tras ejecutar la secuencia de comandos, detenga y reinicie el servidor de aplicaciones web. Deberá aparecer correctamente cuando ejecute un nuevo informe.

- `acctAttr01label-acctAttr05label VARCHAR(50)`: Estas cinco celdas `NAME` adicionales son columnas que pueden propiciar el almacenamiento de hasta cinco nombres de atributo en sus propias columnas, en lugar de la columna blob grande. Un atributo puede ascenderse desde la página de configuración de esquemas de recursos mediante el parámetro "`¿auditar?`", con lo cual el atributo quedará disponible para minería de datos.
- `acctAttr01value-acctAttr05value VARCHAR(128)`: Cinco celdas `NAME` adicionales que pueden propiciar el almacenamiento de hasta cinco valores de atributo en una columna distinta, en lugar de la columna blob.
- `parm01label-parm05label VARCHAR(50)`: Cinco celdas donde se almacenan los parámetros asociados a un evento, por ejemplo, los nombres de IP de cliente y ID de sesión.
- `parm01value-parm05value VARCHAR(128*)` o `CLOB`: Cinco celdas donde se almacenan los parámetros asociados a un evento, por ejemplo, los valores de IP de cliente y ID de sesión. El límite de longitud de estas columnas es configurable. El tipo de datos predeterminado es `VARCHAR`, mientras que el límite de tamaño predeterminado es 128. Consulte "Configuración del registro de auditoría" en la página 358 para obtener información sobre cómo ajustar el límite de tamaño.
- `id VARCHAR(50)`: ID único que asigna a cada registro el depósito referenciado en la tabla `waveset.logattr`.
- `name VARCHAR(128)`: Nombre generado asignado a cada registro.

- `xml BLOB`: Para uso interno de Identity Manager.

La tabla `waveset.logattr`

La tabla `waveset.logattr` sirve para almacenar los ID de la afiliación organizativa correspondiente a cada evento, que se utiliza para determinar el ámbito del registro de auditoría por organización.

- `id VARCHAR(50)`: ID del registro `waveset.log` .
- `attrname VARCHAR(50)`: En la actualidad es siempre `MEMBEROBJECTGROUPS`.
- `attrval VARCHAR(255)`: ID del grupo `MemberObject` al que pertenece el evento.

Truncamiento del registro de auditoría

Cuando una o varias columnas de datos del registro de auditoría exceden los límites de longitud de columna especificados, sus datos se truncan para que quepan. En concreto, los datos se truncan hasta el límite especificado menos tres caracteres. Para indicar que los datos se han truncado, se les añaden puntos suspensivos (...) al final de la columna.

Además, al principio de la columna `NAME` de ese registro de auditoría se añade la cadena `#TRUNCATED#` para facilitar la consulta de los registros truncados.

Nota – Identity Manager adopta la codificación UTF–8 cuando calcula dónde truncar los mensajes. Si su configuración utiliza otro tipo de codificación, es posible que los datos truncados sigan excediendo el tamaño de columna actual en la base de datos. En tal caso, el mensaje truncado no aparecerá en el registro de auditoría y se incluirá un error en el registro del sistema.

Configuración del registro de auditoría

Algunas columnas del registro de auditoría pueden configurarse para almacenar grandes cantidades de datos en el depósito.

Cambio de los límites de longitud de columna

Varias columnas del registro de auditoría tienen límites de longitud de columna configurables. Son:

- La columna `message`
- Las columnas `parmNNvalue` (donde `NN` = `01`, `02`, `03`, `04` o `05`)

- La columna `xml`

Nota – Las columnas del registro de auditoría se describen en "Esquema de la base de datos" en la página 355.

Los límites de longitud de las columnas se pueden cambiar editando el objeto `RepositoryConfiguration` . Encontrará instrucciones para editar el objeto `RepositoryConfiguration` en "Edición de objetos de configuración de Identity Manager" en la página 118.

- Para cambiar el límite de longitud de la columna `message`, modifique el valor de `maxLogMessageLength`.
- Para cambiar el límite de longitud de la columna `parmNNvalue`, modifique el valor de `maxLogParmValueLength`. El mismo valor límite se aplica a las cinco columnas. No es posible definir valores de longitud de columna distintos.
- Para cambiar el límite de longitud de la columna `xml`, modifique el valor de `maxLogXmlLength`.

Reinicie el servidor para que los nuevos valores surtan efecto.

Los valores de límite de longitud de columna indicados en el objeto `RepositoryConfiguration` determinan la cantidad máxima de datos que pueden almacenarse en una columna. Si los datos que se van a almacenar superan estos valores de configuración, Identity Manager trunca los datos. Para obtener más información, consulte "Truncamiento del registro de auditoría" en la página 358.

Si aumenta el valor de longitud de columna en el objeto `RepositoryConfiguration`, compruebe también si el valor de tamaño de columna en la base de datos es al menos igual al tamaño configurado en dicho objeto.

Supresión de registros del registro de auditoría

Conviene truncar el registro del sistema periódicamente para evitar que alcance un tamaño excesivo. Utilice Tarea de mantenimiento de AuditLog para programar una tarea que suprima los registros viejos del registro de auditoría.

1. **En la interfaz de administración, seleccione Tareas del servidor → Administrar programación.**
2. **Dentro de la sección Tareas disponibles para programación, haga clic en Tarea de mantenimiento de AuditLog.**

   Aparece la página Crear nueva programación de tareas Tarea de mantenimiento de AuditLog.

3. **Rellene el formulario y pulse Guardar.**

Uso de publicadores de auditoría personalizados

Identity Manager puede enviar eventos de auditoría a publicadores de auditoría personalizados.

Hay disponibles los siguientes publicadores personalizados:

- **Consola**. Imprime los eventos de auditoría en la salida estándar o el error estándar.
- **Archivo**. Escribe los eventos de auditoría en un archivo sin formato.
- **JDBC**. Graba los eventos de auditoría en un almacén de datos JDBC.
- **JMS**. Graba los eventos de auditoría en un tema o una cola de JMS.
- **JMX**. Publica los eventos de auditoría de manera que un cliente JMX (Java Management Extensions) pueda supervisar la actividad del registro de auditoría de Identity Manager.
- **Secuencia de comandos**. Permite usar secuencias de comandos personalizadas para almacenar eventos de auditoría.

Si prefiere crear su propio publicador, consulte "Desarrollo de publicadores de auditoría personalizados" en la página 368.

En esta sección se tratan los temas siguientes:

▼ Para habilitar publicadores de auditoría personalizados

Los publicadores de auditoría personalizados se habilitan en la página Configuración de auditoría.

1 **En la interfaz de administración, seleccione Configurar en el menú principal y después Auditoría en el menú secundario.**

Aparece la página Configuración de auditoría.

2 **Seleccione la opción Utilizar publicador personalizado al final de la página.**

Se abre una tabla con los publicadores de auditoría actualmente configurados.

3 **Para configurar un publicador de auditoría nuevo, seleccione el tipo de publicador personalizado en el menú desplegable Nuevo publicador.**

Rellene el formulario Configurar nuevo publicador de auditoría. Pulse Aceptar.

4 **Importante. Pulse Guardar para guardar el nuevo publicador de auditoría.**

Los tipos de publicadores de consola, archivo, JDBC y secuencia de comandos

Para habilitar los publicadores de auditoría de consola, archivo, JDBC o secuencia de comandos, siga los pasos indicados en el apartado "Para habilitar publicadores de auditoría personalizados" en la página 360. Seleccione el tipo de publicador adecuado en el menú desplegable Nuevo publicador.

Rellene el formulario Configurar nuevo publicador de auditoría. Para cualquier cuestión sobre el formulario, consulte los elementos i-Help y la ayuda en línea.

- El publicador de auditoría de consola imprime los eventos de auditoría en la salida estándar o en el error estándar.
- El publicador de auditoría de archivo escribe los eventos de auditoría en un archivo sin formato.
- El publicador de auditoría JDBC graba los eventos de auditoría en un almacén de datos JDBC.
- El publicador de auditoría de secuencia de comandos permite crear secuencias de comandos personalizadas en JavaScript o BeanShell para almacenar eventos de auditoría.

El tipo de publicador JMS

El publicador personalizado JMS de registro de auditoría permite publicar registros de eventos de auditoría en un tema o una cola de JMS (Java Message Service).

¿Por qué utilizar JMS?

Publicar en JMS ofrece más flexibilidad de correlación en los entornos con varios servidores de Identity Manager. Además, JMS puede utilizarse en los casos que presentan restricciones para utilizar el publicador de registro de auditoría en archivo, como los entornos de Windows que impiden que una herramienta de informes cliente acceda al registro mientras se está ejecutando el servidor.

JMS aporta diversas ventajas en los entornos con varios servidores:

- El almacén de mensajes de JMS centraliza (y simplifica) el almacenamiento y la recuperación de mensajes.
- La arquitectura de JMS no restringe el número de clientes que pueden acceder al servicio.
- El protocolo JMS es fácil de transmitir a través de servidores de seguridad y otra infraestructura de red.

¿Punto a punto o publicar y suscribir?

Java Message System ofrece dos modelos de mensajería: el modelo punto a punto o de cola y el modelo publicar y suscribir o de temas. Identity Manager admite ambos modelos.

En el modelo punto a punto, un productor envía los mensajes a una cola determinada y un consumidor lee los mensajes de la cola. En este caso, el productor conoce el destino del mensaje y lo envía directamente a la cola del consumidor.

El modelo punto a punto posee las características siguientes:

- El mensaje llega a un único consumidor.
- No es necesario que el productor se esté ejecutando en el momento en que el destinatario consume el mensaje, ni que el destinatario se esté ejecutando en el momento en que se envía el mensaje.
- El destinatario acusa recibo de cada mensaje procesado.

Por su parte, el modelo de publicar y suscribir permite publicar mensajes en un tema de mensaje específico. Ninguno o más suscriptores pueden registrar su interés en recibir mensajes sobre un tema determinado. Con este modelo, el publicador y el suscriptor se desconocen entre sí. Los tablones de anuncios anónimos son metáforas representativas de este modelo.

El modelo de publicar y suscribir posee las características siguientes:

- Pueden recibir los mensajes múltiples consumidores.
- Hay una dependencia temporal entre publicadores y suscriptores. El publicador debe crear una suscripción a la que puedan abonarse los clientes. Una vez abonados, los suscriptores han de permanecer activos continuamente para poder recibir los mensajes, salvo que se haya definido una suscripción duradera. Si la suscripción es duradera, los mensajes publicados mientras el suscriptor no está conectado se redistribuirán cuando vuelva a conectarse.

Nota – Encontrará información sobre JMS, en `http://www.sun.com/software/products/message_queue/index.xml`

Configuración del tipo de publicador JMS

El publicador de JMS asigna a los eventos de auditoría formato de mensajes de texto de JMS. Según la configuración, estos mensajes de texto se envían a una cola o a un tema. También según la configuración, los mensajes de texto pueden adoptar formato XML o formato de registro universal (UFL).

Para habilitar el tipo de publicador JMS, siga los pasos indicados "Para habilitar publicadores de auditoría personalizados" en la página 360 y seleccione JMS en el menú desplegable Nuevo publicador.

Para configurar el tipo de publicador JMS, rellene el formulario Configurar nuevo publicador de auditoría. Para cualquier cuestión sobre el formulario, consulte los elementos i-Help y la ayuda en línea.

El tipo de publicador JMX

El publicador de registro de auditoría JMX publica los eventos de auditoría de manera que un cliente JMX (Java Management Extensions) pueda supervisar la actividad del registro de auditoría de Identity Manager.

¿Qué es JMX?

Java Management Extensions (JMX) es una tecnología Java que permite administrar y/o supervisar aplicaciones, objetos del sistema, dispositivos y redes orientadas al servicio. La entidad administrada/supervisada se representa mediante objetos llamados MBean (del inglés "Managed Bean", bean administrado).

Implementación del publicador JMX de Identity Manager

El publicador de registro de auditoría JMX de Identity Manager supervisa los eventos del registro de auditoría. Cuando detecta un evento, el publicador JMX ajusta el registro de eventos de auditoría con un MBean y también actualiza un historial temporal (que se conserva en memoria). Por cada evento se envía una pequeña notificación específica al cliente de JMX. Si el evento interesa, el cliente de JMX puede consultar el MBean y ajustar el evento de auditoría para obtener más información.

Nota – Para obtener información sobre los registros de eventos de auditoría, consulte el Javadoc `com.waveset.object.AuditEvent`. El Javadoc está disponible en el kit REF, que se describen en "Desarrollo de publicadores de auditoría personalizados" en la página 368.

Para recuperar información del MBean correcto, se necesita un número de secuencia del historial. Este número se incluye en la notificación del evento.

Cada notificación de evento contiene la siguiente información:

- **Tipo**. Una cadena descriptiva del tipo de evento. La cadena sigue el formato `AuditEvent.<ObjectType>.<Action>` donde `ObjectType` y `Action` se devuelven desde `com.waveset.AuditEvent`. Por ejemplo, si se envía un evento desbloqueado, el tipo sería `AuditEvent.LighthouseAccount.Unlock` .
- **Número de secuencia**. La clave de búfer del historial que se utiliza para consultar información del MBean.

▼ Para configurar el tipo de publicador JMX

1. **Para habilitar el tipo de publicador JMX, siga los pasos indicados "Para habilitar publicadores de auditoría personalizados" en la página 360 y seleccione JMX en el menú desplegable Nuevo publicador.**

2. **Para configurar el tipo de publicador JMX, rellene el formulario Configurar nuevo publicador de auditoría. Para cualquier cuestión sobre el formulario, consulte los elementos i-Help y la ayuda en línea.**

   - **Nombre de publicador**. Escriba un nombre único para el publicador de eventos de auditoría JMX.
   - **Límite de historial**. Cambie el valor predeterminado para indicar el número de elementos de evento que el publicador debe conservar en la memoria. (El valor predeterminado es 100.)

3. **Haga clic en Probar para asegurarse de que el nombre de publicador es aceptable.**

4. **Haga clic en Aceptar. El formulario Configurar nuevo publicador de auditoría se cierra.**

5. **Importante. Pulse Guardar.**

Visualización de eventos de auditoría con un cliente de JMX

Use un cliente de JMX para ver le publicador JMX. Las capturas de pantalla siguientes se han generado con JConsole, que se incluye en JDK 1.5.

Si utiliza JConsole, elija "attach to process" para ver el MBean `IDM:type=AuditLog` . Encontrará información para configurar JConsole con el fin de usarlo como un cliente de JMX en la sección "Viewing JMX Data" de *Sun Identity Manager 8.1 System Administrator's Guide* .

En JConsole, seleccione la ficha "Notifications" para ver los eventos de auditoría. Fíjese en el número de secuencia de la notificación. Necesitará el número de secuencia si quiere consultar más información en el MBean.

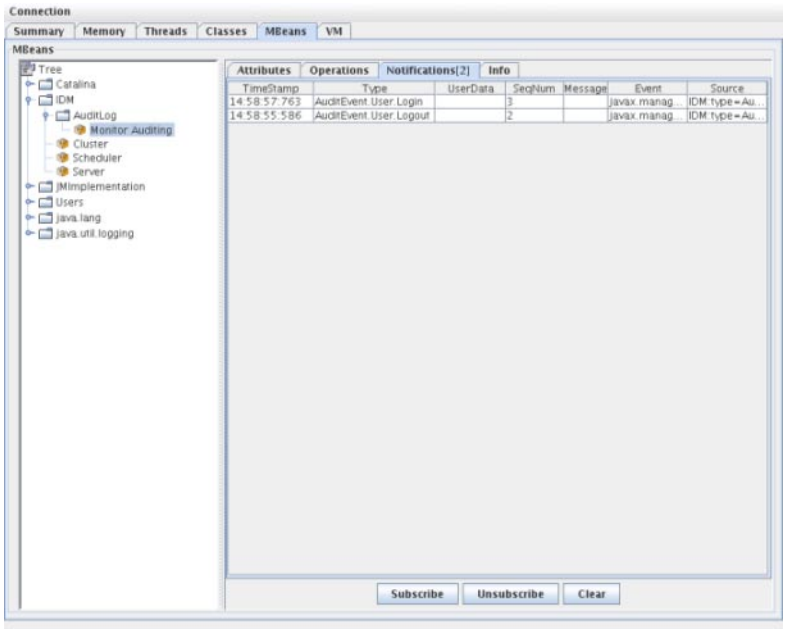


FIGURA 10–1 Visualización de notificaciones de eventos de auditoría JMX en JConsole

Consulta de información adicional en el MBean

En JConsole, seleccione la ficha "Operations". Use el número de secuencia de la notificación para consultar los detalles del evento en el MBean. Cada operación lleva el prefijo 'get' y el único parámetro es el número de secuencia.

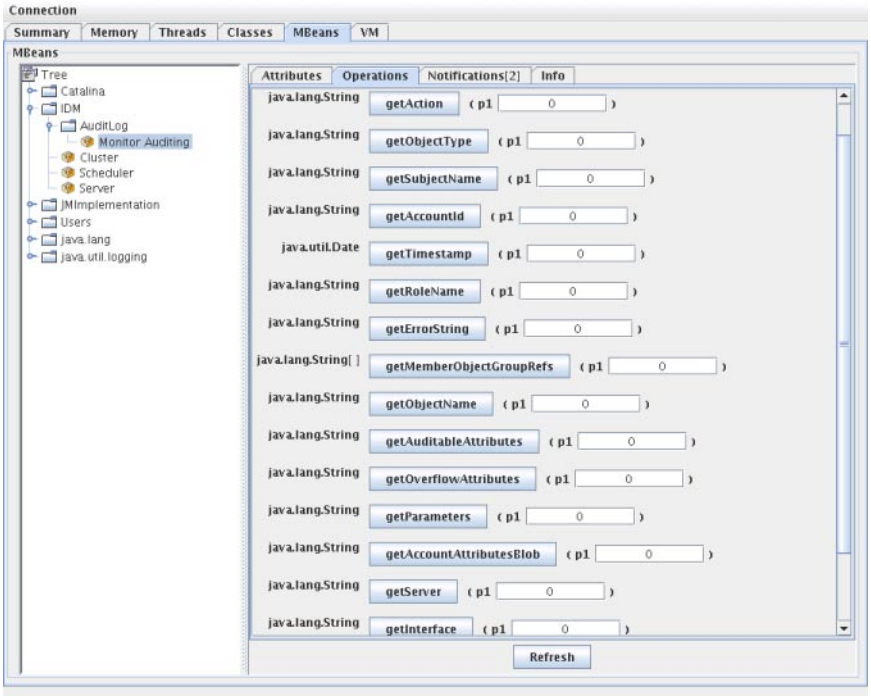


FIGURA 10–2 Consulta de información adicional en el MBean desde JConsole

El MBean es una asignación virtual de uno a uno a la clase `com.waveset.object.AuditEvent`. En la Tabla 10–19 se describe cada atributo/operación que ofrece el MBean.

TABLA 10–19 Descripciones de atributo/operación de MBeanInfo

Atributo/Operación	Descripción
`AccountAttributesBlob`	La lista de atributos modificados.
`AccountId`	ID de cuenta asociado al evento.
`Action`	Acción realizada durante el evento.
`AuditableAttributes`	Los atributos susceptibles de auditoría.
`ErrorString`	Cualquier cadena de error.
`Interface`	La interfaz de auditoría.
`MemberObjectGroupRefs`	Las referencias de grupos de objetos afiliados.
`ObjectName`	El nombre del objeto.
`ObjectType`	El tipo de objeto.

TABLA 10–19 Descripciones de atributo/operación de MBeanInfo *(Continuación)*

Atributo/Operación	Descripción
`OverflowAttributes`	Todo los atributos de desbordamiento.
`Parameters`	Todos los parámetros.
`Reason`	La razón del evento.
`ResourceName`	El recurso asociado al evento.
`RoleName`	El rol asociado al evento.
`SubjectName`	El usuario o servicio asociado al evento.
`Server`	El nombre del servidor para el que se activa el evento.
`Status`	El estado del evento de auditoría.
`Timestamp`	Fecha/hora del evento de auditoría.

En JConsole, seleccione la ficha "Attributes". Los atributos llevan el prefijo `Current` para indicar que contienen el último evento de auditoría enviado al sistema.

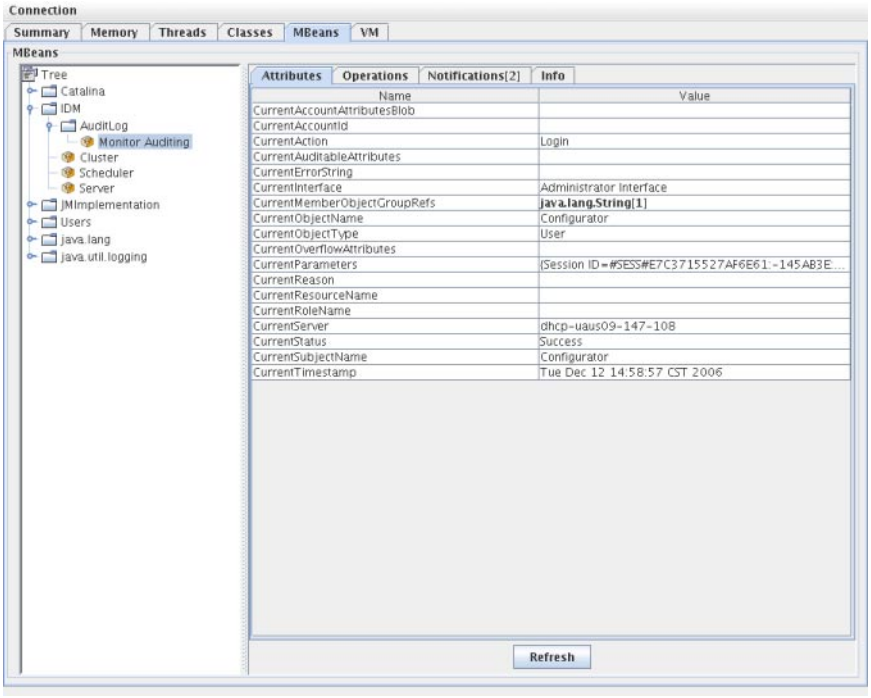


FIGURA 10–3 Visualización de atributos de MBean en JConsole

Desarrollo de publicadores de auditoría personalizados

En esta sección se explica cómo crear un publicador de auditoría personalizado nuevo en Java.

Los publicadores personalizados de consola, archivo y JDBC que se suministran con Identity Manager implementan la interfaz `AuditLogPublisher`. El código fuente de estos publicadores se halla en el kit REF. La documentación de las interfaces también está disponible en el kit REF en formato Javadoc. (Consulte los detalles de la interfaz en el Javadoc.)

Nota – El kit REF (Resource Extension Facility) se encuentra en el directorio `/REF` del CD del producto o en la imagen de instalación.

Animamos a los desarrolladores a que amplíen la clase `AbstractAuditLogPublisher`. Esta clase analiza la configuración y se asegura de que todas las opciones necesarias se hayan suministrado al publicador. (Consulte los publicadores de ejemplo en el kit REF.)

Los publicadores necesitan un constructor `no-arg`.

Ciclo de vida de los publicadores

Un publicador sigue el ciclo de vida siguiente:

1. Se instancia el objeto.
2. El Formateador (en su caso) se define con el método `setFormatter()`.
3. Se suministran las opciones con el método `configure(` *Map*`)`.
4. Se publican los eventos con el método `publish(` *Map, LoggingErrorHandler*`)`.
5. Se termina el publicador con el método `shutdown()`.

Los pasos 1-3 se ejecutan cuando se inicia Identity Manager y siempre que se actualiza la configuración de auditoría. El paso 4 no se produce si no se genera ningún evento de auditoría antes de llamar al cierre.

El método `configure(`*Map* `)` sólo se llama una vez en el mismo objeto de publicador. (No es necesario que el publicador se prepare para los cambios de configuración puntuales.) Una vez actualizada la configuración de auditoría, los publicadores actuales se cierran y se crean los nuevos.

El método `configure()` del paso 3 puede lanzar una excepción `WavesetException`. En tal caso, no se tendrá en cuenta el publicador ni se efectuarán más llamadas a él.

Configuración del publicador

Los publicadores pueden tener varias opciones o ninguna. El método `getConfigurationOptions()` devuelve la lista de opciones que admite el publicador. Las opciones se encapsulan mediante la clase `PublisherOption` (consulte los detalles de esta clase en el Javadoc). El visor de configuración de auditoría invoca este método cuando genera la interfaz de configuración para el publicador.

Identity Manager configura el publicador con el método `configure(` *Map*`)` al iniciarse el servidor y cuando se modifica la configuración de auditoría.

Desarrollo de formateadores

El kit REF incluye el código fuente de los siguientes formateadores:

- `XmlFormatter`. Asigna a los eventos de auditoría formato de cadenas XML.
- `UlfFormatter`. Asigna a los eventos de auditoría formato de registro universal (ULF). Sun Application Server utiliza este formato.

Los formateadores deben implementar la interfaz `AuditRecordFormatter`. Además, necesitan un constructor `no-arg`. Consulte los detalles en el Javadoc incluido con el kit REF.

Registro de publicadores/formateadores

El atributo de auditoría del objeto `#ID#Configuration:SystemConfiguration` ofrece una lista con todos los publicadores y formateadores registrados. En la interfaz de usuario de configuración de auditoría sólo están disponibles esos publicadores y formateadores.

◆ ◆ ◆ CAPÍTULO 11

PasswordSync

PasswordSync detecta los cambios de contraseña de usuario iniciados en los dominios de Windows y reenvía esos cambios a Identity Manager. A continuación, Identity Manager sincroniza los cambios de contraseña con los demás recursos definidos en Identity Manager.

El capítulo se ha organizado como sigue:

¿Qué es PasswordSync?

La funcionalidad PasswordSync mantiene sincronizados los cambios de contraseñas de usuario realizados en dominios de Windows Active Directory con otros recursos definidos en Identity Manager. PasswordSync debe instalarse en cada controlador de dominio dentro de los dominios que vayan a sincronizarse con Identity Manager. PasswordSync debe instalarse por separado de Identity Manager.

PasswordSync consta de una DLL (`lhpwic.dll`) que reside en cada controlador de dominio. Esta DLL recibe las notificaciones de actualización de contraseña procedentes de Windows, las cifra y las envía por HTTPS al servlet de PasswordSync. El servlet de PasswordSync se halla en el servidor de aplicaciones donde se ejecuta Identity Manager.

Nota – Aunque es preferible utilizar HTTPS, también se admite HTTP.

El servlet de PasswordSync convierte la notificación a un formato comprensible para Identity Manager. A continuación, el servlet envía el cambio de contraseña (aún cifrado) a Identity Manager con uno de los siguientes métodos:

- **Método directo**. El servlet comunica el cambio de contraseña directamente a Identity Manager utilizando clases nativas de Identity Manager. (Consulte "¿Qué es PasswordSync?" en la página 371.)

  El método de conexión directa sólo se recomienda para los pequeños entornos poco complejos que únicamente precisan entregar mensajes a un sistema, sin necesidad de garantía de entrega. (Si por algún motivo falla la entrega del mensaje, éste se perderá. No es posible entregar una copia de seguridad.)
- **Método JMS**. El servlet envía la información de contraseña a Identity Manager utilizando JMS (Java Message Service). Con JMS, el servlet envía los cambios de contraseña a la cola de mensajes de JMS. Por su parte, el adaptador de recursos del receptor de JMS de Identity Manager comprueba si hay nuevos mensajes en la cola. Si en la cola aguarda un mensaje de cambio de contraseña, el adaptador del receptor de JMS lo quita de la cola y lo importa a Identity Manager. (Consulte la Figura 11–2.)

  El método JMS se recomienda para entornos más complejos con grandes exigencias de volumen, necesidad de entregar mensajes a diversos sistemas y garantía de entrega de los mensajes. Puede asignarse ata disponibilidad a la cola de mensajes de JMS. En tanto que un mensaje llegue a la cola, si falla la entrega a Identity Manager, la cola conservará el cambio hasta que sea posible entregar el mensaje a Identity Manager.

  JMS se debe instalar y configurar por separado.

En la Figura 11–1 se representa una conexión directa. En esta configuración, el servlet de PasswordSync envía los mensajes de actualización directamente a Identity Manager

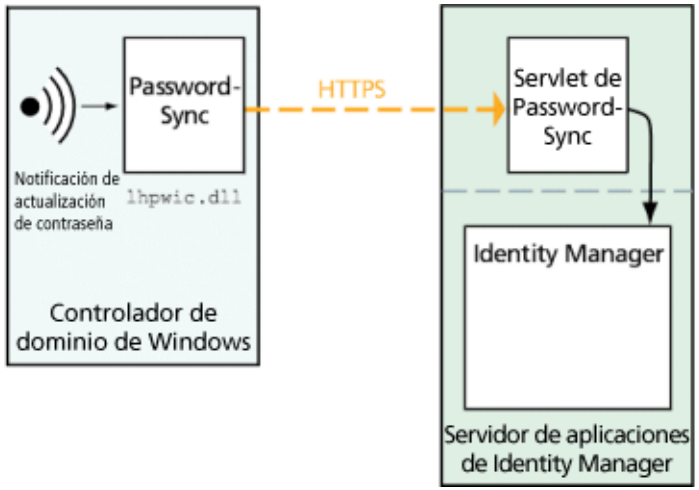


FIGURA 11–1 Diagrama lógico de PasswordSync (conexión directa)

En la Figura 11–2 se representa una conexión JMS. En esta configuración, el servlet de PasswordSync envía los mensajes de actualización a la cola de mensajes de JMS. El adaptador de recursos del receptor de JMS de Identity Manager comprueba periódicamente si hay nuevos mensajes en la cola (flecha azul claro en el diagrama). La cola responde enviando los mensajes a Identity Manager (flecha azul más oscura).

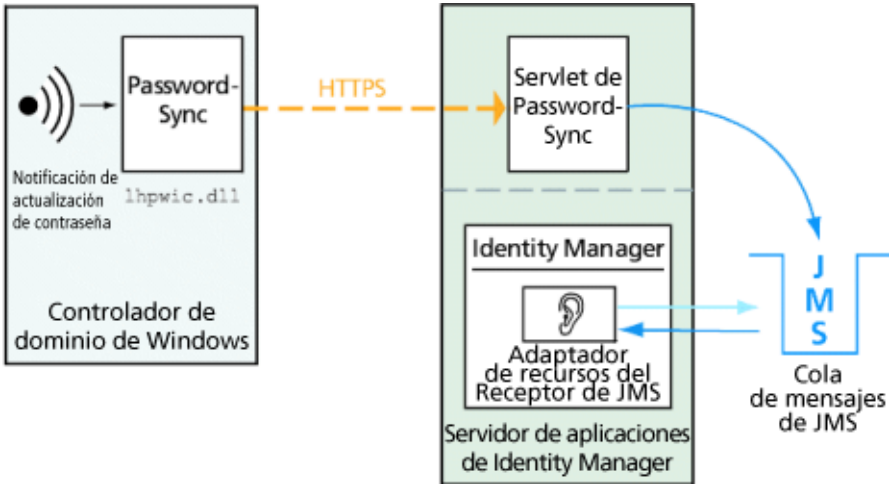


FIGURA 11–2 Diagrama lógico de PasswordSync (conexión JMS)

Cuando Identity Manager recibe una notificación de cambio de contraseña, la descifra y procesa el cambio mediante una tarea de flujo de trabajo. La contraseña se actualiza en todos los recursos asignados al usuario, y un servidor SMTP le notifica por correo electrónico el estado del cambio de contraseña.

Nota – Windows sólo envía una notificación de actualización si el cambio de contraseña es satisfactorio. Si una solicitud de cambio de contraseña no cumple la directiva de contraseñas del dominio, Windows la rechaza y no se envían datos de sincronización a Identity Manager.

En la Figura 11–3 se muestra cómo Identity Manager inicia un flujo de trabajo y envía correo electrónico al usuario tras recibir una notificación de actualización de contraseña.

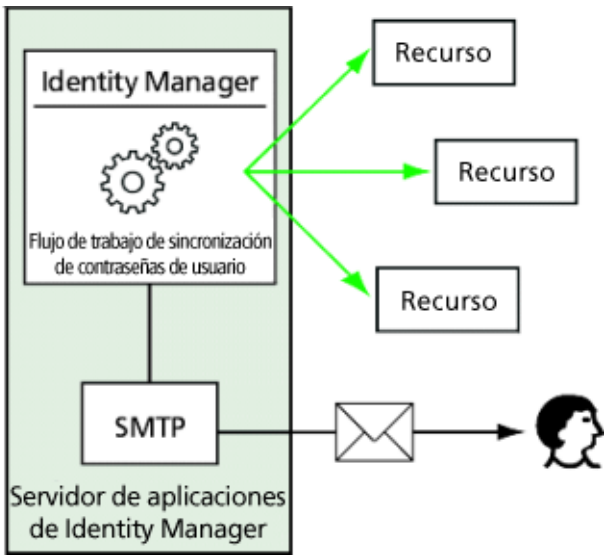


FIGURA 11–3 PasswordSync activa un flujo de trabajo

Nota – PasswordSync descarta todas las notificaciones de cambio de contraseña para los nombres de cuenta terminados en $ (símbolo de dólar). Los nombres de cuenta terminados en $ se consideran cuentas físicas de Windows. Todos los nombres de cuenta de usuario terminados en símbolo de dólar quedan sin reenviar a Identity Manager.

Antes de la instalación

La funcionalidad PasswordSync puede configurarse sólo en controladores de dominio de Windows 2008, Windows 2003 y Windows 2000. (La compatibilidad con los controladores de dominio de Windows NT cesó en la versión 8.0 de Identity Manager.) PasswordSync debe instalarse en cada controlador de dominio principal y de copia de seguridad dentro de los dominios que vayan a sincronizarse con Identity Manager. Se recomienda encarecidamente configurar PasswordSync para HTTPS.

Nota – Las versiones de PasswordSync anteriores a la 7.1.1 deben actualizarse al menos a la versión 7.1.1 en todos los controladores de dominio.

La compatibilidad del servlet rpcrouter2 se ha desaprobado en la versión 8.0 y se eliminará en una versión futura. PasswordSync admite el nuevo protocolo desde la versión 7.1.1

Si se utiliza JMS, PasswordSync requiere conectividad con un servidor de JMS. Consulte la sección que trata sobre el adaptador de recursos del Receptor de JMS en la guía *Sun Identity Manager 8.1 Resources Reference* para obtener más información sobre los requisitos del sistema JMS.

Además, PasswordSync requiere:

- Instalar al menos Microsoft .NET 1.1 en cada controlador de dominio.
- Suprimir todas las versiones anteriores de PasswordSync;.

Estos requisitos se detallan en las próximas secciones.

Instalación de Microsoft .NET 1.1

Para usar PasswordSync, debe instalar al menos Microsoft .NET 1.1 Framework. Esta estructura se instala de manera predeterminada cuando se utiliza un controlador de dominio de Windows 2003. Microsoft .NET 2.0 Framework se instala de manera predeterminada en los controladores de dominio de Windows 2008. Con los controladores de dominio de Windows 2000 no se instala ninguna estructura predeterminada. Puede descargar el kit de herramientas desde el centro de descargas de Microsoft:

`http://www.microsoft.com/downloads`

Nota –

- Escriba **`.NET Framework Redistributable`** en el campo de búsqueda por palabras clave para encontrar rápidamente el kit de Framework.
- El kit de herramientas instala .NET Framework.

Configuración de PasswordSync para SSL

Aunque la información delicada se cifra antes de enviarla al servidor de Identity Manager, Sun Microsystems recomienda configurar PasswordSync para que use una conexión SSL segura (es decir, HTTPS).

Encontrará información para instalar los certificados SSL importados en el siguiente artículo práctico de la base de conocimientos de Microsoft:

`http://support.microsoft.com/kb/816794`

Una vez instalado PasswordSync, puede verificar si la conexión SSL está bien configurada especificando una URL de HTTPS en el cuadro de diálogo de configuración de PasswordSync. Encontrará instrucciones en "Verificación de la configuración" en la página 402.

Desinstalación de versiones anteriores de PasswordSync;

Es necesario suprimir todas las versiones anteriores de PasswordSync; que haya instaladas antes de instalar una nueva.

- Si la versión anterior de PasswordSync instalada admite el instalador `IdmPwSync.msi`, puede suprimirla mediante la utilidad normal de Windows para agregar y guitar programas.
- Si la versión anterior de PasswordSync instalada *no* admite el instalador `IdmPwSync.msi`, quítela con el desinstalador de InstallAnywhere.

Instalación y configuración de PasswordSync en Windows

Esta sección contiene información e instrucciones para instalar y configurar PasswordSync.

Esta información se ha dividido como sigue:

▼ Para instalar la aplicación de configuración de PasswordSync

El procedimiento siguiente sirve para instalar la aplicación de configuración de PasswordSync.

Nota – PasswordSync debe instalarse en cada controlador de dominio dentro de los dominios que vayan a sincronizarse con Identity Manager.

No olvide desinstalar todas las versiones anteriores de PasswordSync antes de continuar.

---

1 **Desde el soporte de instalación de Identity Manager:**

- Si va a instalar en una versión de 32 bits de Windows, haga doble clic en `pwsync\IdmPwSync_x86.msi`.
- Si va a instalar en una versión de 64 bits de Windows, haga doble clic en `pwsync\IdmPwSync_x86.msi`.

Se abre el asistente de instalación con la ventana de bienvenida, que contiene los botones siguientes:

- **Cancel**. Púlselo para salir del asistente en cualquier momento sin guardar los cambios.
- **Back**. Sirve para retroceder a un cuadro de diálogo anterior.
- **Next**. Sirve para avanzar al próximo cuadro de diálogo.

2 **Lea la información de la pantalla de bienvenida y pulse Next para acceder a la ventana Choose Setup Type.**

3 **Seleccione Typical o Complete para instalar el paquete completo de PasswordSync, o bien Custom para elegir qué componentes se instalan. Haga clic en Next para continuar.**

4 **Cuando aparezca la ventana Ready to Install, seleccione Install para instalar el producto.**

5 **Aparece una última ventana. Marque la casilla Launch Configuration Application para poder empezar a configurar Password Sync y después pulse Finish para completar el proceso de instalación.**

Encontrará instrucciones para configurar PasswordSync en el Capítulo 11, “PasswordSync”.

Nota – Se abre un cuadro de diálogo donde se le indica que debe reiniciar el sistema para que se apliquen los cambios. No es necesario reiniciar hasta después de configurar PasswordSync, pero sí hay que reiniciar el controlador de dominio antes de implementar PasswordSync.

Los archivos que se instalan en cada controlador de dominio se describen dentro de “Instalación y configuración de PasswordSync en Windows” en la página 376.

Componente instalado	Descripción
`%$INSTALL_DIR$%\configure.exe`	Programa de configuración de PasswordSync
`%$INSTALL_DIR$%\configure.exe.manifest`	Archivo de datos para el programa de configuración
`%$INSTALL_DIR$%\passwordsyncmsgs.dll`	DLL que controla los mensajes de PasswordSync
`%SYSTEMROOT%\SYSTEM32\lhpwic.dll`	DLL de notificación de contraseñas que implementa la función `PasswordChangeNotify()` de Windows

▼ Para configurar PasswordSync

Si ejecuta la aplicación de configuración desde el instalador, la aplicación mostrará las pantallas de configuración como un asistente. Una vez completado el asistente, siempre que vuelva a ejecutar la aplicación de configuración de PasswordSync podrá navegar por las pantallas seleccionando una ficha.

1 Inicie la aplicación de configuración de PasswordSync (si aún no se está ejecutando).

De manera predeterminada, la aplicación de configuración se instala dentro de Archivos de programa → Sun Identity Manager PasswordSync → Configuration.

Nota – Si no tiene intención de utilizar JMS, ejecute la aplicación de configuración desde una línea de comandos, sin olvidar incluir la marca `-direct` así:

```
C:\InstallDir\Configure.exe -direct
```

Aparece el cuadro de diálogo del asistente de configuración de PasswordSync (observe la Figura 11–4).

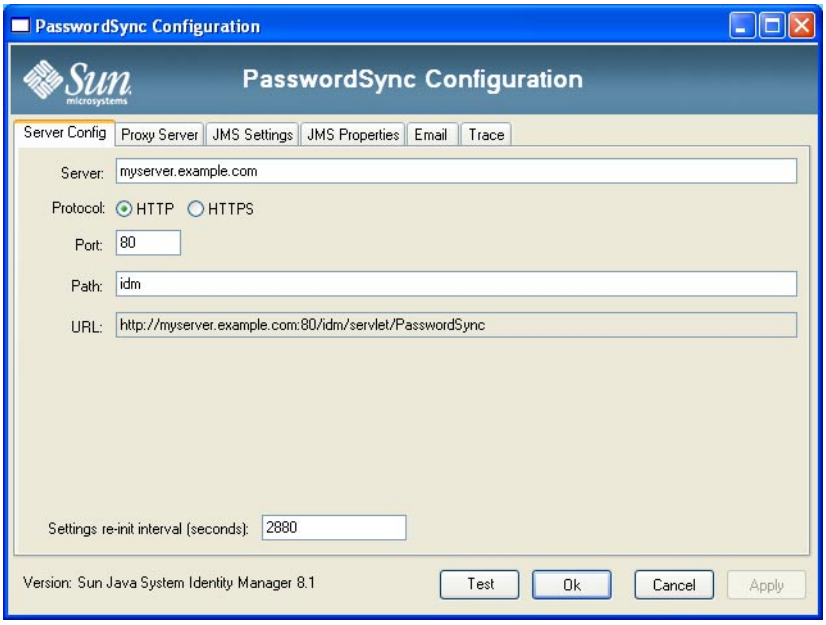


FIGURA 11–4 Asistente de configuración de PasswordSync

2 Edite los campos necesarios de este cuadro de diálogo.

Estos campos incluyen:

- **Server**, donde debe introducirse el nombre de host completo o dirección IP donde está instalado Identity Manager.
- **Protocol**, que indica si se deben establecer conexiones seguras con Identity Manager.

PasswordSync permite configurar el comportamiento de verificación de certificados para las conexiones HTTPS. Si habilita HTTPS, aparecen estas opciones:

- **Allow revoked certificates**. Este valor de configuración adopta el valor del registro `securityIgnoreCertRevoke` durante la conexión. De manera predeterminada, PasswordSync no omite los problemas de revocación y el valor de registro `securityIgnoreCertRevoke` se configura en 0.

  Si prefiere que PasswordSync no haga caso a los mensajes de revocación de certificados, marque esta casilla (o defina el valor de registro `SECURITY_FLAG_IGNORE_REVOCATION` en 1).

- **Allow invalid certificates**. Este valor afecta a las opciones `SECURITY_FLAG_IGNORE_CERT_CN_INVALID`, `SECURITY_FLAG_IGNORE_CERT_DATE_INVALID` y `SECURITY_FLAG_IGNORE_UNKNOWN_CA` durante la conexión. De manera predeterminada, PasswordSync no admite los certificados no válidos y los valores de registro se configuran en 0.

  Si marca esta casilla o define en 1 el valor de registro `securityAllowInvalidCert`, PasswordSync podrá utilizar los certificados que no superen diversas verificaciones de seguridad. *Se desaconseja* habilitar esta opción en los entornos de producción.

Nota – Estos valores no se muestran con el tipo de protocolo HTTP ni afectan a la configuración de HTTP.

- **Port** indica un puerto disponible para el servidor. El puerto predeterminado para HTTP es 80. El puerto predeterminado para HTTPS es 443.
- **Path** especifica la ruta de acceso a Identity Manager en el servidor de aplicaciones.
- La **URL** se genera concatenando los demás campos. El valor no se puede editar en el campo URL.
- **Settings re-init interval (seconds)** especifica la frecuencia con que la `dll` de PasswordSync debe volver a leer los valores de configuración del registro. El valor predeterminado es 2880 segundos u 8 horas.

Nota – El asistente de configuración de PasswordSync muestra el valor en segundos, pero se almacena en milisegundos en el registro.

La `dll` de PasswordSync lee los valores de configuración en el registro mientras está activa. El valor del intervalo se almacena en el valor del registro `reinitIntervalMilli`.

Las contraseñas no se pueden sincronizar mientras se actualizan los valores de configuración, lo que puede ocasionar un pequeño retraso al procesar los cambios de contraseña. Dicho retraso suele ser inferior a un segundo. PasswordSync procesa directamente todos los cambios de contraseña recibidos durante una actualización una vez

que se ha completado ésta. Asimismo, PasswordSync no procesa las actualizaciones de los valores de configuración mientras se están sincronizando contraseñas. La actualización se reprograma y se realiza más tarde.

3 Pulse Next para acceder a la página Proxy Server Configuration (Figura 11–5) y editar los campos necesarios.

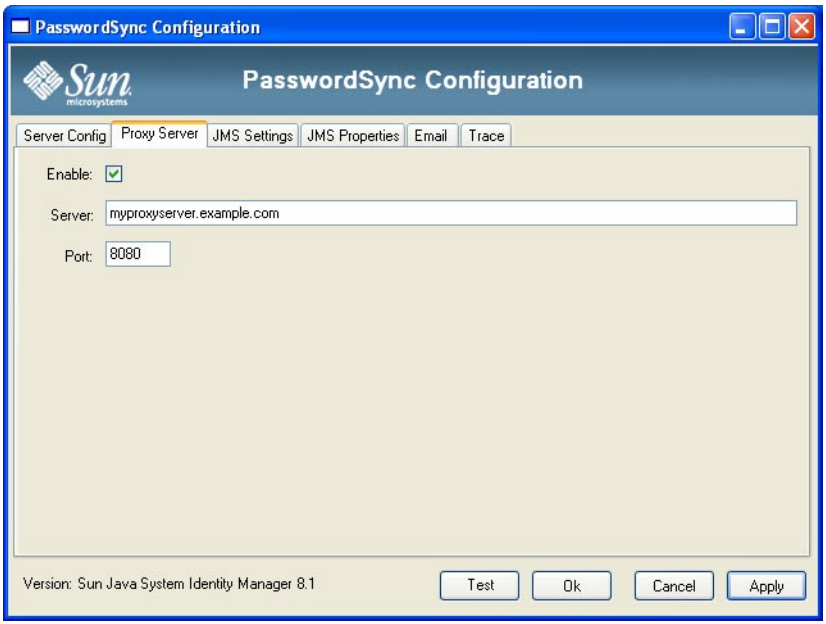


FIGURA 11–5 Cuadro de diálogo Proxy Server del asistente de PasswordSync

Estos campos incluyen:

- **Enable**. Indique si es necesario un servidor proxy.
- **Server**. Debe especificar el nombre de host completo o la dirección IP del servidor proxy.
- **Port**. Indique un número de puerto disponible para el servidor. (El puerto proxy predeterminado es 8080 y el puerto HTTPS predeterminado es 443.)

4 Pulse Siguiente.

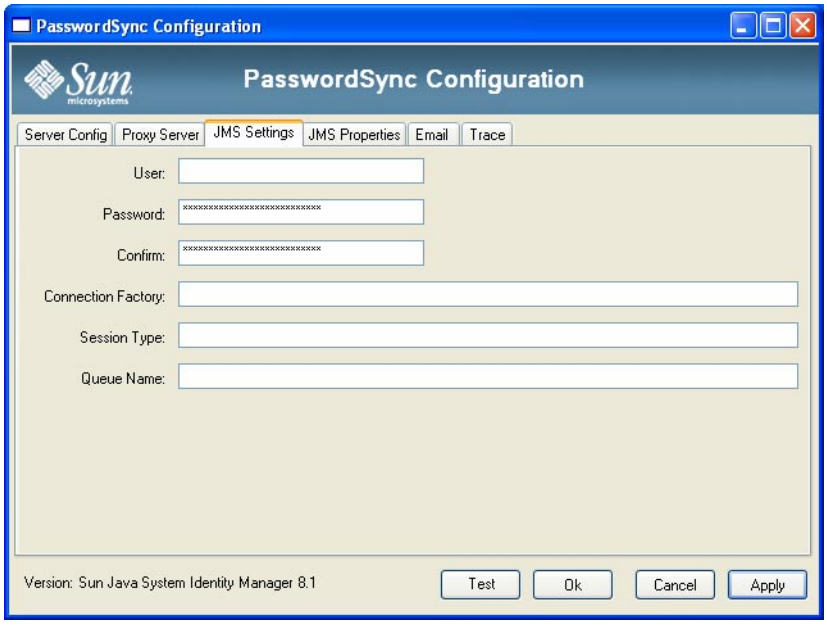


FIGURA 11–6 Cuadro de diálogo JMS Settings del asistente de PasswordSync

Cuando aparezca el cuadro de diálogo JMS Settings (Figura 11–6), realice una de estas acciones:

- Edite los campos siguientes según convenga:
  - **User** especifica el nombre del usuario de JMS que incluye mensajes nuevos en la cola.
  - **Password** y **Confirm** sirven para especificar la contraseña del usuario de JMS.
  - **Connection Factory** indica el nombre de la fábrica de conexiones de JMS que debe usarse. Esta fábrica debe existir previamente en el sistema JMS.
  - En la mayoría de los casos, **Session Type** debe definirse en `LOCAL` para indicar que es utilizará una transacción de sesiones local. La sesión se confirmará tras recibir cada mensaje. Otros posibles valores son `AUTO`, `CLIENT` y `DUPS_OK`.
  - **Queue Name** especifica el nombre de búsqueda del destino para los eventos de sincronización de contraseñas.
- Si no prevé utilizar JMS y ha ejecutado el asistente de configuración con la marca `-direct`, pulse Next para abrir el cuadro de diálogo de usuario. Vaya al paso 7Figura 11–7.

5 Pulse Next para acceder al cuadro de diálogo JMS Properties (Figura 11–7).

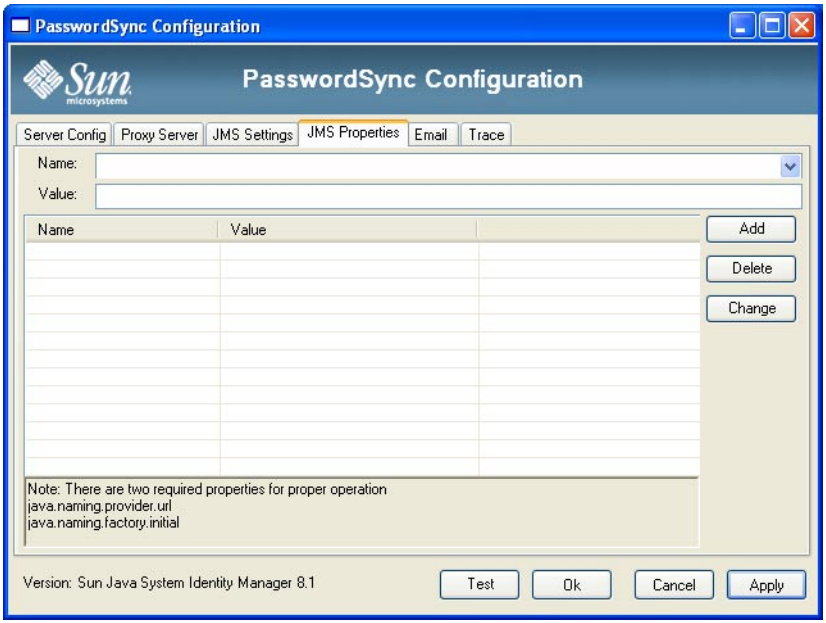


FIGURA 11–7 Cuadro de diálogo JMS Properties del asistente de PasswordSync

El cuadro de diálogo JMS Properties sirve para definir el conjunto de propiedades utilizadas para crear el contexto JNDI inicial. Debe definir los siguientes pares de nombre/valor:

- `java.naming.provider.url`: Especifique la URL de la máquina donde se ejecuta el servicio JNDI.
- `java.naming.factory.initial`: Indique el nombre de clase (incluyendo el paquete) del contexto de fábrica inicial para el proveedor de servicios JNDI.

  El menú desplegable Name contiene una lista de clases del paquete `java.naming`. Seleccione una clase o tipo en un nombre de clase, después escriba el valor correspondiente en el campo Value.

6 Si no prevé utilizar JMS y ha ejecutado el asistente de configuración con la marca `-direct`, configure la ficha User. De lo contrario, omita este paso y continúe en el siguiente.

Para configurar la ficha User, edite los campos pertinentes.

- **Account ID**. Escriba el nombre de usuario que se empleará en la conexión con Identity Manager.
- **Password**. Escriba la contraseña que se empleará en la conexión con Identity Manager.

7 Pulse Next para acceder al cuadro de diálogo Email (Figura 11–8) y edite los campos necesarios.

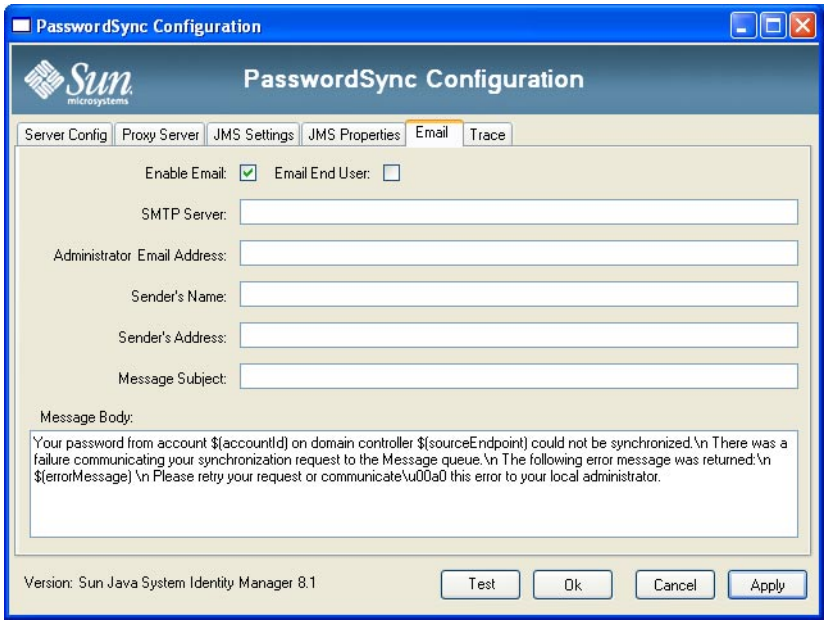


FIGURA 11–8 Cuadro de diálogo Email del asistente de PasswordSync

Si desea enviar una notificación por correo electrónico cuando el cambio de contraseña de un usuario no se sincronice satisfactoriamente debido a un error de comunicación u otro error fuera de Identity Manager, use las siguientes opciones del cuadro de diálogo Email para configurar la notificación y el correo electrónico.

- **Enable Email**. Márquela para habilitar el correo electrónico.
- **Email End User**. Marque esta casilla para que el usuario reciba notificaciones. De lo contrario, sólo se notificará al administrador.
- **SMTP Server**. Introduzca el nombre completo o la dirección IP del servidor SMTP que se debe usar al enviar notificaciones de fallo.
- **Administrator Email Address**. Escriba la dirección de correo electrónico donde desea enviar las notificaciones.
- **Sender's Name**. Escriba el nombre coloquial del remitente.
- **Sender's Address**. Escriba la dirección de correo electrónico del remitente.
- **Message Subject**. Introduzca la línea de asunto de todas las notificaciones.
- **Message Body**. Escriba el texto de la notificación.

El cuerpo del mensaje puede contener las siguientes variables:

- `$(accountId)`: ID de cuenta del usuario que intenta cambiar la contraseña.
- `$(sourceEndpoint)`: Nombre de host del controlador de dominio donde está instalado el notificador de contraseñas, para facilitar la localización de las máquinas con problemas.
- `$(errorMessage)`: Mensaje de error explicativo del error que ha ocurrido.

8 Haga clic en la ficha Trace Figura 11–9.

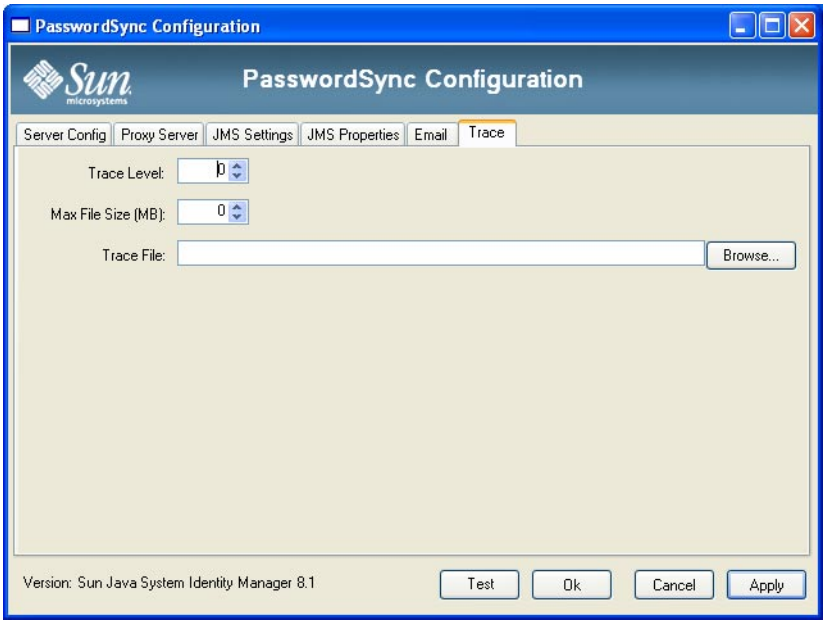


FIGURA 11–9 Ficha Trace

Defina los campos siguientes:

- **Trace Level**.
- **Max File Size (MB)**.
- **Trace File**.

9 Pulse Finish para guardar los cambios.

Si vuelve a ejecutar la aplicación de configuración, aparece un grupo de fichas en lugar de un asistente. Para ver la aplicación en forma de asistente, introduzca este comando en la línea de comandos:

`C:\`*`InstallDir`*`\Configure.exe -wizard`

Para verificar la configuración de PasswordSync, consulte "Verificación de la configuración" en la página 402.

Instalación silenciosa de PasswordSync

El instalador de PasswordSync se puede configurar para realizar una instalación silenciosa. Para utilizar esta función, primero debe grabar los parámetros de configuración en un archivo durante la instalación de PasswordSync. Las instalaciones que se efectúen posteriormente se remitirán al archivo y reproducirán los valores de configuración.

Nota – Si desea utilizar el procedimiento de instalación silenciosa, deberá instalar el producto completo en cada servidor donde vaya a usarse. La grabación y reproducción de los valores de configuración depende de la aplicación de configuración que se va a instalar en el sistema.

El proceso de instalación silenciosa emplea una utilidad de Windows denominada `msiexec` , que instala los archivos `.msi` desde la línea de comandos.

Escriba `msiexec /?` en una solicitud de comandos para obtener información sobre el funcionamiento de esta utilidad.

La documentación también está disponible en la web de Microsoft. Por ejemplo, la documentación sobre el uso de `msiexec` en Windows Server 2003 se encuentra en `http://technet.microsoft.com/en-us/library/cc759262.aspx`.

▼ Para capturar parámetros de instalación en un archivo de configuración

Siga estas instrucciones para instalar PasswordSync mediante el asistente de instalación. La utilidad de configuración captura los parámetros de configuración y los graba en un archivo XML.

Antes de empezar Antes de instalar, quite las versiones anteriores de PasswordSync.

1. **Vaya al directorio que contiene el archivo (`.msi`) de instalación de PasswordSync.**

   Encontrará más información en "Para instalar la aplicación de configuración de PasswordSync" en la página 377.

2. **Escriba lo siguiente en la solicitud de comandos. En los argumentos y los valores se diferencian mayúsculas de minúsculas.**

   `msiexec /i` *pwSyncInstallFile* `CONFIGARGS="-writexml` *fullPathToFile*`"`

   donde:

- **pwSyncInstallFile** es el archivo de instalación de PasswordSync. (`IdmPwSync_86.msi` o `IdmPwSync_x64.msi`).
- **fullPathToFile** especifica dónde guardar el archivo XML.

Por ejemplo:

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-writexml c:\tmp\myconfig.xml"
```

3 **Instale el producto.**

▼ Para instalar PasswordSync en modo silencioso

Antes de empezar

- Debe haber creado un archivo XML de configuración para la instalación. Consulte las instrucciones en "Para capturar parámetros de instalación en un archivo de configuración" en la página 386.
- Antes de instalar, quite las versiones anteriores de PasswordSync.

1 **Copie el archivo XML de configuración para la instalación en una ubicación donde pueda leerlo el instalador.**

2 **Escriba lo siguiente en la solicitud de comandos. En los argumentos y los valores se diferencian mayúsculas de minúsculas.**

```
msiexec /i pwSyncInstallFile ADDLOCAL="installFeature" CONFIGARGS="-readxml fullPathToFile"
 INSTALLDIR="installDir" /q
```

donde:

- **pwSyncInstallFile** es el archivo de instalación de PasswordSync. (`IdmPwSync_86.msi` o `IdmPwSync_x64.msi`).
- **installFeature** especifica las funciones de PasswordSync que se instalan. Elija una de estas opciones:
  - `MainProgram`: Sólo se instala el archivo `.dll` del interceptor.
  - `Configuration`: Sólo se instalar la aplicación de configuración.
  - `ALL`: Instala el producto completo.

  Si no se especifica nada, de manera predeterminada se utiliza `MainProgram` cuando se ha incluido la opción `/q`.
- **fullPathToFile** especifica la ruta de acceso al archivo XML de configuración.
- **installDir** especifica la ruta completa a un directorio de instalación personalizado. Opcional.
- **/q** especifica una instalación no GUI que reinicia automáticamente el servidor al terminar. Si no se incluye, se verá el asistente de instalación, pero la configuración se efectuará con los valores predefinidos. Opcional.

Ejemplos:

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-readxml c:\tmp\myconfig.xml"

msiexec /i IdmPwSync_x86.msi ADDLOCAL="MainProgram"
CONFIGARGS="-readxml c:\tmp\myconfig.xml" /q

msiexec /i IdmPwSync_x64.msi ADDLOCAL="Complete"
CONFIGARGS="-readxml c:\tmp\myconfig.xml"
INSTALLDIR="C:\Program Files\Sun Microsystems\MyCustomInstallDirectory" /q
```

Implementación de PasswordSync en el servidor de aplicaciones

Una vez que ha instalado PasswordSync en los controladores de dominio de Windows, debe efectuar algunas otras operaciones en el servidor donde se ejecuta Identity Manager.

No es preciso instalar el servlet de PasswordSync en el servidor de aplicaciones. Se instala automáticamente a la vez que Identity Manager

Sin embargo, para finalizar la implementación de PasswordSync debe realizar las siguientes acciones en Identity Manager:

- Agregar y configurar el adaptador del Receptor de JMS (si utiliza JMS).
- Implementar el flujo de trabajo de sincronización de contraseñas de usuario.
- Configurar las notificaciones.

Adición y configuración del adaptador del Receptor de JMS

Si el servlet de PasswordSync utiliza JMS para enviar mensajes a Identity Manager, debe agregar el adaptador del Receptor de JMS de Identity Manager. El adaptador de recursos del Receptor de JMS verifica periódicamente la cola de mensajes de JMS para comprobar si contiene mensajes incluidos por el servlet de PasswordSync. Si la cola contiene un mensaje nuevo, lo envía a Identity Manager para que lo procese.

▼ Para agregar el adaptador de recursos del Receptor de JMS

1 **Inicie la sesión en la interfaz de administración de Identity Manager ("Interfaz de administración de Identity Manager" en la página 37).**

2 **Seleccione Recursos → Configurar tipos en menú principal.**

Aparece la página Configurar recursos administrados tal como muestra la Figura 11–10.

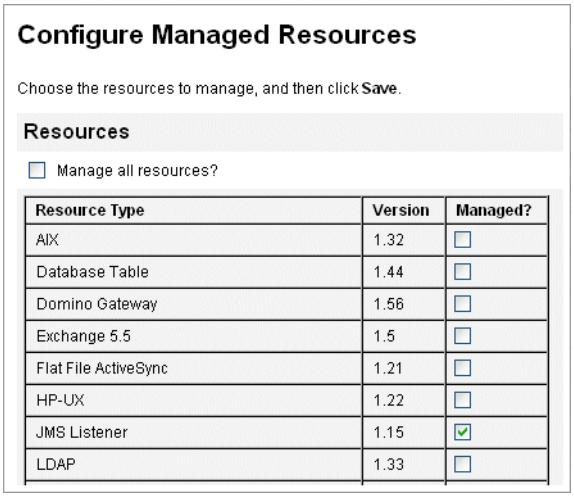


FIGURA 11–10 Página Configurar recursos administrados.

3 **Asegúrese de que esté seleccionada la casilla Receptor de JMS en la columna ¿Administrado?, como ilustra la Figura 11–10.**

Si no está seleccionada dicha casilla, márquela y pulse Guardar.

4 **Elija Listar recursos en el menú secundario.**

5 **Busque el menú desplegable Acciones de tipo de recurso y elija Nuevo recurso.**

Aparece la página Nuevo recurso.

6 **Para agregar el adaptador del Receptor de JMS, seleccione Receptor de JMS en el menú desplegable (como muestra la Figura 11–11) y pulse Nuevo.**

FIGURA 11–11 El asistente de Nuevo recurso

7 Configure los valores siguientes en la página Parámetros de recurso y después pulse Siguiente.

- **Tipo de destino**. Indica el tipo de destino, que suele estar configurado en Cola. (Los temas raramente son importantes, porque hay un único suscriptor y múltiples publicadores potenciales.)
- **Contexto inicial de propiedades de JNDI**. Defina el conjunto de propiedades usado para crear el contexto JNDI inicial.

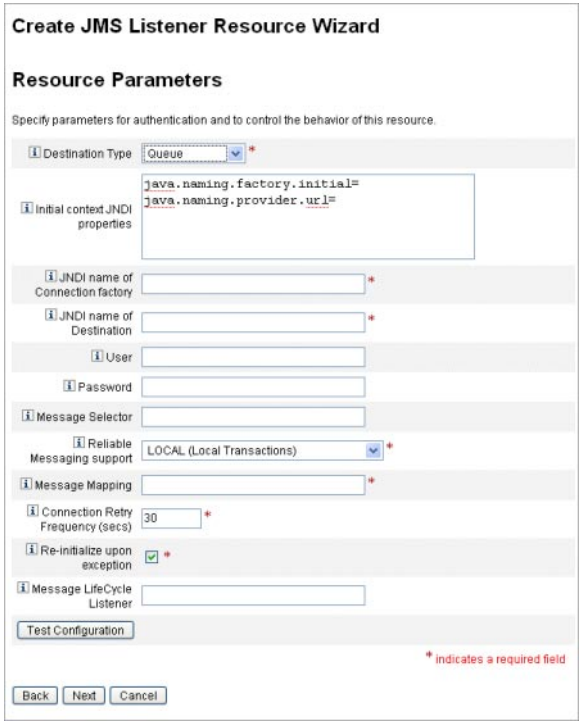
  Debe definir los siguientes pares de nombre/valor:

  - `java.naming.factory.initial`. Indique el nombre de clase (incluyendo el paquete) del contexto de fábrica inicial para el proveedor de servicios JNDI.
  - `java.naming.provider.url`. Especifique la URL de la máquina donde se ejecuta el servicio JNDI.

    Quizá tenga que definir otras propiedades. La lista de propiedades y valores debe coincidir con los especificados en la página de valores de configuración de JMS en el servidor de JMS. Por ejemplo, para suministrar las credenciales y el método de enlace, tal vez deba especificar las siguientes propiedades de ejemplo:

    - `java.naming.security.principal`: DN de enlace (por ejemplo, cn=Directory manager)
    - `java.naming.security.authentication`: Método de enlace (por ejemplo, simple)
    - `java.naming.security.credentials`: Contraseña
- **Nombre JNDI de la fábrica de conexiones**. Introduzca el nombre de una fábrica de conexiones definida en el servidor de JMS.
- **Nombre JNDI de destinos**. Introduzca el nombre de un destino definido en el servidor de JMS.
- **Usuario** y **Contraseña**. Introduzca el nombre de cuenta y la contraseña del administrador que solicita nuevos eventos de la cola.

- **Compatibilidad fiable con envío de mensajes**. Seleccione `LOCAL (Transacciones locales)`. Las otras opciones no son aplicables a la sincronización de contraseñas.
- **Asignación de mensaje**. Introduzca `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`. Esta clase convierte los mensajes del servidor de JMS a un formato utilizable en el flujo de trabajo de sincronización de contraseñas de usuario.



8 **En la página Atributos de cuenta del asistente (Figura 11–12), pulse Agregar atributo y asigne los siguientes atributos, que `PasswordSyncMessageMapper` pone a disposición del adaptador del Receptor de JMS.**

- `IDMAccountId`: `PasswordSyncMessageMapper` resuelve este atributo basándose en los atributos `resourceAccountId` y `resourceAccountGUID` transferidos en el mensaje de JMS.
- `password`: La contraseña cifrada que se reenvía en el mensaje de JMS.

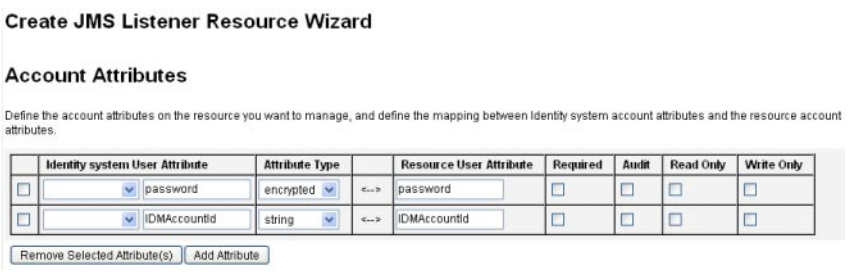


FIGURA 11–12 Página Atributos de cuenta en Crear asistente de recurso Receptor de JMS

9 Pulse Siguiente.

Aparece la página del asistente de Plantilla de identidades tal como muestra la Figura 11–13. Observe que los atributos que añadió en el paso anterior están disponibles en la sección Asignaciones de atributos del Asistente de recursos (Figura 11–13).

FIGURA 11–13 Asignaciones de atributos del asistente de recursos del Receptor de JMS

10 Pulse Siguiente y configure las opciones pertinentes de la página Parámetros de Identity System (Sistema de identidad).

Encontrará más información para configurar el adaptador de recursos del Receptor de JMS en la guía *Sun Identity Manager 8.1 Resources Reference*.

Implementación del flujo de trabajo de sincronización de contraseñas de usuario

Cuando Identity Manager recibe una notificación de cambio de contraseña, inicia el flujo de trabajo de sincronización de contraseñas de usuario. El flujo de trabajo de sincronización de contraseñas de usuario predeterminado examina el visor ChangeUserPassword y después

vuelve a comprobarlo. A continuación, el flujo de trabajo procesa todas las cuentas de recursos (excepto en el recurso de Windows que ha enviado la notificación inicial de cambio de contraseña). Por último, Identity Manager notifica por correo electrónico al usuario si la contraseña se ha cambiado correctamente en todos los recursos.

Si desea utilizar la implementación predeterminada del flujo de trabajo de sincronización de contraseñas de usuario, asígnela como regla de proceso a la instancia del adaptador del Receptor de JMS. Puede asignar reglas de proceso al configurar el Receptor de JMS para la sincronización ("Configuración de Active Sync" en la página 400).

Si prefiere modificar el flujo de trabajo, copie el archivo `$WSHOME/sample/wfpwsync.xml` y realice las modificaciones que desee. Después, importe el flujo de trabajo modificado a Identity Manager.

Estas son algunas modificaciones que quizá le interese efectuar en el flujo de trabajo predeterminado:

- Las entidades a las que se notifica cuando cambia una contraseña.
- Qué sucede si no se encuentra una cuenta de Identity Manager.
- Cómo se seleccionan los recursos en el flujo de trabajo.
- Si se permiten cambios de contraseña desde Identity Manager.

Encontrará información para utilizar los flujos de trabajo en el Capítulo 1, "Workflow" de *Sun Identity Manager Deployment Reference*.

Configuración de notificaciones

Identity Manager proporciona dos plantillas de correo electrónico para informar a los usuarios si una contraseña se ha cambiado correctamente en todos los recursos.

Estas plantillas son:

- Aviso de sincronización de contraseña
- Aviso de fallo de flujo de trabajo de sincronización

Ambas plantillas deben actualizarse con información específica de la empresa sobre cómo deben proceder los usuarios si necesitan más ayuda. Para obtener más información, consulte "Personalización de plantillas de correo electrónico" en la página 106 en el Capítulo 4, "Configuración de objetos de administración de negocio".

Configuración de PasswordSync con un servidor Sun JMS

Identity Manager puede utilizar Java Message Service (JMS) para recibir notificaciones de cambio de contraseña desde el servlet de PasswordSync. Además de garantizar la entrega, JMS puede distribuir los mensajes a múltiples sistemas.

Nota – Encontrará más información sobre este adaptador en la guía *Sun Identity Manager 8.1 Resources Reference*.

En esta sección se utiliza un escenario de ejemplo para explicar cómo configurar PasswordSync con un servidor de Sun JMS.

La información se ha organizado como sigue:

Escenario de ejemplo

Un caso de uso típico (simple) para configurar PasswordSync con un servidor de JMS es con el objeto de que los usuarios puedan cambiar sus contraseñas en Windows, Identity Manager tome la nueva contraseña y después se actualicen las cuentas de usuario con las nuevas contraseñas en un servidor Sun Directory Server.

El entorno siguiente se ha configurado para este escenario:

- Windows Server 2003 Enterprise Edition– Active Directory
- Sun Java™ System Identity Manager 6.0 2005Q4M3
- MySQL ejecutado en SUSE Linux 10.0
- Tomcat 5.0.28 ejecutado en SUSE Linux 10.0
- Sun Java System Message Queue 3.6 SP3 2005Q4 ejecutado en SUSE Linux 10.0
- Sun Java System Directory Server 5.2 SP4 ejecutado en SUSE Linux 10.0
- Java 1.5 (Java 5.0)

Los archivos siguientes se copiaron al directorio `common/lib` de Tomcat para habilitar JMS y JNDI:

- `jms.jar` (de Sun Message Queue)
- `fscontext.jar` (de Sun Message Queue)
- `imq.jar` (de Sun Message Queue)
- `jndi.jar` (de Java JDK)

Creación y almacenamiento de objetos administrados

En esta sección se explica cómo crear y almacenar los siguientes objetos administrados, necesarios para el funcionamiento correcto del escenario de ejemplo.

- Objetos de fábrica de conexiones
- Objetos de destino

Los objetos administrados se pueden almacenar en un directorio LDAP o en un archivo. Si utiliza un archivo, todas las instancia del archivo deben ser iguales.

Encontrará instrucciones en:

- "Almacenamiento de objetos administrados en un directorio LDAP" en la página 395
- "Almacenamiento de objetos administrados en un archivo" en la página 397

Nota –

- En esta sección se asume que tiene instalado Sun Java System Message Queue. (Las herramientas necesarias se hallan en el directorio `bin/` de la instalación de Message Queue.)
- Para crear estos objetos administrados puede utilizar la GUI administrativa de Message Queue (`imqadmin`) o la herramienta de línea de comandos (`imqobjmgr`). En las instrucciones siguientes se usa la línea de comandos.

Almacenamiento de objetos administrados en un directorio LDAP

Es posible configurar PasswordSync y el Receptor de JMS para utilizar los objetos administrados almacenados en un directorio LDAP. La Figura 11–14 ilustra dicho proceso. Tanto el servlet de PasswordSync como el adaptador del Receptor de JMS deben recuperar los valores de fábrica de conexiones y de destino del directorio LDAP para poder enviar y recibir mensajes.

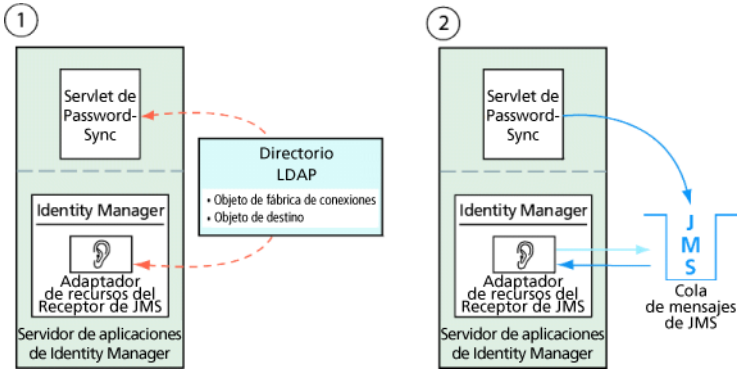


FIGURA 11–14 Recuperación de objetos de fábrica de conexiones y de destino del directorio LDAP

Uso de la herramienta de línea de comandos de Message Queue

A continuación se explica cómo utilizar la herramienta de línea de comandos de Message Queue (`imqobjmgr`) para almacenar objetos administrados en un directorio LDAP.

Almacenamiento de objetos de fábrica de conexiones

Abra la herramienta de línea de comandos de Message Queue (`imqobjmgr`) e introduzca los comandos indicados en "Almacenamiento de objetos de fábrica de conexiones" en la página 396 para almacenar los objetos de fábrica de conexiones.

EJEMPLO 11–1 Almacenamiento de objetos de fábrica de conexiones

```
#> ./imqobjmgr add -l "cn=mytestFactory"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t qf -o "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements] ...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name: cn=mytestFactory The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url
ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication
simple java.naming.security.credentials netscape
java.naming.security.principal
cn=directory manager Object successfully added.
```

Dentro de "Almacenamiento de objetos de fábrica de conexiones" en la página 396 `imqAddressList`, define el nombre de host del servidor/agente de JMS (`gwenig.coopsrc.com`), su puerto (`7676`) y el método de acceso (`jms`).

Almacenamiento de objetos de destino

En la herramienta de línea de comandos de Message Queue (`imqobjmgr`), introduzca los comandos indicados en "Almacenamiento de objetos de destino" en la página 397 para almacenar los objetos de destino.

EJEMPLO 11–2 Almacenamiento de objetos de destino

```
#> ./imqobjmgr add -l "cn=mytestDestination"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t q -o "imqDestinationName=mytestDestination"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description]
A Description for the Destination Object imqDestinationName [Destination Name]
mytestDestination Using the following lookup name: cn=mytestDestination
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/ ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager Object successfully added.
```

Puede verificar un objeto recién creado mediante `ldapsearch` o un navegador LDAP.

Con esto termina la sección sobre almacenamiento de objetos administrados en un servidor LDAP. Omita la próxima sección, donde se explica cómo almacenar objetos administrados en un archivo, y continúe en la sección "Configuración del adaptador del Receptor de JMS para este escenario" en la página 400.

Almacenamiento de objetos administrados en un archivo

Es posible configurar PasswordSync y el Receptor de JMS para utilizar los objetos administrados almacenados en un archivo. Si no va a almacenar los objetos administrados en un servidor LDAP"Almacenamiento de objetos administrados en un directorio LDAP" en la página 395), siga las instrucciones de esta sección.

Almacenamiento de objetos de fábrica de conexiones

Abra la herramienta de línea de comandos de Message Queue (`imqobjmgr`) e introduzca los comandos indicados en "Almacenamiento de objetos de fábrica de conexiones" en la página 398 para almacenar los objetos de fábrica de conexiones y especificar un nombre de búsqueda.

EJEMPLO 11–3 Almacenamiento de objetos de fábrica de conexiones y especificación de nombres de búsqueda

```
#> ./imqobjmgr add -l "mytestFactory" -j
"java.naming.factory.initial= com.sun.jndi.fscontext.RefFSContextFactory"
 -j "java.naming.provider.url=file:///home/gael/tmp" -t qf -o
 "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name:
mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
To specify a destination:
#> ./imqobjmgr add -l "mytestQueue" -j
"java.naming.factory.initial=com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t q -o
"imqDestinationName=myTestQueue"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] myTestQueue
Using the following lookup name:
mytestQueue
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
```

Creación del destino en el agente

De manera predeterminada, el agente de Sun Message Queue permite crear automáticamente el destino de la cola (consulte `config.properties`, donde el valor predeterminado de `imq.autocreate.queue` es `true`).

Si el destino de la cola no se crea automáticamente, deberá crear el objeto de destino en el agente con el comando indicado en "Creación del destino en el agente" en la página 398 (donde *myTestQueue* es el destino).

EJEMPLO 11–4 Creación de un objeto de destino en el agente

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username: <admin>
Password: <admin>
Creating a destination with the following attributes:
Destination Name mytestQueue
Destination Type Queue On the broker specified by:
------------------------
Host Primary Port
------------------------ localhost 7676
Successfully created the destination.
```

Los objetos administrados se pueden almacenar en un archivo:

- **En un directorio:** Un directorio permite centralizar el almacenamiento de los objetos de fábrica de conexiones y los objetos de destino.

  Cuando se utiliza un directorio, estos objetos administrados se almacenan como entradas de directorio.

  Nota – Si el servlet de Identity Manager PasswordSync y el servidor de Identity Manager no se encuentran en la misma máquina, cada uno de ellos debe tener acceso al archivo `.bindings`. Puede repetir dos veces la creación del objeto administrado (en cada máquina) o bien copiar el archivo `.bindings` en la ubicación adecuada de cada máquina.

- **En un archivo:** Si el servlet de Identity Manager PasswordSync y el servidor de Identity Manager se ejecutan en el mismo servidor (o si no hay disponible un directorio), puede almacenar los objetos administrativos en un archivo.

  Cuando se utiliza un archivo, ambos objetos administrados se almacenan en un solo archivo (denominado `.bindings` tanto en Windows como en UNIX), dentro del directorio que haya especificado para java.naming.provider.url (por ejemplo, `file:///c:/temp` en Windows o `file:///tmp` en UNIX).

Configuración del adaptador del Receptor de JMS para este escenario

Configure el adaptador del Receptor de JMS en el servidor de aplicaciones. Siga las instrucciones de la sección "Adición y configuración del adaptador del Receptor de JMS " en la página 388.

Configuración de Active Sync

Ahora debe configurar el Receptor de JMS para la sincronización. Necesitará Active Sync si utiliza JMS, aunque no se usa con las conexiones directas.

▼ Para configurar el Receptor de JMS para la sincronización

1. **En la interfaz de administración, seleccione Recursos en el menú.**
2. **En la Lista de recursos, marque la casilla de verificación Receptor de JMS.**
3. **En la lista Acciones de recurso, elija Editar directiva de sincronización.**

   Aparece la página Editar directiva de sincronización para el recurso Receptor de JMS (Figura 11–15).

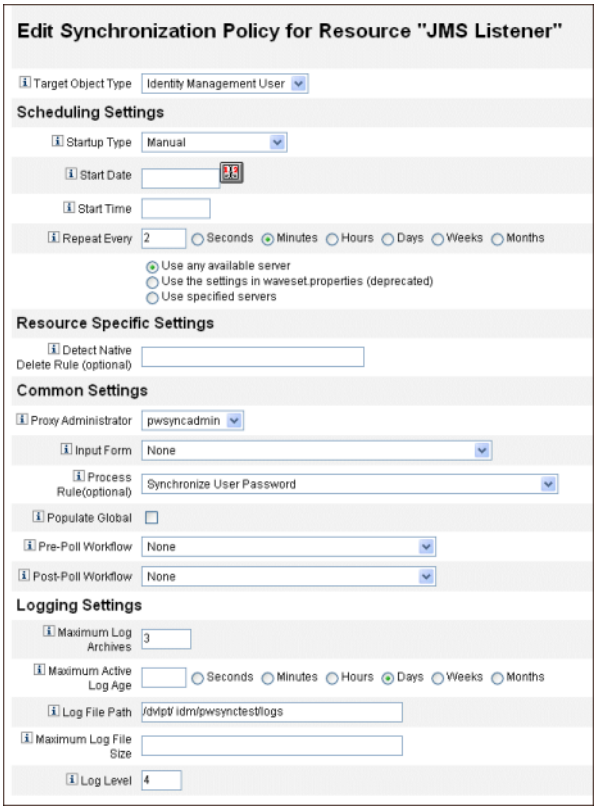


FIGURA 11–15 Configuración de Active Sync para el Receptor de JMS

4 **Dentro de Preferencias comunes, busque Administrador de proxy y seleccione `pwsyncadmin`. (Esta interfaz de administración está asociada a un formulario vacío.)**

5 **Dentro de Preferencias comunes, busque Regla de proceso y seleccione Synchronize User Password (sincronizar contraseñas de usuario) en la lista. El flujo de trabajo de sincronización de contraseñas de usuario predeterminado toma cada solicitud procedente del adaptador del Receptor de JMS, examina el visor ChangeUserPassword y después vuelve a comprobarlo.**

6 **En el cuadro Ruta del archivo de registro, especifique una ruta de acceso al un directorio donde deban crearse los archivos de registro activos y archivados.**

7 **Para la depuración, configure el Nivel de registro en 4 con el fin de generar un registro detallado.**

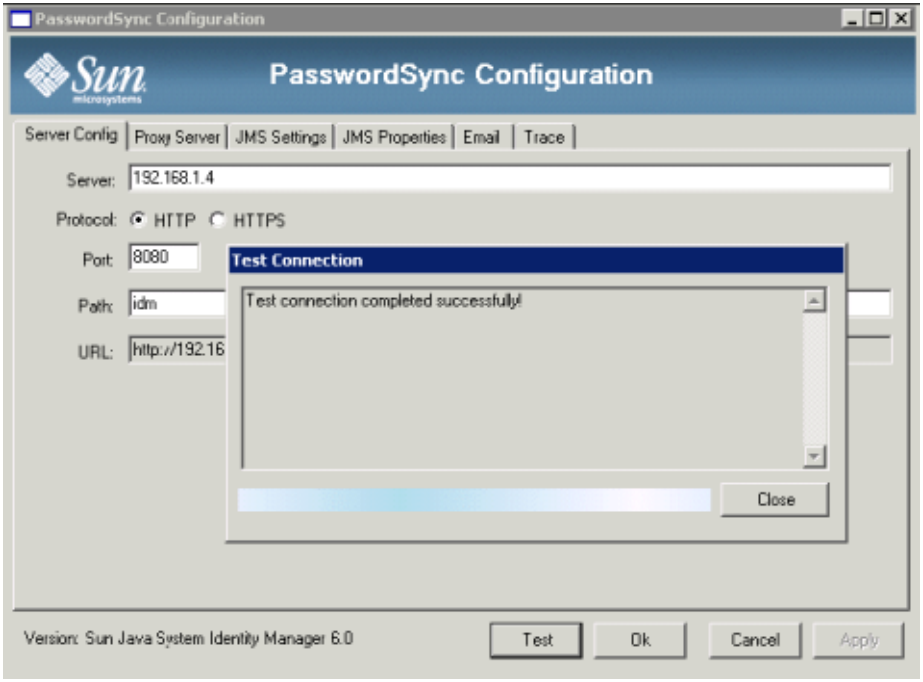
8 **Pulse Guardar.**

Verificación de la configuración

Puede utilizar la aplicación de configuración de PasswordSync en Windows para depurar la parte de Windows de la configuración.

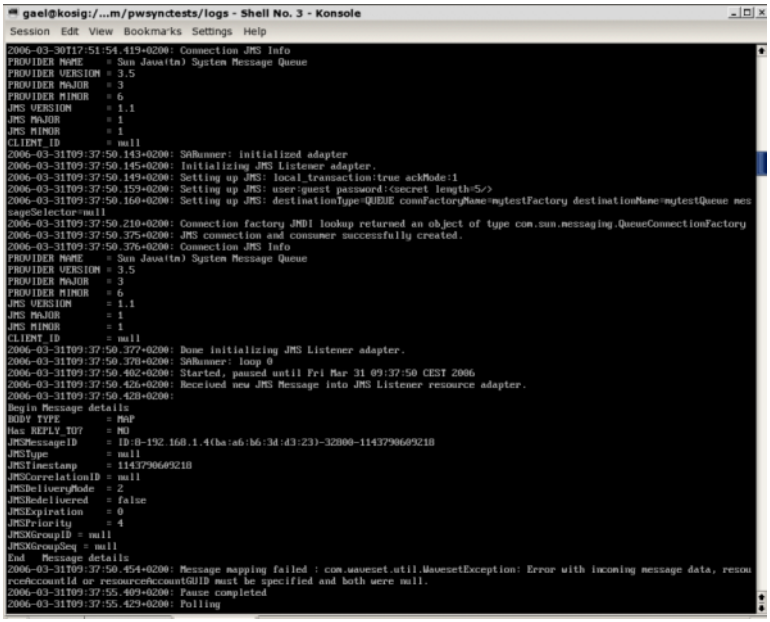
1. **Inicie la aplicación de configuración de PasswordSync si aún no se está ejecutando.**

   De manera predeterminada, la aplicación de configuración se instala dentro de Archivos de programa → Sun Java System Identity Manager PasswordSync → Configuration.
2. **Cuando aparezca el cuadro de diálogo PasswordSync Configuration, pulse el botón Test.**
3. **Si utiliza JMS, aparece el cuadro de diálogo Test Connection con un mensaje que indica si la conexión de prueba se ha realizado satisfactoriamente.**



4. Pulse Close para cerrar el cuadro de diálogo Test Connection.
5. Pulse OK para cerrar el cuadro de diálogo PasswordSync Configuration.

   A continuación, se ejecuta el adaptador del Receptor de JMS en modo de depuración y genera información de depuración en un archivo análogo al de la figura siguiente.



Depuración de PasswordSync en Windows

PasswordSync graba todos los fallos en el Visor de eventos de Windows. (En la ayuda de Windows en línea se explica cómo utilizar el Visor de eventos.) El nombre de origen de las entradas del registro de errores es *PasswordSync*.

En *Sun Identity Manager 8.1 System Administrator's Guide* se explica cómo solucionar problemas con PasswordSync en Windows.

Desinstalación de PasswordSync en Windows

Para desinstalar la aplicación PasswordSync, vaya al Panel de control de Windows y seleccione Agregar o quitar programas. A continuación, seleccione Sun Java System Identity Manager PasswordSync y pulse Quitar.

Nota – PasswordSync también se puede desinstalar (o reinstalar) cargando el medio de instalación de Identity Manager y haciendo clic en el icono `pwsync\IdmPwSync.msi`.

Debe reiniciar el sistema para completar el proceso.

Preguntas frecuentes sobre PasswordSync

En esta sección respondemos a algunas preguntas frecuentes sobre PasswordSync.

Pregunta: ¿Se puede implementar PasswordSync sin Java Messaging Service?

Respuesta: Sí, pero a costa de renunciar a las ventajas de usar JMS para rastrear los cambios de contraseña.

Para implementar PasswordSync sin JMS, ejecute la aplicación de configuración con esta marca:

```
Configure.exe -direct
```

Cuando se especifica la marca `-direct`, la aplicación de configuración muestra la ficha User.

Si implementa PasswordSync sin JMS, no necesita crear un adaptador del Receptor de JMS. Por tanto, deberá omitir los procedimientos explicados en "Implementación de PasswordSync en el servidor de aplicaciones" en la página 388. Para configurar las notificaciones, quizá tenga que cambiar el flujo de trabajo Modificar contraseña de usuario.

Nota – Si después ejecuta la aplicación de configuración sin especificar la marca `-direct`, PasswordSync requerirá que se configure JMS. Vuelva a ejecutar la aplicación con la marca `-direct` para omitir de nuevo JMS.

Pregunta: ¿Se puede usar PasswordSync junto con otros filtros de contraseña de Windows que sirven para aplicar directivas de contraseñas personalizadas?

Respuesta: Sí, PasswordSync puede combinarse con otros filtros de contraseña `_WINDOWS_`. No obstante, debe ser el último filtro de contraseña en la lista del valor de registro Notification Package.

Ha de utilizar esta ruta para el registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages (value of type REG_MULTI_SZ)
```

El instalador incluye el interceptor de contraseñas de Identity Manager al final de la lista de manera predeterminada, pero si ha instalado el filtro de contraseña personalizado después de la instalación, deberá trasladar `lhpwic` al final de la lista Notification Packages.

PasswordSync puede combinarse con otras directivas de contraseñas de Identity Manager. Cuando se verifican las directivas en el lado del servidor de Identity Manager, se deben pasar todas las directivas de contraseñas de recursos para que la sincronización de contraseñas se propague a otros recursos. Por tanto, la directiva de contraseñas nativa de Windows debe ser tan restrictiva como la directiva de contraseñas más restrictiva que se defina en Identity Manager

Nota – La DLL interceptora de contraseñas no impone directivas de contraseñas.

Pregunta: ¿Se puede instalar el servlet de PasswordSync en un servidor de aplicaciones distinto al de Identity Manager?

Respuesta: Sí. El servlet de PasswordSync necesita los archivos `jar` `spml.jar` e `idmcommon.jar`, además de todos los demás archivos `jar` que precise la aplicación de JMS.

Pregunta: ¿El servicio PasswordSync envía contraseñas a través del servidor de `lh` en texto sin cifrar?

Respuesta: Aunque lo mejor es ejecutar PasswordSync a través de SSL, todos los datos delicados se cifran antes de enviarlos al servidor de Identity Manager.

Encontrará información al respecto en "Configuración de PasswordSync para SSL" en la página 376.

Pregunta: ¿Por qué algunos cambios de contraseña generan `com.waveset.exception.ItemNotLocked` ?

Respuesta: Si habilita PasswordSync, cualquier un cambio de contraseña (incluso iniciado en la interfaz de usuario) producirá un cambio de contraseña en el recurso, que en consecuencia entrará en contacto con Identity Manager.

Si configura correctamente la variable de flujo de trabajo `passwordSyncThreshold`, Identity Manager examinará el objeto de usuario y determinará que ya ha controlado el cambio de contraseña. No obstante, si el usuario o el administrador efectúa otro cambio de contraseña simultáneo para el mismo usuario, quizá se bloquee el objeto de usuario.

◆ ◆ ◆ CAPÍTULO 12

12 Seguridad

Este capítulo contiene información acerca de las funciones de seguridad de Identity Manager e instrucciones detalladas para reducir aún más los riesgos de seguridad.

Los temas siguientes le ayudarán a administrar mejor la seguridad del sistema con Identity Manager.

Funciones de seguridad

Identity Manager ayuda a reducir los riesgos de seguridad con las siguientes funciones:

- **Inhabilitación instantánea del acceso a las cuentas**. Identity Manager le permite inhabilitar los derechos de acceso de organizaciones o usuarios individuales con una sola acción.
- **Limitaciones de sesiones**. Puede establecer limitaciones sobre las sesiones que se inician.
- **Análisis de riesgo activo** Identity Manager efectúa análisis constantes para detectar riesgos de seguridad, como cuentas inactivas y actividades de contraseña sospechosas.
- **Administración completa de contraseñas**. Las capacidades completas y flexibles para administrar contraseñas garantizan un control total del acceso.

- **Auditoría e informes para supervisar las actividades de acceso**. Puede ejecutar toda una gama de informes para suministrar información específica sobre las actividades de acceso. Para obtener más información sobre las funciones de informes, consulte el Capítulo 8, "Informes".
- **Controles minuciosos de los privilegios administrativos**. Puede conceder y gestionar el control administrativo en Identity Manager asignando una única capacidad a un usuario o un conjunto de tareas administrativas definidas mediante roles de administrador.
- **Cifrado de claves de servidor**. Identity Manager le permite crear y administrar claves de cifrado de servidor en el área Tareas.

Además, la arquitectura del sistema está diseñada para reducir los riesgos de seguridad al máximo. Por ejemplo, una vez cerrada una sesión, no es posible acceder a las páginas recién visitadas con la función *Retroceder* del navegador.

Limitación de sesiones concurrentes

De manera predeterminada, un usuario de Identity Manager puede iniciar sesiones simultáneas. No obstante, las sesiones simultáneas se pueden limitar a una por aplicación de inicio de sesión. Para ello, abra el objeto de configuración del sistema para modificarlo ("Edición de objetos de configuración de Identity Manager" en la página 118) y edite el valor del atributo de configuración `security.authn.singleLoginSessionPerApp`. Este atributo es un objeto que contiene un atributo para cada nombre de aplicación de inicio de sesión (por ejemplo, la interfaz de administración, la interfaz de usuario o Identity Manager IDE). Al cambiar el valor de este atributo a `true`, se asegura que haya una sola sesión por cada usuario.

Si se ejecuta, un usuario podrá iniciar sesión en varias sesiones; sin embargo, sólo la última sesión iniciada permanecerá activa y válida. Si el usuario realiza una acción en una sesión no válida, se le expulsará automáticamente de la sesión y ésta terminará.

Administración de contraseñas

Identity Manager ofrece administración de contraseñas en varios niveles:

- **Administración de cambios**
  - Es posible cambiar la contraseña de un usuario desde diversas ubicaciones (páginas Editar usuario, Buscar usuario o Cambiar contraseña).
  - Puede cambiar las contraseñas en cualquiera de los recursos de un usuario seleccionándolos detalladamente.
- **Reinicialización administrativa de contraseñas**
  - Se pueden generar contraseñas aleatorias.
  - Puede mostrar las contraseñas al usuario final o al administrador.

- **Cambio de contraseña por parte del usuario**
  - Puede conceder al usuario final autoservicio para cambiar contraseñas en:

    http://*localhost*:8080/idm/user
  - Existe la posibilidad de personalizar la página de autoservicio en consonancia con el entorno del usuario final.
- **Datos de actualización de usuario**

  Cualquier atributo de esquema de usuario puede configurarse para que lo administre el usuario final.
- **Recuperación del acceso por parte del usuario**
  - Las respuestas de autenticación permiten conceder al usuario acceso para cambiar su contraseña.
  - Con la autenticación al paso puede conceder acceso al usuario con una de varias contraseñas.
- **Directivas de contraseñas**

  Los parámetros de contraseña se pueden definir mediante reglas.

Autenticación al paso

Utilice autenticación al paso para conceder acceso de usuario y administrador con una o más contraseñas distintas.

Identity Manager administra la autenticación mediante la implementación de:

- *Aplicaciones de inicio de sesión* (una colección de grupos de módulos de inicio)
- *Grupos de módulos de inicio de sesión* (un conjunto ordenado de módulos de inicio de sesión)
- *Módulos de inicio de sesión* (se define la autenticación para cada recurso asignado y se especifica uno de varios requisitos satisfactorios para la autenticación)

Acerca de las aplicaciones de inicio de sesión

Las aplicaciones de inicio de sesión hacen referencia a un conjunto de grupos de módulos de inicio de sesión que definen el conjunto y orden de los módulos de inicio de sesión que se utilizarán cuando un usuario inicie una sesión de Identity Manager. Cada aplicación de inicio de sesión consta de uno o más grupos de módulos de inicio de sesión.

Al iniciar la sesión, la aplicación comprueba el conjunto de los grupos de módulos de inicio de sesión. Si sólo hay un grupo de módulos de inicio de sesión establecido, se utiliza dicho módulo y se procesan los módulos de inicio de sesión contenidos en él en el orden definido por el grupo.

Si la aplicación de inicio de sesión tiene más de un grupo de módulos de inicio de sesión definido, Identity Manager comprueba las *reglas de restricción de inicio de sesión* que se aplican a cada grupo de módulos de inicio de sesión para determinar el grupo que va a procesar.

Reglas de restricciones de inicio de sesión

Las reglas de restricciones de inicio de sesión se aplican a los grupos de módulos de inicio de sesión. Para cada conjunto de grupos de módulos de inicio de sesión de una aplicación de inicio de sesión, sólo puede haber uno que no tenga una regla de restricciones de inicio de sesión aplicada.

Al determinar el grupo de módulos de inicio de sesión de un conjunto que se va a procesar, Identity Manager evalúa la primera regla de restricciones del grupo de módulos de inicio de sesión. Si la evalúa correctamente, procesa ese grupo de módulos de inicio de sesión. Si falla, evalúa cada grupo de módulos de inicio de sesión hasta encontrar una regla de restricciones adecuada o evaluar un grupo de módulos de inicio de sesión sin regla de restricciones (que será el que se utilice).

Nota – Si una aplicación de inicio de sesión contiene más de un grupo de módulos de inicio de sesión, el grupo de módulos de inicio de sesión sin reglas de restricciones de inicio de sesión debe colocarse en último lugar.

Ejemplo de regla de restricciones de inicio de sesión

En el siguiente ejemplo de una regla de restricciones de inicio de sesión basada en la ubicación, la regla toma la dirección IP del solicitante del encabezado HTTP y después la comprueba para ver si se encuentra en la red 192.168. Si se encuentra 192.168. en la dirección IP, la regla devolverá un valor "true" y se seleccionará el grupo de módulos de inicio de sesión.

EJEMPLO 12–1 Regla de restricciones de inicio de sesión basada en ubicación

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
<match> <ref>remoteAddr</ref> <s>192.168.</s> </match>
<MemberObjectGroups> <ObjectRef type='ObjectGroup' name='All'/> </MemberObjectGroups>
</Rule>
```

Edición de aplicaciones de inicio de sesión

En la barra de menús, seleccione Seguridad → Inicio de sesión para acceder a la página de inicio de sesión.

La lista de aplicaciones de inicio de sesión muestra:

- Cada aplicación de inicio de sesión (interfaz) de Identity Manager definida.
- Los grupos de módulos de inicio de sesión que componen la aplicación de inicio de sesión.
- Los límites de tiempo de espera de sesión de Identity Manager establecidos para cada aplicación de inicio de sesión.

En la página de inicio de sesión puede:

- Crear aplicaciones de inicio de sesión personalizadas.
- Borrar aplicaciones de inicio de sesión personalizadas.
- Administrar grupos de módulos de inicio de sesión.

Para editar una aplicación de inicio de sesión, selecciónela en la lista.

Configuración de los límites de sesión de Identity Manager

En la página Modificar aplicación de inicio de sesión puede definir un valor de tiempo de espera (límites) para cada sesión iniciada en Identity Manager. Seleccione horas, minutos y segundos y, a continuación, haga clic en Guardar. Los límites que establezca se mostrarán en la lista de aplicaciones de inicio de sesión.

Puede definir tiempos de espera de sesión para cada aplicación de inicio de sesión en Identity Manager. Cuando un usuario inicia una sesión en una aplicación de Identity Manager, el valor de tiempo de espera de sesión configurado actualmente se aplica para calcular la fecha y la hora en que la sesión del usuario terminará por inactividad. La fecha calculada se almacena con la sesión de Identity Manager del usuario de modo que pueda comprobarse cada vez que se efectúe una solicitud.

Si un administrador de inicio de sesión cambia el valor de tiempo de espera de sesión de una aplicación de inicio de sesión, dicho valor se aplicará a todos los inicios de sesión posteriores. Las sesiones existentes terminarán de acuerdo con el valor que había vigente cuando el usuario inicio la sesión.

El valor definido para el tiempo de espera de HTTP afecta a todas las aplicaciones de Identity Manager tiene prioridad sobre el valor de tiempo de espera de sesión de la aplicación de inicio de sesión.

Inhabilitación del acceso a aplicaciones

En las páginas Crear aplicación de inicio de sesión y Modificar aplicación de inicio de sesión se puede seleccionar la opción Inhabilitar para inhabilitar una aplicación de inicio de sesión, con el fin de impedir el acceso de los usuarios. Si un usuario intenta iniciar una sesión en una aplicación inhabilitada, se le redirige a una página alternativa que le advierte de que la aplicación está inhabilitada en ese momento. Para editar el mensaje que aparece en dicha página puede editar el catálogo personalizado.

Las aplicaciones de inicio de sesión permanecen inhabilitadas hasta que se desactiva la opción. Como medida de seguridad, el usuario no puede inhabilitar el inicio de sesión del administrador.

Edición de grupos de módulos de inicio de sesión

La lista de grupos de módulos de inicio de sesión muestra:

- Cada grupo de módulos de inicio de sesión
- Los distintos módulos de inicio de sesión que forman un grupo
- Si un grupo de módulos de inicio de sesión contiene reglas de restricciones.

En la página Grupos de módulos de inicio de sesión puede crear, editar y eliminar grupos de módulos de inicio de sesión. Para editar un grupo de módulos de inicio de sesión, selecciónelo en la lista.

Edición de módulos de inicio de sesión

A continuación se explica cómo introducir detalles o seleccionar opciones para los módulos de inicio de sesión. (No todas las opciones están disponibles para cada módulo de inicio de sesión.).

- **Requisito para un inicio de sesión correcto**. Seleccione un requisito que se aplique a este módulo. Las opciones son:
  - **Requerido**. Es necesario el módulo de inicio de sesión para una autenticación con éxito. Independientemente de si se realiza con éxito o falla, la autenticación continúa con el siguiente módulo de inicio de sesión de la lista. Si es el único módulo de inicio de sesión, el usuario o el administrador ha iniciado la sesión con éxito.
  - **Requisito**. Es necesario el módulo de inicio de sesión para una autenticación con éxito. Si se realiza con éxito, la autenticación continúa con el siguiente módulo de inicio de sesión de la lista. Si falla, la autenticación no continúa.
  - **Suficiente**. No es necesario el módulo de inicio de sesión para una autenticación con éxito. Si se realiza con éxito, el proceso de autenticación no necesita pasar al siguiente módulo de inicio de sesión y el administrador accede correctamente. Si fracasa, el proceso de autenticación continúa con el siguiente módulo de inicio de sesión de la lista.
  - **Opcional**. No es necesario el módulo de inicio de sesión para una autenticación con éxito. Independientemente de si se realiza con éxito o falla, la autenticación continúa con el siguiente módulo de inicio de sesión de la lista.
- **Atributos de búsqueda de inicio de sesión**. (Sólo LDAP.) Especifique la lista ordenada de nombres de atributos de usuarios de LDAP que se vaya a utilizar al intentar iniciar la sesión en el servidor LDAP asociado. Cada atributo de usuario de LDAP especificado, junto con el nombre de inicio de sesión especificado del usuario, se utiliza para buscar un usuario de

LDAP que coincida. Esto permite que un usuario inicie la sesión en Identity Manager utilizando una dirección de correo electrónico o un cn de LDAP (cuando Identity Manager está configurado para autenticación al paso en LDAP).

Por ejemplo, si especifica lo siguiente y el usuario intenta iniciar la sesión como `gwilson`, el recurso de LDAP intentará primero encontrar un usuario de LDAP cuyo `cn=gwilson`.

```
cn
```

```
mail
```

Si lo encuentra, se intenta establecer la conexión utilizando la contraseña especificada por el usuario. Si no se consigue, el recurso de LDAP buscará un usuario de LDAP cuyo `mail=gwilson`. Si también falla esto, se producirá un error en el inicio de sesión.

Si no especifica un valor, los atributos predeterminados de búsqueda de LDAP son:

```
uid
```

```
cn
```

- **Regla de correlación de inicio de sesión**. Seleccione una regla de correlación de inicio de sesión para usarla con objeto de asignar la información de inicio de sesión que proporciona el usuario a un usuario de Identity Manager. Esta regla se utiliza para buscar usuarios de Identity Manager mediante la lógica especificada en la regla. La regla debe ofrecer una lista de uno o varios elementos `AttributeConditions` que se utilizarán para buscar el usuario de Identity Manager que coincida. La regla que seleccione debe tener el tipo de autenticación `LoginCorrelationRule` `authType`. Los pasos que sigue Identity Manager para asignar un ID de usuario autenticado a un usuario de Identity Manager se describen en el Ejemplo 12–2.
- **Regla de nombre de usuario nuevo**. Seleccione una regla de nombre de usuario nuevo para usarla al crear automáticamente usuarios de Identity Manager como parte del inicio de sesión.

Haga clic en Guardar para guardar el módulo de inicio de sesión. Una vez guardado, puede ubicar el módulo con relación a los otros módulos del grupo de módulos de inicio de sesión.

Precaución – Si el inicio de sesión de Identity Manager está configurado para autenticar en más de un sistema, se debe definir el mismo ID de usuario de cuenta y la misma contraseña en todos los sistemas en los que Identity Manager realiza la autenticación.

Si varían las combinaciones de ID de usuario y contraseña, el inicio de sesión puede fallar en los sistemas cuyos ID de usuario y contraseña no coincidan con aquéllos introducidos en el formulario de inicio de sesión de Identity Manager.

Algunos de estos sistemas pueden tener una directiva de bloqueo que fuerce el bloqueo de una cuenta tras un número de intentos erróneos de inicio de sesión. En estos casos, las cuentas se acaban bloqueando, incluso aunque los usuarios sigan iniciando las sesiones satisfactoriamente en Identity Manager.

El Ejemplo 12–2 contiene seudocódigo que describe los pasos que sigue Identity Manager para asignar IDs de usuario autenticado a usuarios de Identity Manager.

EJEMPLO 12–2 Lógica de proceso de módulo de inicio de sesión

```
if an existing IDM user's ID is the same as the specified user ID

   if that IDM user has a linked resource whose resource name matches the
   resource that was authenticated and whose accountId matches the resource
   accountId returned by successful authentication (e.g. dn), then we have
   found the right IDM user

   otherwise if there is a LoginCorrelationRule associated with the
   configured login module

      evaluate it to see if it maps the login credentials to a single IDM
      user

      otherwise login fails

   otherwise login fails

if the specified userID does not match an existing IDM user's ID

   try to find an IDM user that has a linked resource whose resource
   name matches the resource accountID returned by successful authentication

     if found, then we have found the right IDM user

     otherwise if there is a LoginCorrelationRule associated with the
     configured login module
```

EJEMPLO 12–2 Lógica de proceso de módulo de inicio de sesión *(Continuación)*

```
        evaluate it to see if it maps the login credentials to a single
        IDM user

        otherwise login fails

    otherwise login fails
```

En el Ejemplo 12–2, el sistema intentará encontrar un usuario coincidente de Identity Manager empleando los recursos vinculados del usuario (información de recursos). Si falla el intento con la información de recursos y hay configurada una regla de correlación de inicio de sesión, el sistema intentará encontrar un usuario coincidente aplicando dicha regla.

Configuración de la autenticación para recursos comunes

Si tiene múltiplos recursos que son lógicamente iguales (por ejemplo, varios servidores de dominio de Active Directory que comparten una relación de confianza), o diversos recursos que residen en el mismo host físico, puede especificar que son *recursos comunes*.

Debe declarar los recursos comunes para que Identity Manager sepa que sólo debe intentar autenticar con un grupo de recursos a la vez. De lo contrario, si un usuario escribe una contraseña equivocada, Identity Manager probará la misma contraseña en cada recurso. Ello puede ocasionar el bloqueo de la cuenta del usuario a raíz de varios fallos de inicio de sesión, incluso aunque el usuario sólo haya introducido mal la contraseña una vez.

Los recursos comunes permiten que un usuario autentique en un solo recurso común, mientras que Identity Manager intentará asignar el usuario a los demás recursos del grupo de recursos comunes. Por ejemplo, una cuenta de usuario de Identity Manager se puede vincular a una cuenta de recursos para el recurso AD-1. Sin embargo, el grupo de módulos de inicio de sesión puede establecer que los usuarios deben autenticarse en el recurso AD-2.

Si AD-1 y AD-2 se han definido como recursos comunes (en este caso, en el mismo dominio de confianza), cuando el usuario autentica con éxito en AD-2, Identity Manager también puede asignar el usuario a AD-1 buscando el mismo ID de cuenta de usuario en el recurso AD-1.

Precaución – Todos los recursos incluidos en un grupo de recursos comunes también deben incluirse en la definición del módulo de inicio de sesión. Si dicha definición no contiene una lista completa de los recursos comunes, la funcionalidad de recursos comunes no actuará correctamente.

Los recursos comunes pueden definirse en el objeto de configuración del sistema ("Edición de objetos de configuración de Identity Manager" en la página 118) con el formato indicado a continuación.

EJEMPLO 12–3 Configuración de la autenticación para recursos comunes

```
<Attribute name='common resources'>
<Attribute name='Common Resource Group Name'>
<List>
<String>Common Resource Name</String>
<String>Common Resource Name</String>
</List
</Attribute> </Attribute>
```

Configuración de la autenticación mediante certificado X509

Utilice la información y los procedimientos descritos a continuación para configurar la autenticación basada en el certificado X509 para Identity Manager.

Requisitos previos de configuración

Para poder realizar autenticación basada en el certificado X509 en Identity Manager, asegúrese de que esté bien configurada la autenticación SSL bidireccional (de cliente y servidor). Desde la perspectiva del cliente, esto significa que se debe haber importado al navegador un certificado de usuario conforme con X509 (o tenerlo disponible en un lector de tarjetas inteligentes), y que el certificado de confianza empleado para firmar el certificado de usuario debe importarse al almacén de claves de certificados de confianza situado en el servidor de aplicaciones.

Asimismo, el certificado de cliente debe habilitarse para autenticación de cliente.

▼ Para verificar si está seleccionada la opción de autenticación de cliente del certificado de cliente

1. **En Internet Explorer, elija Herramientas y después Opciones de Internet.**
2. **Seleccione la ficha Contenido.**
3. **En el área Certificados, pulse Certificados.**
4. **Seleccione el certificado de cliente y pulse Avanzadas.**
5. **Dentro de Propósito del certificado, asegúrese de que esté marcada la opción Autenticación del cliente.**

Configuración de la autenticación mediante certificado X509 en Identity Manager

▼ Para configurar la autenticación mediante certificado X509

1 **Inicie una sesión en la interfaz de administración como configurador (o con permisos equivalentes).**

2 **Seleccione Configurar y después Inicio de sesión para acceder a la página de inicio de sesión.**

3 **Haga clic en Administrar grupos de módulos de inicio de sesión para ver la página Grupos de módulos de inicio de sesión.**

4 **Seleccione un grupo de módulos de inicio de sesión en la lista.**

5 **Elija Módulo de inicio de sesión con certificado X509 de Identity Manager en la lista Asignar módulo de inicio de sesión. Identity Manager muestra la página Modificar módulo de inicio de sesión.**

6 **Defina el requisito para un inicio de sesión correcto.**

Se admiten los valores siguientes:

- **Requerido**. Es necesario el módulo de inicio de sesión para una autenticación con éxito. Independientemente de si se realiza con éxito o falla, la autenticación continúa con el siguiente módulo de inicio de sesión de la lista. Si es el único módulo de inicio de sesión, el usuario o el administrador ha iniciado la sesión con éxito.
- **Requisito**. Es necesario el módulo de inicio de sesión para una autenticación con éxito. Si se realiza con éxito, la autenticación continúa con el siguiente módulo de inicio de sesión de la lista. Si falla, la autenticación no continúa.
- **Suficiente**. No es necesario el módulo de inicio de sesión para una autenticación con éxito. Si se realiza con éxito, el proceso de autenticación no necesita pasar al siguiente módulo de inicio de sesión y el administrador accede correctamente. Si fracasa, el proceso de autenticación continúa con el siguiente módulo de inicio de sesión de la lista.
- **Opcional**. No es necesario el módulo de inicio de sesión para una autenticación con éxito. Independientemente de si se realiza con éxito o falla, la autenticación continúa con el siguiente módulo de inicio de sesión de la lista.

7 **Seleccione una regla de correlación de inicio de sesión. Puede ser una regla de correlación interna o personalizada. (En la próxima sección se explica cómo crear reglas de correlación personalizadas.)**

8 **Pulse Guardar para volver a la página Modificar grupo de módulos de inicio de sesión.**

9 **Si lo desea, reordene los módulos de inicio de sesión (cuando hay varios módulos de inicio de sesión asignados al grupo) y pulse Guardar.**

10 **Asigne el grupo de módulos de inicio de sesión a una aplicación de inicio de sesión si aún no está asignado. En la página Grupos de módulos de inicio de sesión, haga clic en Volver a las aplicaciones de inicio de sesión y seleccione una aplicación de inicio de sesión. Una vez asignado un grupo de módulos de inicio de sesión a la aplicación, hacer clic, pulse Guardar.**

Nota – Si la opción `allowLoginWithNoPreexistingUser` está definida en `true` en el archivo `waveset.properties`, al configurar el Módulo de inicio de sesión con certificado X509 de Identity Manager, se le pedirá que seleccione una regla de nombre de usuario nuevo. Esta regla determina cómo se nombran los nuevos usuarios creados cuando no los encuentra la `regla de correlación de inicio de sesión` asociada. La regla de nombre de usuario nuevo tiene disponibles los mismos argumentos de entrada que la regla de correlación de inicio de sesión. Devuelve una sola cadena, consistente en el `nombre de usuario empleado para crear la nueva cuenta de usuario de Identity Manager.` En `idm/sample/rules, hay un ejemplo de regla de nombre de usuario nuevo` denominada `NewUserNameRules.xml.`

Creación e importación de reglas de correlación de inicio de sesión

Una regla de correlación de inicio de sesión sirve al Módulo de inicio de sesión con certificado X509 de Identity Manager para establecer cómo asignar los datos del certificado al usuario adecuado de Identity Manager. Identity Manager incluye una regla de correlación de inicio de sesión interna, denominada Correlacionar con SubjectDN de Certificado X509.

También se pueden agregar reglas de correlación propias. Consulte el ejemplo de `LoginCorrelationRules.xml` , situado en el directorio `idm/sample/rules`.

Cada regla de correlación debe respetar estas pautas:

- Su atributo `authType` debe definirse en `LoginCorrelationRule`
- Se espera que devuelva una instancia de una lista de `AttributeConditions` que el módulo de inicio de sesión utilizará para buscar el usuario asociado de Identity Manager. Por ejemplo, la regla de correlación de inicio de sesión podría devolver una condición `AttributeCondition` que busque el usuario asociado de Identity Manager por la dirección de correo electrónico.

Estos son los argumentos que admiten las reglas de correlación de inicio de sesión:

- Campos de certificado X509 estándar (como `subjectDN`, `issuerDN` y fechas válidas)
- Propiedades de extensión críticas y no críticas

Los argumentos de certificado que admiten las reglas de correlación de inicio de sesión siguen esta convención de nomenclatura:

```
cert.field name.subfield name
```

Los nombres de argumento de ejemplo disponibles para la regla incluyen:

- `cert.subjectDN`
- `cert.issuerDN`
- `cert.notValidAfter`
- `cert.notValidBefore`
- `cert.serialNumber`

La regla de correlación de inicio de sesión, con los argumentos admitidos, devuelve una lista de una o varias `AttributeConditions`. El Módulo de inicio de sesión con certificado X509 de Identity Manager utiliza estas condiciones para encontrar el usuario de Identity Manager asociado.

En `idm/sample/rules` hay un ejemplo de regla de correlación de inicio de sesión denominada `LoginCorrelationRules.xml`.

Tras crear una regla de correlación personalizada, debe importarla a Identity Manager. En la interfaz de administración, seleccione Configurar y después Importar archivo de intercambio para usar la utilidad de importación.

Verificación de la conexión SSL

Para verificar la conexión SSL, acceda a la URL de la interfaz de la aplicación configurada mediante SSL (por ejemplo, `https://idm007:7002/idm/user/login.jsp`). Se le advertirá que está entrando en un sitio seguro y luego se le pedirá que elija un certificado personal para enviarlo al servidor web.

Diagnóstico de problemas

Puede informar sobre los problemas de autenticación utilizando los certificados X509 como mensajes de error en el formulario de inicio de sesión.

Para realizar diagnósticos más completos, habilite el seguimiento en el servidor de Identity Manager para estas clases y niveles:

- `com.waveset.session.SessionFactory 1`
- `com.waveset.security.authn.WSX509CertLoginModule 1`
- `com.waveset.security.authn.LoginModule 1`

Si el atributo de certificado de cliente tiene un nombre distinto a `javaxservlet.request.X509Certificate` en la solicitud HTTP, un mensaje le advertirá que este atributo no se puede encontrar dicho atributo en la solicitud HTTP.

▼ Para corregir un nombre de atributo de certificado de cliente en una solicitud HTTP

1. **Habilite el seguimiento de `SessionFactory` para ver la lista completa de atributos HTTP y averiguar el nombre del certificado X509.**
2. **Con la utilidad de depuración de Identity Manager ("Página de depuración de Identity Manager" en la página 45), edite el objeto `LoginConfig`.**
3. **Cambie el nombre de `<AuthnProperty>` en `<LoginConfigEntry>` por el nombre correcto para el Módulo de inicio de sesión con certificado X509 de Identity Manager.**
4. **Guarde y vuelva a intentarlo.**

   Quizá también necesite suprimir y después volver a añadir el Módulo de inicio de sesión con certificado X509 de Identity Manager en la aplicación de inicio de sesión.

Uso y administración del cifrado

El cifrado sirve para garantizar la confidencialidad y la integridad de los datos del servidor en la memoria y en el depósito, así como todos los datos transmitidos entre el servidor y la puerta de enlace de Identity Manager.

Los próximos apartados contienen más información sobre el uso y la administración del cifrado en el servidor y la puerta de enlace de Identity Manager, con respuestas a preguntas sobre las claves de cifrado de ambos.

Datos protegidos mediante cifrado

En la tabla siguiente se enumeran los tipos de datos protegidos mediante cifrado en el producto Identity Manager, incluidos los tipos de cifrado con que se protegen.

TABLA 12–1 Tipos de datos protegidos mediante cifrado

Tipo de datos	RSAMD5	Clave NIST Triple DES de 168 Bits (DESede/ECB/NoPadding)	Clave de cifrado de 56 bits basada en contraseña PKCS#5 (PBEwithMD5andDES)
Claves de cifrado de servidor		predeterminado	opción de configuración
Claves de cifrado de puerta de enlace		predeterminado	opción de configuración 1

TABLA 12–1 Tipos de datos protegidos mediante cifrado *(Continuación)*

Tipo de datos	RSAMD5	Clave NIST Triple DES de 168 Bits (DESede/ECB/NoPadding)	Clave de cifrado de 56 bits basada en contraseña PKCS#5 (PBEwithMD5andDES)
Palabras del diccionario de directivas	sí		
Contraseñas de usuario		sí	
Historial de contraseñas de usuario		sí	
Respuestas de usuario		sí	
Contraseñas de recurso		sí	
Historial de contraseñas de recurso	sí		
Toda la carga útil entre el servidor y las puertas de enlace		sí	

Preguntas frecuentes sobre claves de cifrado de servidor

A continuación encontrará respuestas a preguntas frecuentes sobre el origen de las claves de cifrado de servidor, su ubicación, mantenimiento y uso.

Pregunta: ¿De dónde proceden las claves de cifrado de servidor?

Respuesta: Las claves de cifrado de servidor son claves Triple-DES simétricas de 168 bits.

El servidor admite dos tipos de claves:

- **Clave predeterminada**. La clave se compila en el código del servidor.
- **Clave generada aleatoriamente**. Esta clave puede generarse la primera vez que se inicia el servidor o siempre que se cuestiona la clave actual.

Pregunta: ¿Dónde se mantienen las claves de cifrado de servidor?

Respuesta: Las claves de cifrado de servidor son objetos que se mantienen en el depósito. Cualquier depósito puede contener muchas claves de cifrado.

Pregunta: ¿Cómo sabe el servidor qué clave utilizar para descifrar y volver a cifrar datos cifrados?

Respuesta: Cada dato cifrado que se almacena en el depósito va precedido por el ID de la clave de cifrado del servidor utilizada para cifrarlo. Cuando un objeto que contiene datos cifrados se lee

en la memoria, Identity Manager utiliza la clave de cifrado de servidor asociada al ID que precede a los datos cifrados para descifrarlos y después vuelve a cifrarlos con la misma clave si los datos han cambiado.

Pregunta: ¿Cómo se actualizan las claves de cifrado de servidor?

Respuesta: Identity Manager ofrece una tarea llamada Administrar el cifrado del servidor.

Esta tarea permite que un administrador de seguridad autorizado realice diversas tareas de administración de claves, incluidas:

- Generar una nueva clave de servidor "actual".
- Volver a cifrar por tipo objetos existentes que contienen datos cifrados con la clave de servidor "actual".

Encontrará más información sobre el uso de esta tarea dentro de la sección "Administración de cifrado del servidor" en la página 425 en este mismo capítulo.

Pregunta: ¿Qué sucede con los datos cifrados existentes si cambia la clave de servidor "actual"?

Respuesta: Nada. Los datos cifrados se descifran o vuelven a cifrar igualmente con la clave referenciada por el ID que les precede. Si se genera una nueva clave de cifrado de servidor y se define como clave "actual", todos los nuevos datos que se cifren utilizarán la nueva clave de servidor.

A fin de evitar problemas por exceso de claves y de mantener un mayor grado de integridad de los datos, utilice la tarea Administrar el cifrado del servidor para volver a cifrar todos los datos cifrados existentes con la clave de cifrado de servidor "actual".

Pregunta: ¿Qué sucede cuando se importan datos cifrados para los que no hay disponible una clave de cifrado?

Respuesta: Si importa un objeto que contiene datos cifrados con una clave que no se encuentra en el depósito al que se importa, los datos se importarán, pero no se descifrarán.

Pregunta: ¿Cómo se protegen las claves de servidor?

Respuesta: Si el servidor no está configurado para utilizar el cifrado PKCS#5 basado en contraseña (PBE), que se define en el objeto de configuración del sistema mediante el atributo `pbeEncrypt` o la tarea Administrar el cifrado del servidor, las claves de servidor se cifran utilizando la clave predeterminada. La clave predeterminada es la misma para todas las instalaciones de Identity Manager.

Si el servidor está configurado para utilizar cifrado PBE, se genera una clave PBE cada vea que se inicia el servidor. La clave PBE se genera suministrando al algoritmo de cifrado PBEwithMD5andDES una contraseña, generada a partir de un secreto específico del servidor. La clave PBE se mantiene sólo en la memoria y nunca persiste. Además, la clave PBE es igual para todos los servidores que comparten un depósito común.

Para habilitar el cifrado PBE de las claves de servidor, debe estar disponible el algoritmo de cifrado PBEwithMD5andDES. Identity Manager no ofrece este algoritmo de manera

predeterminada, pero es un estándar PKCS#5 presente en las implementaciones de muchos proveedores de JCE, como los que suministran Sun e IBM.

Pregunta: ¿Puedo exportar las claves de servidor para proteger el almacenamiento externo?

Respuesta: Sí. Si las claves de servidor se cifran mediante PBE, antes de exportarlas se descifrarán y volverán a cifrar con la clave predeterminada. Ello permite importarlas más adelante al mismo servidor o a otro distinto, con independencia de la clave PBE del servidor local. Si las claves de servidor se cifran con la clave predeterminada, no se preprocesan antes de exportarlas.

Cuando se importan a un servidor, si éste se ha configurado para claves PBE, las claves se descifran y se vuelven a cifrar con la clave PBE del servidor local, en caso de que dicho servidor esté configurado para cifrado de claves PBE.

Pregunta: ¿Qué datos se cifran entre el servidor y la puerta de enlace?

Respuesta: Todos los datos (carga útil) transmitidos entre el servidor y la puerta de enlace se cifran en Triple-DES con una clave de 168 bits simétrica generada aleatoriamente por sesión servidor-puerta de enlace.

Preguntas frecuentes sobre claves de puerta de enlace

A continuación encontrará respuestas a preguntas frecuentes sobre el origen de las claves de puerta de enlace, su almacenamiento, distribución y protección.

Pregunta: ¿De dónde proceden las claves de puerta de enlace para cifrar o descifrar los datos?

Respuesta: Cada vez que un servidor de Identity Manager se conecta a una puerta de enlace, el protocolo de enlace inicial genera aleatoriamente una nueva clave de sesión Triple-DES de 168 bits. Esta clave sirve para cifrar o descifrar todos los datos que se transmitan después entre ese servidor y esa puerta de enlace. Por cada par servidor/puerta de enlace se genera una única clave de sesión.

Pregunta: ¿Cómo se distribuyen las claves de puerta de enlace a las puertas de enlace?

Respuesta: El servidor genera aleatoriamente las claves de sesión, que después se intercambian de manera segura entre el servidor y la puerta de enlace cifrándolas con la clave maestra secreta compartida dentro del protocolo de enlace inicial servidor-a-puerta de enlace.

Cuando se ejecuta el protocolo de enlace inicial, el servidor consulta la puerta de enlace para determinar qué modo admite. La puerta de enlace puede operar en dos modos.

- **Modo predeterminado**. El protocolo de enlace inicial nombre de servidor-a-puerta de enlace se cifra con la clave predeterminada Triple-DES de 168 bits, que se compila en el código del servidor.

- **Modo seguro**. Dentro del protocolo de enlace inicial, el servidor genera y comunica a la puerta de enlace una clave de puerta de enlace Triple-DES aleatoria de 168 bits por depósito compartido. Esta clave de puerta de enlace se almacena en el depósito del servidor igual que otras claves de cifrado, y también la almacena la puerta de enlace en su registro local.

  Cuando un servidor entra en contacto con una puerta de enlace en el modo seguro, el servidor cifra datos de prueba con la clave de la puerta de enlace y los envía a la puerta de enlace. A continuación, la puerta de enlace intenta descifrar los datos de prueba, agrega algunos datos exclusivos de la puerta de enlace a los datos de prueba, vuelve a cifrar ambos y los devuelve al servidor. Si el servidor descifra satisfactoriamente los datos de prueba y los exclusivos de la puerta de enlace, genera la clave de sesión única servidor-puerta de enlace, la cifra con la clave de la puerta de enlace y la envía a la puerta de enlace. Cuando la recibe, la puerta de enlace descifra la clave de sesión y la conserva para utilizarla mientras dure la sesión servidor-a-puerta de enlace. Si el servidor no puede descifrar satisfactoriamente los datos de prueba y los exclusivos de la puerta de enlace, cifra la clave de la puerta de enlace utilizando la clave predeterminada y la envía a la puerta de enlace. La puerta de enlace descifra la clave de la puerta de enlace aplicando su clave predeterminada y la almacena en su registro. A continuación, el servidor cifra la clave de sesión única servidor-puerta de enlace y la envía a la puerta de enlace para utilizarla mientras dure la sesión servidor-a-puerta de enlace.

  A partir de entonces, la puerta de enlace sólo aceptará solicitudes de los servidores que hayan cifrado la clave de sesión con su clave de puerta de enlace. Al iniciar, la puerta de enlace verifica si el registro contiene una clave. Si hay una clave, la puerta de enlace la utiliza. Si no hay ninguna clave, la puerta de enlace utiliza la clave predeterminada. Una vez que la puerta de enlace tiene definida una clave en el registro, deja de permitir que se establezcan sesiones utilizando la clave predeterminada, lo que impide que alguien configure un servidor malintencionado y establezca una conexión con una puerta de enlace.

Pregunta: ¿Puedo actualizar las claves de puerta de enlace utilizadas para cifrar o descifrar la carga útil servidor-a-puerta de enlace?

Respuesta: Identity Manager ofrece una tarea llamada Administrar el cifrado del servidor, que permite a un administrador de seguridad autorizado efectuar diversas tareas de administración de claves, incluida la generación de una nueva clave de puerta de enlace "actual" y la actualización de todas las puertas de enlace con dicha clave. Dicha clave se utiliza para cifrar la clave por sesión que sirve para proteger toda la carga útil transmitida entre el servidor y la puerta de enlace. La clave de puerta de enlace recién generada se cifra con la clave predeterminada o la clave PBE, según el valor que tenga el atributo `pbeEncrypt` en la configuración del sistema ("Edición de objetos de configuración de Identity Manager" en la página 118).

Pregunta: ¿Dónde se almacenan las claves de puerta de enlace en el servidor y en la puerta de enlace?

Respuesta: En el servidor, la clave de puerta de enlace se almacena en el depósito, igual que las claves de servidor. En el la puerta de enlace, la clave de puerta de enlace se almacena en una clave de registro local.

Pregunta: ¿Cómo se protegen las claves de puerta de enlace?

Respuesta: Las claves de puerta de enlace se protegen del mismo modo que las de servidor. Si el servidor está configurado para usar cifrado PBE, la clave de la puerta de enlace se cifrará con una clave generada mediante PBE. Si la opción está definida en false, se cifrará con la clave predeterminada. Encontrará más información dentro de "Preguntas frecuentes sobre claves de cifrado de servidor" en la página 421.

Pregunta: ¿Puedo exportar la clave puerta de enlace para proteger el almacenamiento externo?

Respuesta: La clave de puerta de enlace se puede exportar con la tarea Administrar el cifrado del servidor, igual que las claves de servidor. Encontrará más información dentro de "Preguntas frecuentes sobre claves de cifrado de servidor" en la página 421.

Pregunta: ¿Cómo se destruyen las claves de servidor y de puerta de enlace?

Respuesta: Las claves de servidor y de puerta de enlace se destruyen eliminándolas del depósito del servidor. Recuerde que no se debe eliminar una clave mientras aún haya datos del servidor cifrados con dicha clave o alguna puerta de enlace que dependa de ella. Utilice la tarea Administrar el cifrado del servidor para volver a cifrar todos los datos del servidor con la clave de servidor actual y para sincronizar la clave de puerta de enlace actual con todas las puertas de enlace a fin de asegurarse de que no se siguen utilizando claves obsoletas antes de borrarlas.

Administración de cifrado del servidor

La funcionalidad de cifrado de servidor de Identity Manager permite crear nuevas claves de cifrado de servidor 3DES y cifrarlas con 3DES, PKCS#5 o AES (estándar de cifrado avanzado). Sólo los usuarios con capacidades de administrador de seguridad pueden ejecutar la tarea Administrar el cifrado del servidor, que se configura en la página Administrar el cifrado del servidor.

▼ Para acceder a la página Administrar el cifrado del servidor

Para abrir la página Administrar el cifrado del servidor

1 **Seleccione Tareas del servidor > Ejecutar tareas en la barra de menús.**

2 **Cuando aparezca la página Tareas disponibles, haga clic en Administrar el cifrado del servidor para abrir la página del mismo nombre.**

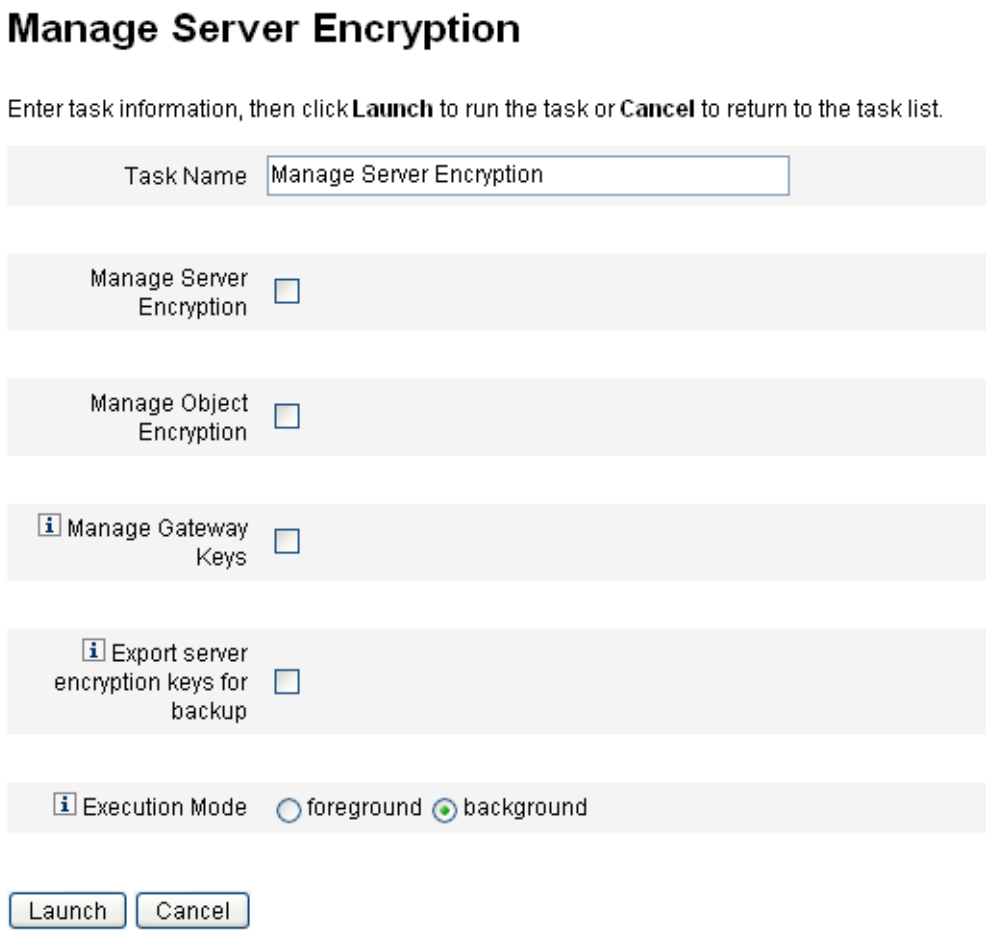


FIGURA 12–1 Página Administrar el cifrado del servidor

▼ Para configurar el cifrado del servidor

Use esta página para configurar el cifrado del servidor y de los objetos, claves de puerta de enlace, opciones de copia de seguridad y el modo de ejecución.

1 **Introduzca un Nombre de tarea.**

El valor predeterminado de este campo es *Administrar el cifrado del servidor*. Si no quiere utilizar el valor predeterminado, puede introducir otro nombre de tarea.

2 **Elija una o varias de las siguientes opciones.**

selección,

- **Administrar el cifrado del servidor**. Seleccione esta opción para configurar el cifrado del servidor.

  Aparecen estas otras opciones:

  - **Cifrado de las claves de cifrado del servidor**. Debe especificar un método para cifrar las claves de cifrado de servidor. Los tipos de cifrado pueden ser Triple DES, PKCS#5 (DES) o PKCS#5 (AES).

Nota –

- En esta página sólo aparecen los tipos de cifrado que pueden instanciarse en el sistema. Por ejemplo, si su sistema no admite PKCS#5 (AES), sólo aparecen Triple DES y PKCS#5 (DES).
- PKCS#5 (AES) requiere descargar y configurar "Unlimited Strength Jurisdiction Policy Files" para la máquina JVM que ejecuta Identity Manager. Encontrará más información en la documentación del proveedor de Java.

  Asimismo, PKCS#5 (AES) requiere instalar y configurar el archivo `jar` `Bouncy Castle` `JCE` `provider` como proveedor de JCE provider para la máquina JVM que ejecuta Identity Manager. Este archivo `jar` se empaqueta en la imagen de instalación de Identity Manager y puede encontrarse en el directorio *wshome*`/WEB-INF/lib`. Se incluyen dos archivos `jar` para usarlos con las correspondientes versiones de Java: `bcprov-jdk15-137.jar` y `bcprov-jdk16-137.jar`. Encontrará más información en la documentación del proveedor de Java y en la de Bouncy Castle.

- **Generar nueva clave de cifrado de servidor y definir como clave actual**. Seleccione esta opción para generar una nueva clave de cifrado de servidor. Cada unidad de datos cifrados generados después de esta selección se cifrará con esa clave. La creación de una nueva clave de cifrado de servidor no afecta a la clave aplicada a los datos cifrados existentes.
- **Genera una nueva contraseña PBE aleatoria segura**. Esta opción genera una contraseña nueva basada en un secreto específico del servidor cada vez que se inicia éste. Si no elige esta opción, o si el servidor no está configurado para utilizar cifrado basado en contraseña, Identity Manager utilizará la clave predeterminada para cifrar las claves de servidor.

- **Administrar cifrado de objetos**. Esta opción sirve para especificar los tipos de objetos que deben volverse a cifrar y el método cifrado que se utiliza.
  - **Cifrado de tipos de objeto** Elija uno de los tipos de cifrado mostrados, que pueden ser: Triple DES (predeterminado), clave AES de 256 bits, clave AES de 192 bits o clave AES de 128 bits.

    Nota – Para usar claves AES de 192 o 256 bits es preciso descargar y configurar "Unlimited Strength Jurisdiction Policy Files" para la máquina JVM que ejecuta Identity Manager. Encontrará más información en la documentación del proveedor de Java.

    En esta página sólo aparecen los tipos de cifrado que pueden instanciarse en el sistema. Por ejemplo, si el sistema no admite claves AES de 192 o 256 bits con "Unlimited Strength Jurisdiction Policy Files", sólo se verán las opciones de claves Triple DES y AES de 128 bits.

  - **Seleccione los tipos de objeto que quiere volver a cifrar con la nueva clave de cifrado del servidor**. Elija uno o más de los tipo de objeto de Identity Manager incluidos en la tabla.
- **Administrar las claves de puerta de enlace**. Seleccione esta opción para configurar el cifrado de la puerta de enlace.

  Aparecen estas opciones:
  - **Opción de selección de claves de puerta de enlace**. Elija una de estas opciones:
    - **Generar una nueva clave y sincronizar todas las puertas de enlace**. Seleccione esta opción cuando habilite por primera vez un entorno de puerta de enlace seguro. Esta opción genera una nueva clave de puerta de enlace y la comunica a todas las puertas de enlace.
    - **Sincronizar todas las puertas de enlace con la clave de puerta de enlace actual**. Seleccione esta opción para sincronizar cualquier puerta de enlace nueva o aquellas puertas de enlace que no han comunicado la nueva clave de puerta de enlace. Seleccione esta opción si tenía una puerta de enlace que estaba inactiva cuando todas las puertas de enlace se sincronizaron con la clave de puerta de enlace actual. También puede seleccionarla cuando desee forzar una actualización de clave para una nueva puerta de enlace.
  - **Tipo de clave de puerta de enlace**. Elija uno de los tipos de clave mostrados, que pueden ser: Triple DES, clave AES de 256 bits, clave AES de 192 bits o clave AES de 128 bits.

Nota – Para usar claves AES de 192 o 256 bits es preciso descargar y configurar "Unlimited Strength Jurisdiction Policy Files" para la máquina JVM que ejecuta Identity Manager. Encontrará más información en la documentación del proveedor de Java.

En esta página sólo aparecen los tipos de cifrado que pueden instanciarse en el sistema. Por ejemplo, si el sistema no admite claves AES de 192 o 256 bits con "Unlimited Strength Jurisdiction Policy Files", sólo se verán las opciones de claves Triple DES y AES de 128 bits.

- **Exportar las claves de cifrado del servidor para copias de seguridad**. Seleccione esta opción para exportar las claves de cifrado de servidor existentes a un archivo con el formato XML. Al seleccionar esta opción, Identity Manager muestra un campo adicional para que especifique la ruta y el nombre de archivo al que exportar las claves.

  Nota – Seleccione también esta opción si utiliza el cifrado PKCS#5 y decide generar y definir una nueva clave de cifrado de servidor. Además, debería almacenar las claves exportadas en soportes extraíbles y en una ubicación segura (no en una red).

3. **Elija el modo de ejecución.**

   Esta tarea se puede ejecutar en primer o segundo plano (valor predeterminado).

   Nota – Si decide volver a cifrar uno o varios tipos de objetos con una clave nueva, esta tarea puede llevar algo de tiempo y sería recomendable que se ejecutase en segundo plano.

4. **Cuando termine de configurar las opciones de esta página, pulse Iniciar.**

Uso de tipos de autorización para proteger los objetos

Los permisos especificados en una capacidad `AdminGroup` suelen emplearse para conceder acceso a un tipo de objeto (`objectType`) de Identity Manager, como Configuración, Regla o `TaskDefinition`. Sin embargo, conceder acceso a todos los objetos de un tipo (`objectType`) de Identity Manager dentro de una o más organizaciones controladas a veces resulta demasiado genérico.

Los tipos de autorización (`AuthType`) permiten delimitar o restringir más este acceso a un subconjunto de objetos para un determinado tipo de de objeto (`objectType`) de Identity Manager. Por ejemplo, quizá no le interese que sus usuarios tengan acceso a todas las reglas de su ámbito de control cuando se rellenan reglas para seleccionar en un formulario de usuario.

Para definir un nuevo tipo de autorización, edite el objeto de configuración `AuthorizationTypes` en el depósito de Identity Manager y agregue un nuevo elemento `<AuthType>`.

Este elemento requiere dos propiedades:

- El nombre del nuevo tipo de autorización.
- El tipo de autorización u `objectType` existente que amplía o delimita el nuevo elemento.

Por ejemplo, si desea agregar un nuevo tipo de autorización de regla denominado `Marketing Rule` para ampliar `Rule`, deberá definir lo siguiente:

```
<AuthType name='Marketing Rule' extends='Rule'/>
```

A continuación, para habilitar el tipo de autorización que se debe usar, hay que referenciarlo en dos sitios:

- Dentro de una capacidad `AdminGroup` personalizada que conceda uno o más derechos al nuevo tipo de autorización.
- Dentro de los objetos que deben ser de ese tipo.

Los siguientes ejemplos corresponden a ambas referencias. El primero muestra una definición de capacidad `AdminGroup` que concede acceso a `Marketing Rules`.

EJEMPLO 12–4 Definición de capacidad `AdminGroup`

```
<AdminGroup name='Marketing Admin'>
  <Permissions>
    <Permission type='Marketing Rule' rights='View,List,Connect,Disconnect/>
  </Permissions>
  <AdminGroups>
    <ObjectRef type='AdminGroup' id='#ID#Account Administrator'/>
  </AdminGroups>
</AdminGroup>
```

El siguiente ejemplo muestra una definición de regla (`Rule`) que permite a los usuarios acceder al objeto, porque disponen de acceso a `Rule` o `Marketing Rule`.

EJEMPLO 12–5 Definición de `Rule`

```
<Rule name='Competitive Analysis Info' authType='Marketing Rule'>
 ...
</Rule>
```

Nota – Todos los derechos de usuario concedidos para un tipo de autorización principal, o para un tipo estático ampliado por un tipo de autorización, son los mismos derechos para todos los tipos de autorización secundarios. Por tanto, en el ejemplo anterior, todos los derechos de usuario concedidos para `Rule` serán los mismos para `Marketing Rule`. En cambio, lo contrario no es cierto.

Prácticas de seguridad

Como administrador de Identity Manager, reducirá aún más los riesgos de seguridad para las cuentas y los datos protegidos si sigue las recomendaciones indicadas a continuación, tanto al configurar como después.

Al configurar

Para reducir los riesgos de seguridad durante la configuración:

- Acceda a Identity Manager a través de un servidor web seguro por HTTPS.
- Reinicialice las contraseñas para las cuentas de administrador de Identity Manager predeterminadas (Administrador y Configurador). Para preservar aún más la seguridad de esas cuentas, puede cambiar sus nombres.
- Limite el acceso a la cuenta de configurador.
- Limite las capacidades de los administradores exclusivamente a las acciones necesarias ejercer sus funciones, configurando jerarquías organizativas para limitar dichas capacidades.
- Cambie la contraseña predeterminada del depósito de índices de Identity Manager.
- Active la auditoría para rastrear las actividades en la aplicación de Identity Manager.
- Edite los permisos sobre los archivos en el directorio de Identity Manager.
- Personalice los flujos de trabajo para insertar aprobaciones u otros puntos de control.
- Establezca un procedimiento de recuperación para detallar cómo se debe recuperar el entorno de Identity Manager en caso de emergencia.

Durante el uso

Para reducir los riesgos de seguridad durante el uso:

- Cambie periódicamente las contraseñas para las cuentas de administrador de Identity Manager predeterminadas (Administrador y Configurador).
- Cierre la sesión de Identity Manager cuando no se esté usando activamente el sistema.

- Defina o determine el tiempo de espera predeterminado para una sesión de Identity Manager. Los valores de tiempo de espera de sesión pueden variar, porque se pueden configurar por separado para cada aplicación de inicio de sesión.

Si su servidor de aplicaciones es conforme con Servlet 2.2, el proceso de instalación de Identity Manager configurará el tiempo de espera de sesión de HTTP en un valor predeterminado de 30 minutos. Este valor se puede cambiar editando la propiedad, pero conviene que sea un valor bajo para elevar la seguridad. No defina un valor superior a 30 minutos.

▼ Para cambiar el valor de tiempo de espera de sesión

1. **Edite el** `archivo web.xml`**, que se encuentra en el directorio** `idm/WEB-INF` **del árbol de directorios del servidor de aplicaciones.**

2. **Cambie el valor numérico en las líneas siguientes:**

```
<session-config>  <session-timeout>30</session-timeout></session-config>
```

◆ ◆ ◆ CAPÍTULO 13

Auditoría de identidades: Conceptos básicos

En este capítulo presentamos los conceptos básicos sobre auditoría de identidades y controles de auditoría. Los controles de auditoría permiten supervisar y administrar la auditoría y el cumplimiento en todos los sistemas de información y las aplicaciones de la empresa.

En este capítulo se explican los siguientes conceptos y tareas:

Qué es la auditoría de identidades

En Identity Manager, *auditar* es capturar, analizar y responder sistemáticamente a los datos de identidad en toda la empresa para garantizar el cumplimiento de las normativas y directivas internas y externas.

No es fácil respetar la legislación sobre la privacidad de los datos y las cuentas. Las funciones de auditoría de Identity Manager tienen un enfoque flexible que le permite implementar una solución de cumplimiento apropiada para su empresa.

En la mayoría de los entornos hay distintos grupos implicados en el cumplimiento: equipos de auditoría internos y externos (cuyo interés primordial es auditar), y el personal ajeno a la auditoría (que pueden considerarla motivo de distracción). El departamento de TI también suele intervenir en el cumplimiento, ayudando en la transición de los requisitos del equipo de auditoría interno hasta la implementación de la solución elegida. La clave para implementar con éxito una solución de auditoría estriba en capturar con precisión los conocimientos, controles y procesos del personal ajeno a la auditoría, para después automatizar la aplicación de dicha información.

Finalidad de la auditoría de identidades

La auditoría de identidades eleva el rendimiento de la auditoría así:

- *La auditoría de identidades detecta automáticamente las infracciones de cumplimiento y facilita su remediación rápida mediante notificaciones inmediatas.*

  Las funciones de directivas de auditoría de Identity Manager permiten definir *reglas* (criterios) para las infracciones. Una vez definidas, el sistema busca condiciones que infringen las directivas establecidas, como el acceso sin autorización o los privilegios de acceso erróneos. Cuando las detecta, el sistema notifica a las personas pertinentes siguiendo una cadena de escalada establecida. A continuación, la infracción se puede remediar (corregir) mediante tareas invocadas por el usuario o flujos de trabajo que se invocan automáticamente al infringir las directivas.

- *Proporciona información fundamental específica sobre la efectividad de los controles de auditoría internos.*

  Los Informes de Auditor resumen la información de estado sobre las infracciones y las excepciones para analizar rápidamente el de riesgo. La ficha Informes también ofrece informes gráficos sobre las infracciones. Las infracciones se pueden visualizar por recurso, organización o directiva, personalizando cada gráfico según las características definidas para el informe.

- *Automatiza las revisiones de certificación de los controles de identidades para reducir el riesgo operativo.*

  Las capacidades de flujo de trabajo permiten automatizar la notificación de las infracciones de directivas y de acceso a los revisores seleccionados.

- *Elabora informes completos y detallados sobre la actividad de los usuarios que cumplen los requisitos de las normativas.*

  El área Informes permite definir informes y gráficos detallados con información sobre el historial y los privilegios de acceso, así como otras infracciones de directivas. El sistema efectúa un seguimiento de la auditoría de identidades seguro y completo, que mediante las capacidades de exportación se puede extraer para actualizar el acceso a los datos y los perfiles de usuario.

- *Agiliza las revisiones periódicas para respetar continuamente la seguridad y el cumplimiento de las normativas.*

  Se pueden realizar revisiones de acceso periódicas para recopilar registros de los derechos de usuario y averiguar cuáles deben revisarse. A continuación, el proceso notifica a los autenticadores designados las solicitudes de revisión pendientes y actualiza el estado de las solicitudes pendientes una vez que los autenticadores han terminado de actuar sobre ellas.

- *Identifica posibles conflictos de intereses en las cuentas de usuario.*

  Identity Manager ofrece un informe Separación de tareas que muestra los usuarios con determinadas capacidades o privilegios que podrían producir conflictos de intereses.

Cómo funciona la auditoría de identidades

Identity Manager incluye una función para auditar los derechos de acceso y los privilegios de las cuentas de usuario, y otra distinta para respetar y certificar el cumplimiento. Estas funciones son el cumplimiento basado en directivas y las revisiones de acceso periódicas.

Cumplimiento basado en directivas

Identity Manager utiliza un sistema de directivas de auditoría que permite a los administradores mantener el cumplimiento de los requisitos establecidos por la empresa en todas las cuentas de usuario.

Las directivas de auditoría se pueden utilizar para garantizar el cumplimiento de dos maneras distintas y complementarias: cumplimiento continuo y periódico.

Ambas técnicas se complementan especialmente en los entornos donde se pueden abastecer operaciones fuera de Identity Manager. El cumplimiento periódico es necesario cuando es posible cambiar una cuenta mediante un proceso que no ejecuta o respeta las directivas de auditoría existentes.

Cumplimiento continuo

Cumplimiento continuo significa que se aplica una directiva de auditoría a todas las operaciones de abastecimiento, de manera que no es posible modificar una cuenta sin cumplir la directiva actual.

Para habilitar el cumplimiento continuo, se asigna una directiva de auditoría a una organización, a un usuario o a ambos. Cualquier operación de abastecimiento aplicada a un usuario ocasionará la evaluación de las directivas asignadas al usuario. Siempre que se incumpla una directiva, se interrumpirá la operación de abastecimiento.

Se define jerárquicamente un conjunto de directivas *por organización*. Sólo se aplica un conjunto de directivas por organización a cualquier usuario. El conjunto de directivas que se aplica es el que está asignado a la organización de nivel inferior. Por ejemplo:

Organización	Conjunto de directivas asignado directamente	Directiva vigente
Austin	Directivas A1, A2	Directivas A1, A2
Marketing		Directivas A1, A2
Desarrollo	Directivas B, C2	Directivas B, C2
Asistencia		Directivas B, C2

Organización	Conjunto de directivas asignado directamente	Directiva vigente
Pruebas	Directivas D, E5	Directivas D, E5
Financiera		Directivas A1, A2
Houston		<ninguna>

Cumplimiento periódico

Cumplimiento periódico significa que Identity Manager evalúa la directiva conforme es necesario. Todas las condiciones de incumplimiento se capturan como infracciones de cumplimiento.

Al ejecutar análisis de cumplimiento periódicos, se pueden seleccionar las directivas implicadas. El proceso de análisis combina las directivas asignadas directamente (a usuarios y organizaciones) y un conjunto arbitrario de directivas seleccionadas.

Los usuarios de Identity Manager con capacidades de Administrador del Auditor pueden crear directivas de auditoría y supervisar su cumplimiento ejecutando periódicamente análisis de las directivas y revisiones de sus infracciones. Las infracciones se pueden administrar mediante procedimientos de remediación y mitigación.

Para obtener más información sobre las capacidades de Administrador del Auditor, consulte "Conceptos y administración de capacidades" en la página 216 en el Capítulo 6, "Administración".

La auditoría de Identity Manager permite realizar análisis periódicos de los usuarios. En ellos se ejecutan directivas de auditoría para detectar posibles desviaciones respecto a los límites de cuenta establecidos. Cuando se detecta una infracción, se inician actividades para remediarla. Pueden aplicarse reglas de directiva de auditoría estándar de Identity Manager o reglas personalizadas definidas por el usuario.

Flujo de tareas lógico del cumplimiento basado en directivas

La Figura 13–1 ilustra un flujo de tareas lógico para establecer controles de auditoría basados en directivas.

Revisiones de acceso periódicas

Identity Manager ofrece revisiones de acceso periódicas con las que los administradores y otros responsables pueden revisar y verificar los privilegios de acceso de los usuarios puntual o periódicamente. Encontrará más información sobre esta función en "Revisiones de acceso periódicas y autenticación" en la página 480.

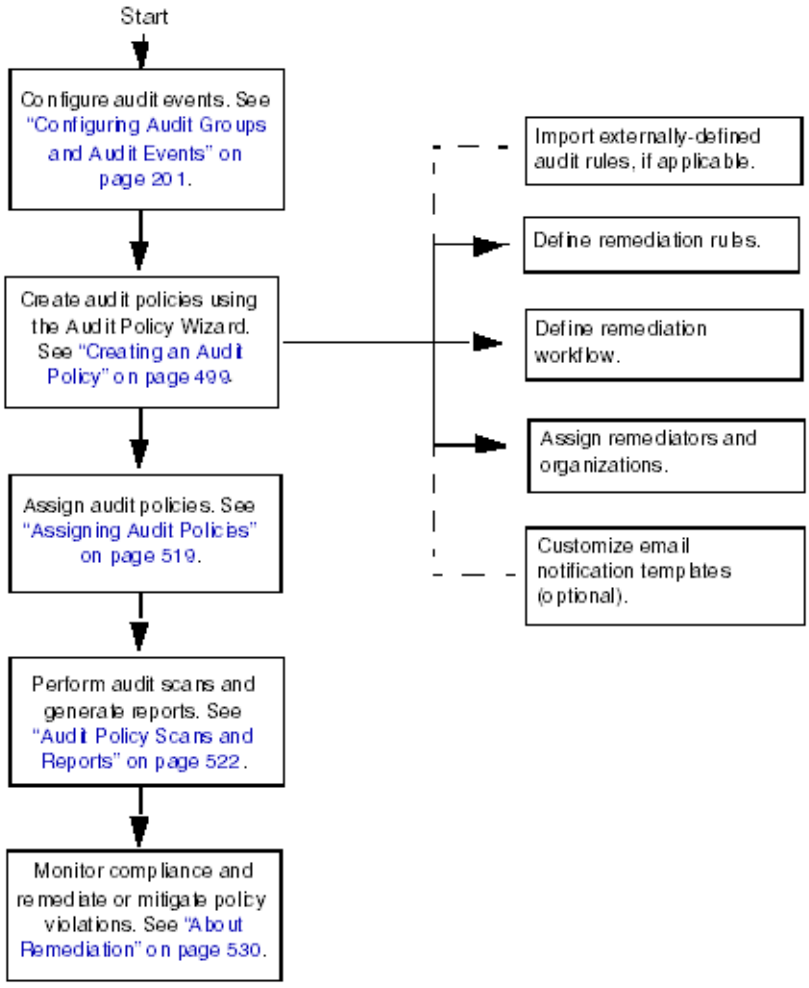


FIGURA 13–1 Flujo de tareas lógico para establecer el cumplimiento basado en directivas

Uso de auditoría de identidades en la interfaz de administración

En esta sección se explica cómo acceder a las funciones de auditoría de identidades en la interfaz de administración. También se tratan las plantillas de notificación por correo electrónico utilizadas en la auditoría de identidades.

La sección Cumplimiento de la interfaz

Las directivas de auditoría se crean y administran en la sección Cumplimiento de la interfaz de administración de Identity Manager.

▼ Para crear y administrador directivas de auditoría en la sección Cumplimiento

1 **Inicie la sesión en la interfaz de administración ("Inicio de sesión en la interfaz de usuario final de Identity Manager" en la página 43).**

2 **Elija Cumplimiento en la barra de menús.**

La sección Cumplimiento ofrece estas fichas secundarias (o elementos de menú):

- Administrar directivas
- Administrar exploraciones de acceso
- Revisiones de acceso

Administrar directivas

La página Administrar directivas muestra las directivas que tiene permiso para ver y editar. En esta área también puede administrar las exploraciones de acceso.

Desde la página Administrar directivas puede utilizar directivas de auditoría para efectuar estas tareas:

- Crear una directiva de auditoría.
- Seleccionar una directiva para ver o editar.
- Eliminar una directiva.

Encontrará información detallada sobre estas tareas dentro de unas páginas en la sección "Ejemplo de escenario de directiva de auditoría " en la página 441.

Administrar exploraciones de acceso

La ficha Administrar exploraciones de acceso sirve para crear, modificar y eliminar las exploraciones de acceso. En ella puede definir exploraciones con el fin de ejecutarlas o programarlas para efectuar revisiones de acceso periódicas. Encontrará más información sobre esta función en "Revisiones de acceso periódicas y autenticación" en la página 480.

Revisiones de acceso

En la ficha Revisiones de acceso puede iniciar, terminar, eliminar y supervisar el progreso de las revisiones de acceso. Muestra un informe resumido con los resultados de las exploraciones y vínculos de información para obtener más detalles sobre las actividades pendientes y el estado de la revisión.

Encontrará más información sobre esta función en "Administración de revisiones de acceso" en la página 491.

Referencia de tareas de auditoría de identidades en la interfaz

Consulte en la Tabla B–8 cómo se realizan otras tareas de auditoría de identidades en la interfaz de administración. Esta referencia rápida le indica desde dónde iniciar diversas tareas de auditoría.

Plantillas de correo electrónico

La auditoría de identidades envía notificaciones por correo electrónico acerca de diversas operaciones. Con cada una de estas notificaciones se utiliza un objeto de plantilla de correo electrónico. Una plantilla de correo electrónico permite personalizar el encabezado y el cuerpo de los mensajes de correo electrónico.

TABLA 13–1 Plantillas de correo electrónico para auditoría de identidades

Nombre de plantilla	Finalidad
Aviso de remediación de revisión de acceso	Lo envía a los remediadores una revisión de acceso cuando se crean inicialmente derechos de usuario en un estado de remediación.
Aviso de autenticación masiva	Lo envía a los autenticadores una revisión de acceso cuando tienen autenticaciones pendientes.
Aviso de infracción de directivas	Lo envía a los remediadores un análisis de directivas de auditoría cuando se producen infracciones.
Aviso de inicio de exploración de acceso	Se envía a un propietario de una exploración de acceso cuando una revisión de acceso inicia una exploración.
Aviso de finalización de exploración de acceso	Se envía a un propietario de una exploración de acceso cuando se termina una exploración de acceso.

Habilitación del registro de auditoría

Antes de empezar a administrar el cumplimiento y las revisiones de acceso, hay que habilitar el sistema de registro de auditoría de Identity Manager y configurarlo para recopilar eventos de auditoría. El sistema de auditoría está habilitado de manera predeterminada. Un administrador de Identity Manager con la capacidad Configurar auditorías puede configurar la auditoría.

Identity Manager proporciona el grupo de configuración de auditoría Administración de cumplimiento.

Siga estos pasos para ver o modificar los eventos almacenados por el grupo Administración de cumplimiento:

1. **Inicie la sesión en la interfaz de administración** ("Inicio de sesión en la interfaz de usuario final de Identity Manager" en la página 43).
2. **Seleccione Configurar en la barra de menús y después Auditoría.**
3. **En la página Configuración de auditoría, seleccione el nombre del grupo de auditoría Administración de cumplimiento.**

Nota –

- Para obtener más información sobre la definición de grupos de auditoría, consulte "Configuración de grupos y eventos de auditoría" en la página 111.
- En el Capítulo 10, "Registro de auditoría", se explica cómo registra los eventos el sistema de auditoría.

Qué son las directivas de auditoría

Una *directiva de auditoría* establece límites de cuenta para un conjunto de usuarios de uno o varios recursos. Incluye *reglas* que definen los límites de una directiva y *flujos de trabajo* para procesar las infracciones después de producirse. Las exploraciones de auditoría aplican los criterios definidos en una directiva de auditoría para evaluar si se han producido infracciones en la organización.

Una directiva de auditoría consta de estos componentes:

- **Reglas de directiva** que definen infracciones específicas. Las reglas de directiva pueden contener funciones escritas en los lenguajes XPRESS, XML Object o JavaScript.
- **Flujo de trabajo de remediación** (opcional), que se inicia cuando una exploración de auditoría detecta una infracción de las reglas de directiva.
- **Remediadores**, usuarios designados que tienen autorización para responder a una infracción de directivas. Los remediadores pueden ser usuarios individuales o grupos de usuarios.

Creación de directivas con reglas de directiva de auditoría

Las reglas definen conflictos potenciales basados en atributos dentro de una directiva de auditoría. Una directiva de auditoría puede contener centenares de reglas que referencien una gran variedad de recursos. Cuando se evalúa una regla, ésta tiene acceso a los datos de las cuentas de usuario de uno o varios recursos. La directiva de auditoría puede restringir los recursos disponibles para la regla.

Es posible tener una regla que verifique un único atributo en un único recurso, o una regla que verifique múltiples atributos en múltiples recursos.

Flujos de trabajo para remediar infracciones de directivas

Después de crear reglas para definir las infracciones de directivas, debe seleccionar el flujo de trabajo que se iniciará siempre que se detecte una infracción durante una exploración de auditoría. Identity Manager incluye un flujo de trabajo predeterminado de remediación estándar, que proporciona un proceso de remediación predeterminado para las exploraciones de directivas de auditoría. Entre otras acciones, este flujo de trabajo de remediación predeterminado genera notificaciones de correo electrónico para cada remediador designado en el nivel 1 (y todos los niveles de remediadores posteriores, si es preciso).

Nota – A diferencia de los procesos de flujo de trabajo de Identity Manager, a los flujos de trabajo de remediación se les debe asignar el tipo de autorización `AuthType=AuditorAdminTask` y el subtipo `SUBTYPE_REMEDIATION_WORKFLOW`. Si va a importar un flujo de trabajo para utilizarlo en exploraciones de auditoría, deberá incluir manualmente este atributo. Encontrará más información en "Importación de reglas de separación de tareas a Identity Manager (opcional)" en la página 445.

Designación de remediadores

Si asigna un flujo de trabajo de remediación, deberá designar al menos un remediador. Puede designar hasta tres niveles de remediadores para una directiva de auditoría. Encontrará más información sobre remediación en "Remediación y mitigación de infracciones del cumplimiento" en la página 470.

Antes de asignar remediadores hay que asignar un flujo de trabajo de remediación.

Ejemplo de escenario de directiva de auditoría

Imagine que se encarga de las cuentas por pagar y por cobrar, y que debe implantar procedimientos para impedir que se acumulen responsabilidades potencialmente arriesgadas en empleados del departamento de contabilidad. Esta directiva debe garantizar que los responsables de cuentas por pagar no tengan también responsabilidades de cuentas por cobrar.

La directiva de auditoría contendrá:

- Un conjunto de reglas. Cada una especifica una condición que constituye una infracción de directivas.
- Un flujo de trabajo que inicia tareas de remediación.
- Un grupo de administradores designados, o remediadores, con permiso para ver y responder ante las infracciones de directivas originadas por las reglas anteriores.

Cuando las reglas identifican infracciones de directivas (en este escenario, usuarios con exceso de autoridad), el flujo de trabajo asociado puede ejecutar tareas específicas relacionadas con la remediación, como notificar automáticamente a los remediadores elegidos.

Los remediadores de nivel 1 son los primeros con quienes se contacta cuando una exploración de auditoría identifica una infracción de directivas. Cuando se supera el periodo de escalada indicado en este área, Identity Manager notifica a los remediadores del nivel siguiente (si se han especificado varios niveles para la directiva de auditoría).

En la próxima sección, “Uso de directivas de auditoría”, se explica cómo utilizar el Asistente de directiva de auditoría para crear una directiva de auditoría.

◆ ◆ ◆ CAPÍTULO 14

Auditoría: Directivas de auditoría

En este capítulo se explica la creación, edición, eliminación y asignación de directivas de auditoría mediante el Asistente de directiva de auditoría.

En este capítulo se explican los siguientes conceptos y tareas:

Uso de directivas de auditoría

Para crear una directiva de auditoría, utilice el Asistente de directiva de auditoría de Identity Manager. Tras definir una directiva de auditoría, puede efectuar diversas acciones con ella, como modificarla o eliminarla.

Reglas de directiva de auditoría

Las reglas de directiva de auditoría definen infracciones específicas. Las reglas de directiva pueden contener funciones escritas en los lenguajes XPRESS, XML Object o JavaScript.

Puede usar el Asistente de directiva de auditoría para crear reglas sencillas, o bien Identity Manager IDE o un editor XML para crear reglas más avanzadas.

- Las reglas deben tener el subtipo `SUBTYPE_AUDIT_POLICY_RULE`. Este subtipo se asigna automáticamente a las reglas generadas por el Asistente de directiva de auditoría.
- Las reglas deben tener el tipo `AuditPolicyRule`. Este tipo de autorización se asigna automáticamente a las reglas generadas por el Asistente de directiva de auditoría.

Las reglas creadas por el Asistente de directiva de auditoría devuelven el valor `true` o `false`. Las reglas de directiva que devuelven `true` producen una infracción de directiva. Sin embargo, con Identity Manager IDE puede crear una regla que omita un usuario durante un análisis de auditoría o una revisión de acceso. Las reglas de directiva de auditoría que devuelven el valor `ignore` dejan de procesarse para ese usuario y pasan al siguiente usuario de destino.

Para obtener más información sobre la creación de reglas de directiva de auditoría, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.

Creación de directivas de auditoría

Para crear una directiva de auditoría, utilice el Asistente de directiva de auditoría.

▼ Para abrir el Asistente de directiva de auditoría

El Asistente de directiva de auditoría le guía por el proceso de creación de una directiva de auditoría. Utilice los pasos siguientes para acceder al asistente:

1. **Inicie la sesión en la interfaz de administración ("Inicio de sesión en la interfaz de usuario final de Identity Manager" en la página 43).**
2. **Haga clic en la ficha Cumplimiento.**

   Se abre la ficha o el menú Administrar directivas.
3. **Para crear una directiva de auditoría nueva, pulse Nuevo.**

Creación de directivas de auditoría: sinopsis

Con el asistente se realizan las siguientes tareas para crear una directiva de auditoría:

- Seleccionar o crear las reglas que se desean aplicar para definir los límites de la directiva.
- Asignar aprobadores y establecer límites de escalada.
- Asignar un flujo de trabajo de remediación.

Tras completar la tarea que aparece en cada pantalla del asistente, pulse Siguiente para continuar con el próximo paso.

Antes de la instalación

Planifique detenidamente la creación de las directivas de auditoría. Antes de empezar, asegúrese de que ha realizado estas tareas:

- Identifique las reglas que va a usar para crear la directiva en el Asistente de directiva de auditoría. Las reglas elegidas dependen del tipo de directiva que se va a crear y de las limitaciones concretas que interesa definir. Encontrará más información dentro del apartado siguiente, "Para identificar qué reglas necesita" en la página 445.
- Importe todas las reglas o flujos de trabajo de remediación que desee incluir en la nueva directiva. Encontrará más información en "Importación de reglas de separación de tareas a Identity Manager (opcional)" en la página 445.
- Asegúrese de que tiene las capacidades necesarias para crear directivas de auditoría. Consulte las capacidades necesarias en "Conceptos y administración de capacidades" en la página 216 dentro del Capítulo 6, "Administración".

▼ Para identificar qué reglas necesita

Las restricciones que especifica en la directiva se implementan en un conjunto de reglas que crea o importa. Siga estos pasos cuando utilice el Asistente de directiva de auditoría para crear una regla:

1. **Identifique el recurso concreto con el que va a trabajar.**
2. **Seleccione un atributo de cuenta en la lista de atributos válidos para el recurso.**
3. **Seleccione una condición para aplicarla al atributo.**
4. **Introduzca un valor de comparación.**

   Para obtener más información sobre la creación de reglas de directiva de auditoría fuera del Asistente de directiva de auditoría, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.

Importación de reglas de separación de tareas a Identity Manager (opcional)

El Asistente de directiva de auditoría no puede crear reglas de separación de tareas. Debe crearlas usted fuera de Identity Manager e importarlas mediante la opción Importar archivo de intercambio de la ficha Configurar.

Importación de flujos de trabajo a Identity Manager (opcional)

▼ Para importar un flujo de trabajo externo

Si desea usar un flujo de trabajo de remediación externo que no está disponible desde Identity Manager, impórtelo. Puede crear flujos de trabajo personalizados con un editor XML editor o Identity Manager IDE.

1. **Defina** `authType='AuditorAdminTask' y agregue subtype='SUBTYPE_REMEDIATION_WORKFLOW'` **. Para definir estos objetos de configuración puede usar Identity Manager IDE o el editor XML que prefiera.**

2. **Importe el flujo de trabajo con la opción Importar archivo de intercambio.**

   a. **Inicie la sesión en la interfaz de administración ("Inicio de sesión en la interfaz de usuario final de Identity Manager" en la página 43).**

   b. **Seleccione la ficha Configurar y después la ficha secundaria o el menú Importar archivo de intercambio.**

      Aparece la página Importar archivo de intercambio.

   c. **Vaya al archivo del flujo de trabajo archivo que desea cargar y pulse Importar.**

      Una vez importado correctamente el flujo de trabajo, aparece en el Asistente de directiva de auditoría ("Creación de directivas de auditoría" en la página 444) dentro de la lista de opciones de Flujo de trabajo de remediación.

Asignación de nombre y descripción de la directiva de auditoría

Introduzca el nombre de la nueva directiva y una breve descripción en el Asistente de directiva de auditoría (Figura 14–1).

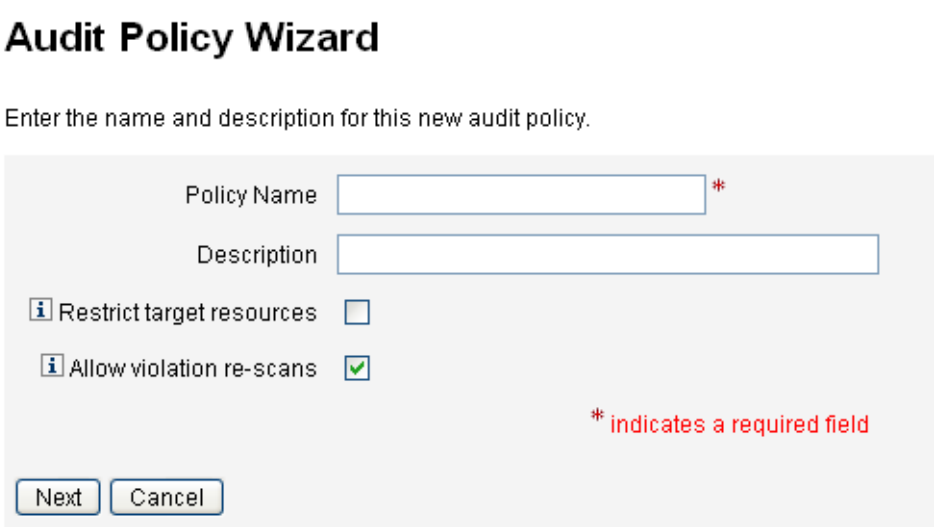


FIGURA 14–1 Asistente de directiva de auditoría: pantalla para introducir nombre y descripción

---

Nota – Los nombres de directiva de auditoría no pueden contener los siguientes caracteres: ' (apóstrofo), . (punto), | (línea), [(corchete izquierdo),] (corchete derecho), , (coma), : (dos puntos), $ (símbolo del dólar), " (comillas), \ (barra inclinada inversa) y = (signo igual).

También conviene evitar los caracteres: _ (subrayado), % (signo de porcentaje), ^ (acento circunflejo) y * (asterisco).

Si prefiere que sólo se acceda a determinados recursos al ejecutar la exploración, seleccione la opción Restringir recursos de destino.

Para que tras remediar una infracción se produzca una reexploración inmediata del usuario, elija Permitir volver a explorar infracciones.

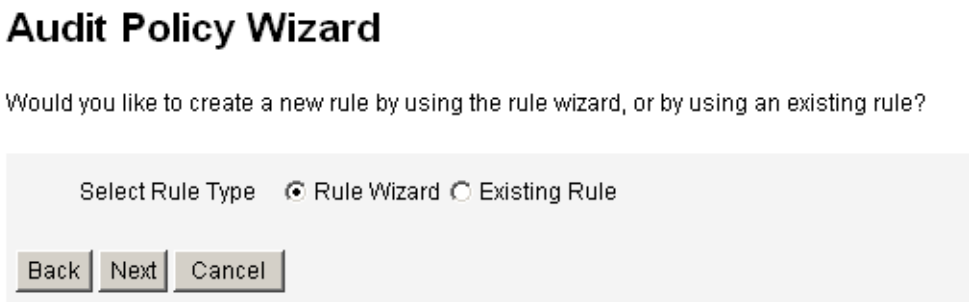
Nota – Si la directiva de auditoría no restringe los recursos, durante la exploración se accederá a todos los recursos donde tenga cuentas un usuario. Si la regla utiliza únicamente algunos recursos, resulta más eficaz restringir la directiva a dichos recursos.

Pulse Siguiente para continuar en la próxima página.

▼ Para seleccionar un tipo de regla

En esta página se inicia el proceso de definición o inclusión de reglas en la directiva. (La mayor parte del trabajo de creación de directivas consiste en definir y crear reglas.)

Como ilustra la figura siguiente, tiene la posibilidad de crear su propia regla con el Asistente para reglas de Identity Manager o de incorporar una regla existente. El Asistente para reglas sólo permite utilizar un tipo de recurso en una regla. Las reglas importadas pueden referenciar cuantos recursos sean necesarios.



1 **Decida si prefiere crear una regla nueva o usar una existente.**

Elija una de estas opciones:

- Para crear una regla nueva, elija la opción Asistente para reglas (valor predeterminado).
- Para incorporar una regla previamente creada con Identity Manager IDE, elija Regla existente.

2 **Haga clic en Siguiente.**

3 **Según lo que haya seleccionado en el paso 1, continúe en una de estas secciones:**

- Si eligió Asistente para reglas, siga las instrucciones de la sección "Para crear una regla nueva con el Asistente para reglas" en la página 449.
- Si eligió Regla existente, siga las instrucciones de la sección "Para seleccionar una regla existente" en la página 448.

Para seleccionar una regla existente

Si desea incluir una regla existente en la nueva directiva, elija Regla existente en la pantalla Seleccionar tipo de regla y pulse Siguiente. A continuación, elija una regla de directiva de auditoría existente en el menú desplegable Seleccionar regla existente.

Nota – Si no ve el nombre de una regla que ya había importado a Identity Manager, compruebe si ha añadido a la regla los atributos adicionales que se describen en "Creación de directivas con reglas de directiva de auditoría" en la página 440.

Haga clic en Siguiente.

Continúe en la sección "Incorporación de reglas" en la página 452.

Para crear una regla nueva con el Asistente para reglas

Si decide crear una regla con el Asistente para reglas en Asistente de directiva de auditoría, introduzca la información indicada en las páginas de las próximas secciones.

Nombre y descripción de la nueva regla

Existe la opción de asignar nombre y describir la nueva regla. En esta página puede introducir texto descriptivo que aparecerá junto al nombre de la regla siempre que Identity Manager la muestre. Escriba una descripción concisa y clara de la regla. Esta descripción aparece en la página Revisar infracciones de directivas de Identity Manager.

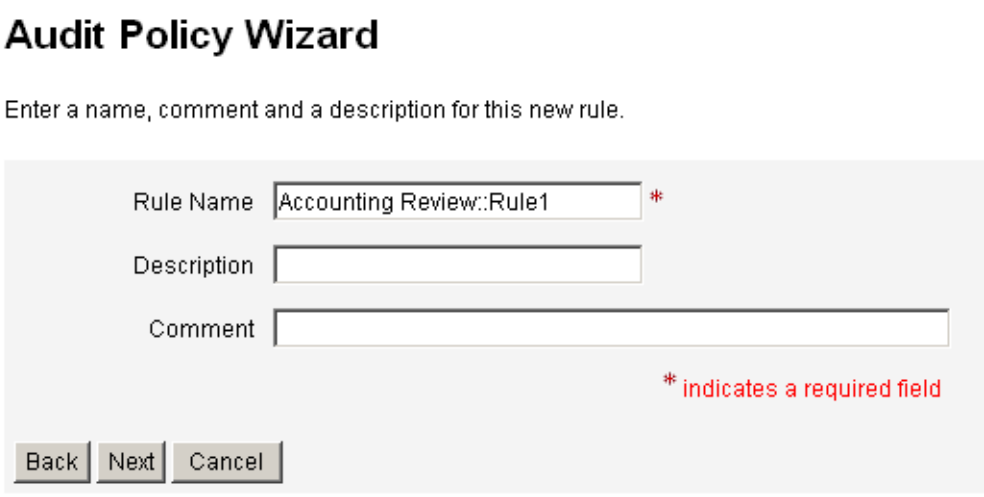


FIGURA 14–2 Asistente de directiva de auditoría: pantalla para introducir la descripción de la regla

Por ejemplo, si va a crear una regla para identificar a los usuarios que tengan simultáneamente los valores `Payable User` y `Receivable User` para el atributo responsibilityKey en Oracle ERP, podría escribir la descripción siguiente: **`Identifica los usuarios con responsabilidades simultáneas de usuarios por pagar y usuarios por cobrar`**.

En el campo Comentario puede introducir cualquier otra información sobre la regla.

Seleccione el recurso al que hará referencia esta regla

En esta página debe seleccionar el recurso al que hará referencia la regla. Cada variable de la regla debe corresponder a un atributo de este recurso. En esta lista de opciones aparecerán todos los recursos sobre los que tenga acceso de visualización. En este ejemplo está seleccionado Oracle ERP.

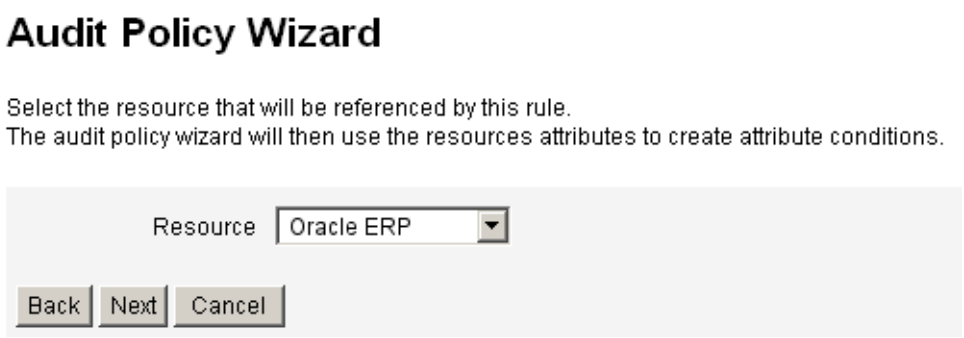


FIGURA 14–3 Asistente de directiva de auditoría: pantalla seleccionar el recurso

---

Nota – Aunque no todos, se admiten la mayoría de los atributos de cada adaptador de recursos disponible. Los atributos específicos disponibles se describen en *Sun Identity Manager 8.1 Resources Reference* .

Pulse Siguiente para continuar en la próxima página.

Crear expresión de regla

Esta pantalla sirve para introducir la expresión de la nueva regla. En este ejemplo se crea una regla que impide que un usuario tenga simultáneamente el atributo `responsibilityKey` de Oracle ERP con el valor `Payable User` y con el valor `Receivable User`.

▼ Para crear una expresión de regla

1. **Seleccione un atributo de usuario en la lista de atributos variables. Este atributo corresponderá directamente a una variable de regla.**

2. **Seleccione una condición lógica en la lista. Las condiciones válidas son "=" (igual a), "!=" (distinto a), "<" (menor que), "<=" (menor o igual que), ">" (mayor que), ">=" (mayor o igual que), "es verdadero", "es nulo", "no es nulo", "está vacío" y "contiene". En este ejemplo podría seleccionar `contiene` en la lista de posibles condiciones de atributo.**

3. **Introduzca un valor para la expresión. Por ejemplo, si introduce `Payable user`, estará especificando un usuario de Oracle ERP con el valor `Payable user` para el atributo `responsibilityKeys`.**

4. **Si lo desea, haga clic en el operador `Y` u `O` para añadir otra línea y crear otra expresión.**

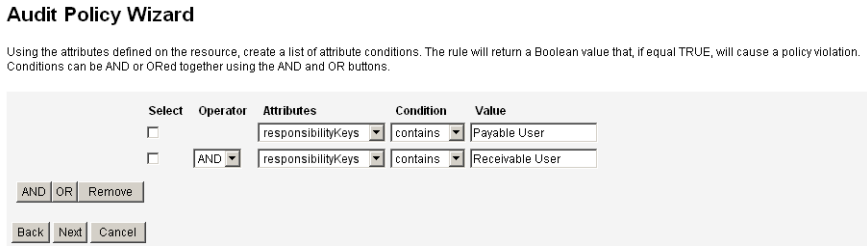


FIGURA 14–4 Asistente de directiva de auditoría: pantalla para seleccionar una expresión de regla

Esta regla devuelve un valor booleano. Si ambas instrucciones son verdaderas, la regla de directiva devuelve el valor TRUE, que ocasiona una infracción de directiva.

Nota – Identity Manager no permite controlar reglas anidadas. Además, el uso del Asistente de directiva de auditoría para crear directivas con distintos operadores booleanos entre las reglas puede tener resultados imprevisibles, porque no se especifica el orden de evaluación.

Para crear expresiones de regla complejas, utilice un editor XML en lugar del Asistente de directiva de auditoría. Con un editor XML puede negar donde sea preciso para utilizar un único operador booleano entre reglas.

El ejemplo de código siguiente ilustra en formato XML la regla creada en esta pantalla:

```
<Description>Payable User/Receivable User</Description>
  <RuleArgument name='resource' value='Oracle ERP'>
    <Comments>Resource specified when  audit policy was created.</Comments>
    <String>Oracle ERP</String>
  </RuleArgument>
    <and>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
```

```
    </and>
    <MemberObjectGroups>
      <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
    </MemberObjectGroups>
</Rule>
```

Para eliminar una expresión de la regla, seleccione la condición del atributo y pulse Suprimir.

Pulse Siguiente para continuar en el Asistente de directiva de auditoría. Tiene la oportunidad de agregar más reglas, ya sea incorporando reglas existentes o volviendo a usar el asistente.

Incorporación de reglas

Para crear más reglas, puede importar otras ya existentes o utilizar el asistente. (Para obtener más información, consulte "Para seleccionar un tipo de regla" en la página 447.)

Haga clic en los operadores `Y` u `O` para seguir añadiendo las reglas que necesite. Para eliminar una regla, selecciónela y, a continuación, pulse Suprimir.

Sólo se producirán infracciones de directivas si la expresión booleana de *todas* las reglas se evalúa como verdadera. La agrupación de reglas con operadores Y/O permite que la directiva se evalúe como verdadera, incluso aunque no ocurra lo mismo con todas las reglas. Identity Manager sólo origina infracciones con las reglas que se evalúan como verdaderas y sólo si la expresión de la directiva se evalúa como verdadera.

Nota – Identity Manager no permite controlar reglas anidadas. Además, el uso del Asistente de directiva de auditoría para crear directivas con distintos operadores booleanos entre las reglas puede tener resultados imprevisibles, porque no se especifica el orden de evaluación.

Para crear expresiones de regla complejas, utilice un editor XML en lugar del Asistente de directiva de auditoría. Con un editor XML puede negar donde sea preciso para utilizar un único operador booleano entre reglas.

Selección de un flujo de trabajo de remediación

En esta pantalla puede seleccionar un flujo de trabajo de remediación para asociarlo a esta directiva. El flujo de trabajo aquí asignado determina las acciones que se emprenden dentro de Identity Manager cuando se detecta la infracción de una directiva de auditoría.

Nota – Por cada directiva de auditoría infringida se inicia un único flujo de trabajo. Cada flujo de trabajo puede contener uno o más elementos de trabajo para cada infracción de cumplimiento detectada al explorar una directiva concreta.

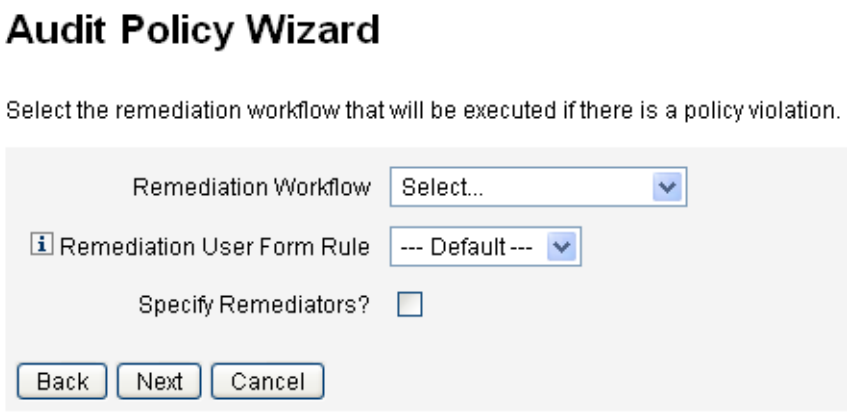


FIGURA 14–5 Asistente de directiva de auditoría: pantalla para seleccionar un flujo de trabajo de remediación

Nota – Encontrará información para importar un flujo de trabajo creado con un editor XML o Identity Manager IDE en "Importación de reglas de separación de tareas a Identity Manager (opcional)" en la página 445.

Utilice el menú desplegable Regla de formulario de usuario de remediación para seleccionar una regla para calcular el formulario de usuario que se aplica al editar un usuario mediante una remediación. Para editar un usuario en respuesta a un elemento de trabajo de remediación, un remediador utiliza de manera predeterminada el formulario de usuario que tiene asignado. Si una directiva de auditoría especifica un formulario de usuario de remediación, se utilizará dicho formulario. Ello permite emplear un formulario muy específico cuando una directiva de auditoría señala el correspondiente problema específico.

Para elegir los remediadores asociados a este flujo de trabajo de remediación, marque la casilla ¿Especificar remediadores? casilla de verificación Si elige esta opción, al pulsar Siguiente aparecerá la página "Asignar Remediadores". De lo contrario, accederá a la pantalla de asignación de organizaciones del Asistente de directiva de auditoría.

Selección de remediadores y tiempos de espera de remediaciones

Si elige remediadores, se notificará a los asignados a esta directiva de auditoría cuando se detecte una infracción de la directiva. Además, el flujo de trabajo predeterminado les asigna un elemento de trabajo de remediación. Cualquier usuario de Identity Manager puede actuar como remediador.

Tiene la opción de asignar al menos un remediador de nivel 1 o usuario designado. Los remediadores de nivel 1 son los primeros a quienes el flujo de trabajo de remediación notifica por correo electrónico cuando se detecta una infracción de directiva. Si transcurre el tiempo de espera de escalada especificado antes de que responda un remediador de nivel 1, Identity Manager se pone en contacto con los remediadores de nivel 2 que usted elija aquí. Identity Manager sólo contacta con los remediadores de nivel 3 si no hay respuesta de ningún remediador de los niveles 1 y 2 antes de que transcurra el periodo de escalada.

Nota – Si especifica un valor de tiempo de espera de escalada para el remediador de máximo nivel seleccionado, el elemento de trabajo desaparecerá de la lista cuando se agote dicho tiempo de espera. El valor predeterminado del tiempo de espera de escalada es 0. Ello significa que el elemento de trabajo no caduca y permanece en la lista del remediador.

Asignar remediadores es opcional. Si selecciona esta opción, pulse Siguiente para pasar a la próxima pantalla tras especificar los valores de configuración.

Si desea agregar usuarios a la lista de remediadores disponibles, introduzca un ID de usuario y después pulse Agregar. Como alternativa, haga clic en **...** (Más) para buscar un ID de usuario. Introduzca uno o varios caracteres en el campo Empieza por y, a continuación, haga clic en Buscar. Tras seleccionar un usuario en la lista de búsqueda, pulse Agregar para incluirlo en la lista de remediadores. Haga clic en Descartar para cerrar el área de búsqueda.

Para eliminar un ID de usuario de la lista de remediadores, selecciónelo y pulse Suprimir.

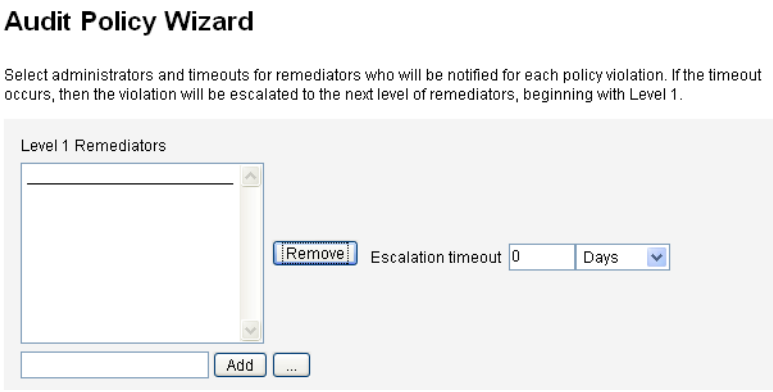


FIGURA 14–6 Asistente de directiva de auditoría: área para seleccionar remediadores de nivel 1

Selección de las organizaciones que pueden acceder a esta directiva

La pantalla ilustrada en la Figura 14–7 sirve para elegir las organizaciones que pueden ver y editar esta directiva.

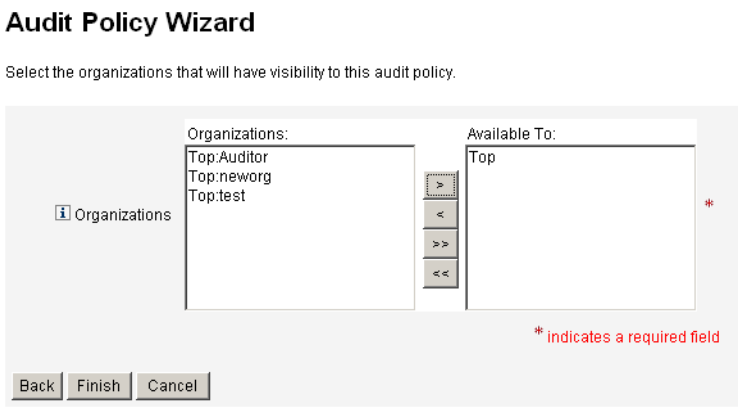


FIGURA 14–7 Asistente de directiva de auditoría: pantalla para asignar visibilidad a las organizaciones

Después de seleccionar las organizaciones, pulse Finalizar para crear la directiva de auditoría y volver a la página Administrar directivas. La directiva recién creada ahora aparece en la lista.

Edición de directivas de auditoría

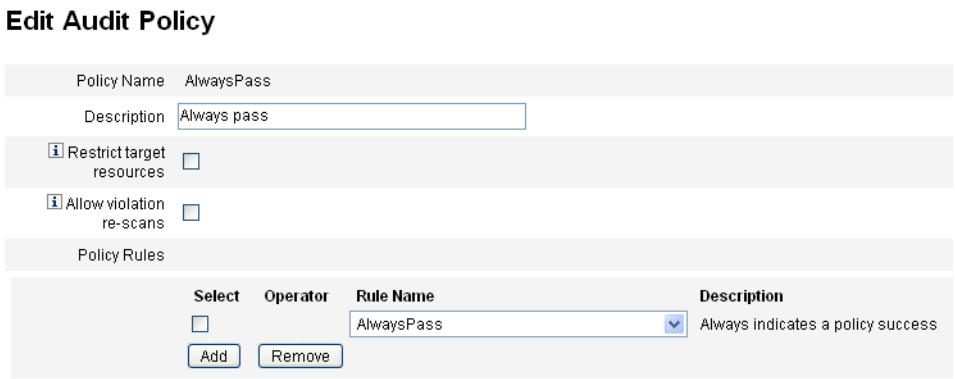
Las tareas habituales al editar directivas de auditoría incluyen:

- Agregar o eliminar reglas.
- Cambiar los recursos de destino.
- Ajustar la lista de organizaciones que tienen acceso a la directiva.
- Modificar el tiempo de espera de escalada asociado a cada nivel de remediación.
- Cambiar el flujo de trabajo de remediación asociado a la directiva.

Página Editar directiva

Seleccione un nombre de directiva en la columna de nombres de directiva auditoría para abrir la página Editar directiva de auditoría. Esta página estructura la información de las directivas de auditoría en varias áreas:

- Identificación y reglas
- Remediadores y Tiempo de espera de escalada
- Flujo de trabajo y Organizaciones



Este área de la página sirve para:

- Editar la descripción de la directiva.
- Agregar o eliminar una regla.

Nota – Con este producto no es posible editar directamente una regla existente. Hay que editarla con Identity Manager IDE o un editor XML y después importarla a Identity Manager. Después puede suprimir la versión anterior y agregar la recién revisada.

Edición de la descripción de una directiva de auditoría

Para editar la descripción de la directiva de auditoría, seleccione el texto en el campo Descripción y escriba el texto nuevo.

Opciones de edición

Si lo desea, marque las casillas Restringir recursos de destino o Permitir volver a explorar infracciones.

Eliminación de una regla de la directiva

Para eliminar una regla de la directiva, haga clic en el botón Seleccionar que precede al nombre de la regla y después pulse Suprimir.

Inclusión de una regla en la directiva

Pulse Agregar para añadir un campo nuevo donde puede elegir una regla para incluirla.

Modificación de una regla utilizada en la directiva

En la columna Nombre de regla, elija otra regla de la lista de selección.

Área Remediadores

La Figura 14–8 ilustra parte del área Remediadores, donde se asignan remediadores de los niveles 1, 2 y 3 a una directiva.

FIGURA 14–8 Página Editar directiva de auditoría: asignación de remediadores

Este área de la página sirve para:

- Suprimir o asignar remediadores a una directiva.
- Ajustar los tiempos de espera de escalada.

Supresión o asignación de remediadores

Para seleccionar un remediador de uno o varios niveles, introduzca un ID de usuario y pulse Agregar. Para buscar un ID de usuario, pulse **...** (Más). Debe especificar al menos un remediador.

Para eliminar un remediador, elija un ID de usuario en la lista y pulse Suprimir.

Ajuste de los tiempos de espera de escalada

Seleccione el valor de tiempo de espera y escriba el nuevo valor. No hay ningún valor de tiempo de espera definido de manera predeterminada.

Nota – Si especifica un valor de tiempo de espera de escalada para el remediador de máximo nivel seleccionado, el elemento de trabajo desaparecerá de la lista cuando se agote dicho tiempo de espera.

Área de Flujo de trabajo y Organizaciones

La Figura 14–9 muestra el área donde se especifica el flujo de trabajo de remediación y las organizaciones para una directiva de auditoría.

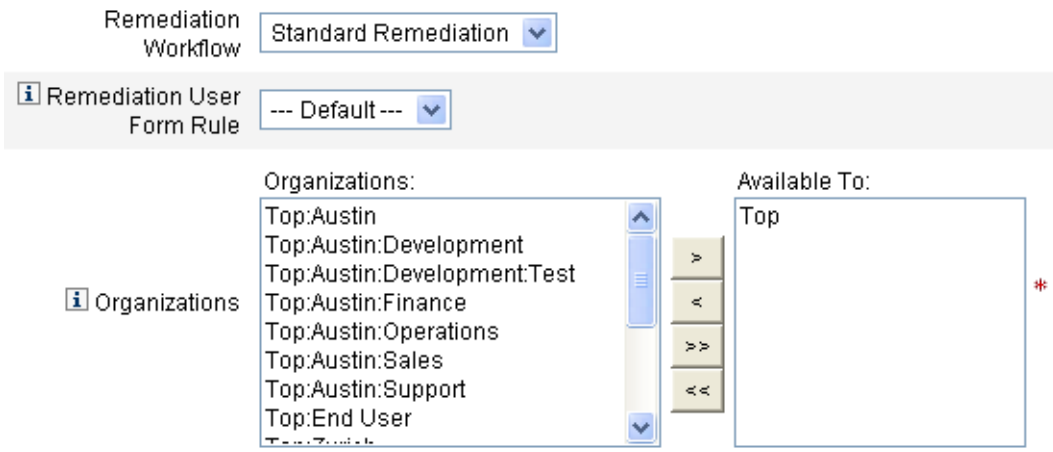


FIGURA 14–9 Página Editar directiva de auditoría: flujo de trabajo de remediación y organizaciones

Este área de la página sirve para:

- Cambiar el flujo de trabajo de remediación que se inicia cuando se comete una infracción de directiva.
- Seleccionar una regla de formulario de usuario de remediación.
- Ajustar las organizaciones que tienen acceso a la directiva.

Cambio del flujo de trabajo de remediación

Para cambiar el flujo de trabajo asignado a una directiva, puede seleccionar otro flujo en la lista de opciones. No se asigna ningún flujo de trabajo de manera predeterminada a una directiva de auditoría.

Nota – Si no hay asignado ningún flujo de trabajo a la directiva de auditoría, las infracciones no se asignarán a ningún remediador.

Seleccione un flujo de trabajo de remediación en la lista y pulse Guardar.

Selección de una regla de formulario de usuario de remediación

Si lo desea, puede elegir una regla para calcular el formulario de usuario que se aplica al editar un usuario mediante una remediación.

Asignación o supresión de visibilidad a las organizaciones

Ajuste las organizaciones para las que estará disponible esta directiva de auditoría y pulse Guardar.

Directivas de ejemplo

Identity Manager proporciona acceso a las siguientes directivas de ejemplo en la lista Directivas de auditoría:

- IDM Role Comparison Policy
- IDM Account Accumulation Policy

IDM Role Comparison Policy

Esta directiva sirve para comparar el acceso actual de un usuario con el acceso especificado por los roles de Identity Manager. La directiva garantiza que todos los atributos de recurso especificados por los roles están configurados para el usuario.

Esta directiva falla si:

- El usuario carece de algún atributo de recurso especificado por roles.
- Los atributos de recurso del usuario difieren de los especificados por los roles.

IDM Account Accumulation Policy

Esta directiva verifica si todas las cuentas de recursos que mantiene el usuario están referenciadas por al menos un rol mantenido por el usuario.

Esta directiva falla si el usuario tiene cuentas en algún recurso no referenciado explícitamente por un rol asignado al usuario.

Eliminación de directivas de auditoría

Cuando se elimina una directiva de auditoría de Identity Manager, también desaparecen todas las infracciones que la referencian.

Las directivas pueden eliminarse desde el área Cumplimiento de la interfaz cuando se pulsa Administrar directivas para ver las directivas. Para eliminar una directiva de auditoría, seleccione su nombre en la vista de directivas y pulse Eliminar.

Solución de problemas de directivas de auditoría

La mejor forma de solucionar los problemas con las directivas de auditoría es depurar sus reglas.

Para depurar una regla, incluya los siguientes elementos de rastreo en el código de la regla.

```
<block trace='true'>
<and>
    <contains>
```

```
        <ref>accounts[AD].firstname</ref>
        <s>Sam</s>
    </contains>
    <contains>
        <ref>accounts[AD].lastname</ref>
        <s>Smith</s>
    </contains>
</and>
</block>
```

- Si no ve el flujo de trabajo en la interfaz de Identity Manager, compruebe lo siguiente:
  - Ha agregado el atributo `subtype='SUBTYPE_REMEDIATION_WORKFLOW '` al flujo de trabajo. Los flujos de trabajo que carecen de este subtipo no se ven en la interfaz de administración de Identity Manager.
  - Tiene capacidad para el tipo de autorización (authType) `AuditorAdminTask`.
  - Tiene control sobre la organización que contiene el flujo de trabajo.
- Si ha importado las reglas, pero no las ve en el Asistente de directiva de auditoría, compruebe lo siguiente:
  - Cada regla tiene el subtipo `subtype="SUBTYPE_AUDIT_POLICY_RULE'` o `subtype="SUBTYPE_AUDIT_POLICY_SOD_RULE'`.
  - Tiene capacidad para el tipo de autorización (authType) `AuditPolicyRule`.
  - Tiene control sobre la organización que contiene el flujo de trabajo.

Asignación de directivas de auditoría

Para asignar una directiva de auditoría a una organización, el usuario debe tener como mínimo la capacidad Asignar de directivas de auditoría de organización. Para asignar una directiva de auditoría a un usuario, el usuario debe tener la capacidad Asignar de directivas de auditoría de usuario. Un usuario posee ambas capacidades si tiene la capacidad Asignar directivas de auditoría.

Para asignar una directiva de nivel de organización, seleccione la organización en la ficha Cuentas y después las directivas en la lista Directivas de auditoría asignadas.

▼ Para asignar una directiva de nivel de usuario

1. **Elija el usuario en el área Cuentas.**
2. **Seleccione Cumplimiento en el formulario de usuario.**
3. **Seleccione las directivas en la lista Directivas de auditoría asignadas.**

Nota – Las directivas de auditoría que se asignan directamente a un usuario (mediante una cuenta de usuario o asignación de organización) siempre vuelven a evaluarse cuando se remedia una infracción de dicho usuario.

Solución de limitaciones de capacidades de auditoría

De manera predeterminada, las capacidades necesarias para realizar tareas de auditoría están incluidas en la organización superior (grupo de objetos). En consecuencia, sólo los administradores que controlan la organización superior pueden asignar dichas capacidades a otros administradores.

Para solucionar esta limitación, puede agregar las capacidades a otra organización. Con el fin de facilitar esta tarea, Identity Manager ofrece dos utilidades en el directorio `sample/scripts` .

▼ Para agregar capacidades

Siga estos pasos para agregar las capacidades que permiten efectuar tareas de auditoría a organizaciones distintas de la superior:

1. **Ejecute el comando siguiente para ver todas las capacidades (grupos de administradores) y las organizaciones asociadas a ellas (grupos de objetos):**

   ```
   beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
   ```

   Este comando captura la salida a un archivo de valores separados por comas (CSV).

2. **Edite el archivo CSV para ajustar las ubicaciones organizativas de las capacidades como convenga.**

3. **Ejecute este comando para actualizar Identity Manager:**

   ```
   beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
   ```

◆ ◆ ◆ CAPÍTULO 15

Auditoría: Cumplimiento de supervisión

En este capítulo se describe la forma de realizar revisiones de auditoría e implementar prácticas que ayudan a controlar la conformidad con las normas exigidas por las autoridades federales.

En este capítulo examinaremos los conceptos y las tareas siguientes:

Exploraciones de directivas de auditorías e informes

Además de incluir información sobre la exploración de directivas de auditoría, en esta sección se describen los procedimientos para ejecutar y administrar las exploraciones de auditoría.

Exploración de usuarios y organizaciones

Las exploraciones ejecutan las directivas de auditoría seleccionadas en usuarios u organizaciones particulares. Puede explorar un usuario o una organización para detectar una infracción determinada o ejecutar directivas no asignadas al usuario o la organización. Las exploraciones se inician desde la sección Cuentas de la interfaz.

Nota – También puede iniciar o programar la exploración de directivas de auditoría desde la ficha Tareas del servidor.

▼ Para explorar una cuenta de usuario o una organización

1 **En la interfaz de administración, seleccione la opción Cuentas del menú principal.**

2 **En la lista Cuentas, lleve a cabo una de las acciones siguientes:**

a. **Seleccione uno o varios usuarios y elija Explorar en la lista de opciones Acciones de Usuario.**

b. **Seleccione una o varias organizaciones y elija Explorar en la lista de opciones Acciones de Organización.**

Aparece el cuadro de diálogo Iniciar tarea. En la Figura 15–1 se muestra un ejemplo de la página Iniciar tarea de una exploración de usuario de directivas de auditoría.

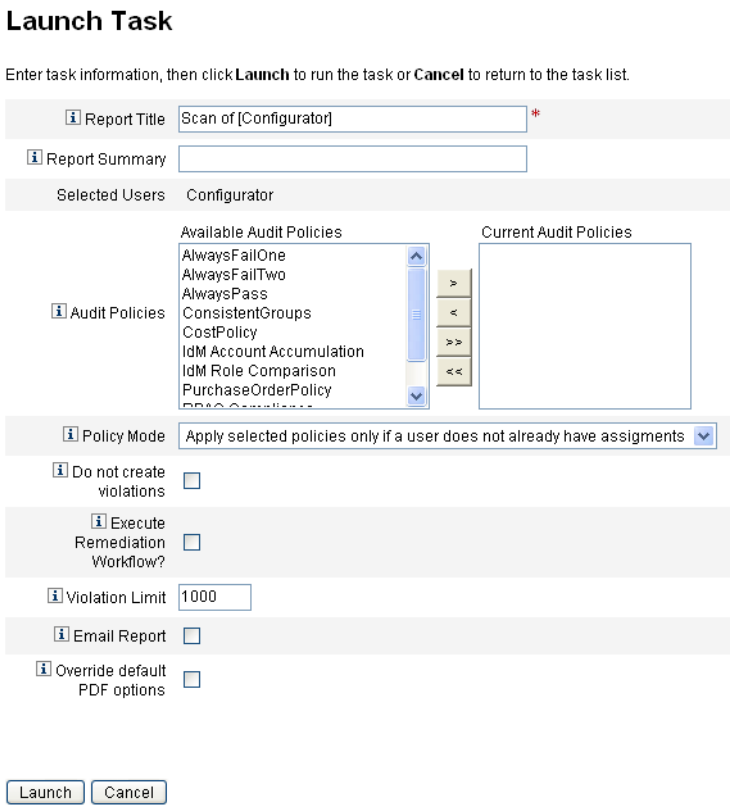


FIGURA 15–1 Cuadro de diálogo Iniciar tarea

3 **Introduzca el nombre de la exploración en el campo Título del informe.** (*imprescindible*)

4 **Especifique las demás opciones.**

Las opciones incluyen:

- **Resumen del informe**: introduzca la descripción de la exploración.
- **Añadir directivas**: seleccione una o varias directivas de auditoría para ejecutarlas. Es necesario que especifique al menos una directiva.
- **Modo de directiva**: seleccione un modo de directiva para determinar la manera en que las directivas seleccionadas interaccionan con usuarios que disponen de asignaciones de directivas. Las asignaciones pueden proceder directamente del usuario o de la organización a la que esté asignado el usuario.
- **No crear infracciones**: active este cuadro si quiere que se evalúen las directivas de auditoría y se informe de las infracciones, pero no desea que se creen ni actualicen las infracciones del cumplimiento y tampoco que se ejecuten los flujos de trabajo de remediación. Esta opción resulta útil para probar directivas de auditoría porque las infracciones generadas aparecen en los resultados de la tarea de exploración.
- **¿Ejecutar flujo de trabajo de remediación?**: active este cuadro para ejecutar el flujo de trabajo de remediación asignado en la directiva de auditoría. Si la directiva de auditoría no define un flujo de trabajo de remediación, no se ejecutará ninguno.
- **Límite de infracción**: edite este cuadro para definir el número máximo de infracciones del cumplimiento que puede emitir esta exploración antes de que se anule. Este valor es una medida de seguridad para limitar el riesgo cuando se ejecute una directiva de auditoría que pueda ser demasiado agresiva en sus comprobaciones. Un valor vací-o indica que no se establece ningún límite.
- }**Informe de correo electrónico**: active este cuadro para especificar los destinatarios del informe. Si también tiene Identity Manager, adjunte un archivo que contenga un informe en formato CSV (valores separados por coma).
- **Ignorar opciones predeterminadas de PDF**: active este cuadro para que se ignoren las opciones predeterminadas de PDF.

5 **Haga clic en Iniciar para comenzar la exploración.**

Para ver los informes que genera la exploración de auditoría, abra Informes de Auditor.

Operaciones con Informes de Auditor

Identity Manager proporciona una serie de informes de auditor. Estos informes se describen en la tabla siguiente.

TABLA 15–1 Descripción de informes de auditor

Tipo de informe de auditor	Descripción
Cobertura de revisión de acceso	Muestra la coincidencia parcial o las diferencias que existen entre los usuarios implicados en las revisiones de acceso seleccionadas. Como la mayoría de revisiones de acceso tienen un ámbito de usuario especificado por una consulta o por cualquier operación de pertenencia, el conjunto exacto de usuarios cambia con el tiempo. Este informe puede mostrar las coincidencias parciales, las diferencias, o ambas, que existen entre los usuarios especificados por dos revisiones de acceso distintas (para comprobar la eficacia de las revisiones en funcionamiento), entre los derechos que generan dos revisiones de acceso diferentes (para comprobar si la cobertura cambia con el tiempo) o entre los usuarios y los derechos (para que pueda determinar si se han generado derechos para todos los usuarios incluidos en el ámbito de la revisión).
Detalle de revisión de acceso	Muestra el estado actual de todos los registros de derechos de usuario. Este informe se puede filtrar por organización de usuario, revisión de acceso, instancia de revisión de acceso, estado de un registro de derechos y autenticador.
Resumen de revisión de acceso	Ofrece información resumida sobre todas las revisiones de acceso. Incluye un resumen de los usuarios explorados, las directivas exploradas y las actividades de autenticación de cada exploración de revisión de acceso de la lista.
Cobertura de ámbito de usuario de exploración de acceso	Compara las exploraciones seleccionadas para determinar qué usuarios están incluidos en el ámbito de exploración. Muestra la superposición (usuarios incluidos en todas las exploraciones) o la diferencia (usuarios no incluidos en todas las exploraciones, pero sí en más de una). Este informe resulta útil cuando se intentan organizar múltiples exploraciones de acceso para cubrir los mismos o distintos usuarios, según las necesidades de exploración.
Resumen de directivas de auditoría	Ofrece un resumen de los elementos fundamentales de todas las directivas de auditoría, lo que incluye las reglas, los remediadores y el flujo de trabajo de cada directiva.
Atributo auditado	Muestra todos los registros de auditoría que reflejan un cambio en un atributo de cuenta de recurso específico. Este informe extrae datos de auditorí-a para atributos auditables que se han almacenado. Los datos se extraen en función de cualquier atributo ampliado, que puede especificarse en WorkflowServices o en atributos de recurso marcados como auditables. Para obtener información sobre la configuración de este informe, consulte "Configuración del informe de atributos auditados" en la página 469.

TABLA 15–1 Descripción de informes de auditor *(Continuación)*

Tipo de informe de auditor	Descripción
Historial de infracciones de directivas de auditoría	Es una vista gráfica en la que aparecen todas las infracciones del cumplimiento por directiva que se han creado durante un periodo de tiempo concreto. Este informe se puede filtrar por directiva y agrupar por día, semana, mes o trimestre.
Acceso de usuario	Muestra el registro de auditoría y los atributos de usuario de un usuario determinado.
Historial de infracciones de la organización	Es una vista gráfica en la que aparecen todas las infracciones del cumplimiento por recurso que se han creado durante un periodo de tiempo concreto. Se puede filtrar por organización y agrupar por día, semana, mes o trimestre.
Historial de infracciones del recurso	Es una vista gráfica en la que aparecen todas las infracciones del cumplimiento por recurso que se han creado durante un periodo de tiempo concreto.
Separación de tareas	Muestra la separación de las infracciones de tareas en una tabla de conflictos. Mediante los vínculos de la interfaz web puede acceder a información adicional. Este informe se puede filtrar por organización y agrupar por día, semana, mes o trimestre.
Resumen de infracciones	Muestra todas las infracciones de cumplimiento actuales. Este informe se puede filtrar por remediador, recurso, regla, usuario o directiva.

Estos informes se encuentran disponibles en la ficha Informes de la interfaz de Identity Manager.

Nota – El valor de `RULE_EVAL_COUNT` equivale al número de reglas que se han evaluado durante una exploración de directiva. A veces se incluye en los informes.

Identity Manager calcula el valor de `RULE_EVAL_COUNT` de la siguiente manera.

```
nº de usuarios explorados x (nº de reglas de la directiva + 1)
```

+1 se incluye en el cálculo porque Identity Manager también tiene en cuenta la *regla de directiva*, ya que es la regla que permite determinar realmente si se infringe una directiva. La regla de directiva examina los resultados de la regla de auditoría y utiliza la lógica booleana para generar el resultado de la directiva.

Por ejemplo, si tiene una directiva A con tres reglas y una directiva B con dos reglas, y ha realizado exploraciones en diez usuarios, el valor de `RULE_EVAL_COUNT` será 70 porque

```
10 usuarios x (3 + 1 + 2 + 1 reglas).
```

Creación de un informe de auditor

Para ejecutar un informe, primero tiene que crear la plantilla del mismo. Puede especificar varios criterios, incluso los destinatarios de correo electrónico que recibirán los resultados del informe. La plantilla del informe creada y guardada se encuentra disponible en la página Ejecutar informes.

En la figura siguiente se muestra un ejemplo de la página Ejecutar informes, en la que aparece la lista de informes de auditor definidos.

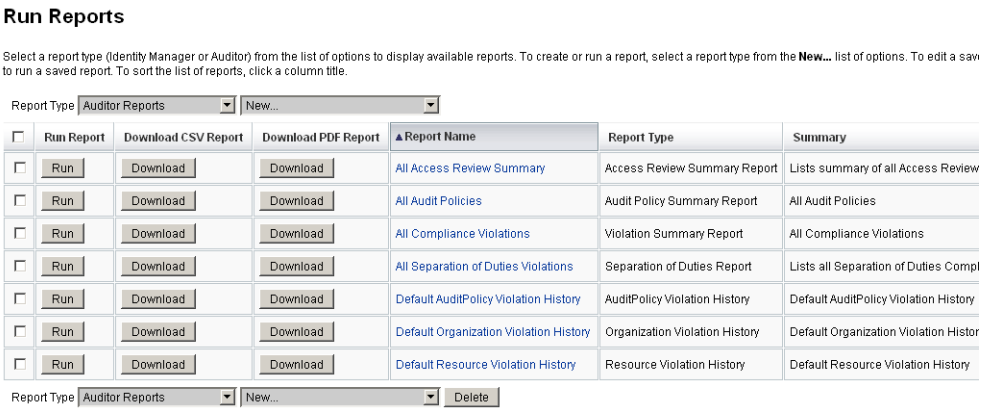


FIGURA 15–2 Opciones de la página Ejecutar informes

▼ Para crear un informe de auditor

1 **En la interfaz de administración, seleccione Informes en el menú principal.**

Aparece la página Ejecutar informes.

2 **Seleccione Informes de Auditor como tipo de informe.**

3 **En la nueva lista de informes, seleccione un informe.**

Aparece la página Definir un informe. Los campos y la distribución del cuadro de diálogo de informes varía según el tipo de informe. Consulte la Ayuda de Identity Manager para obtener información sobre la definición de los criterios del informe.

Después de escribir y seleccionar el criterio de informe podrá:

- Ejecutar el informe sin guardarlo.

  Haga clic en Ejecutar para empezar a ejecutar el informe. Identity Manager no guarda el informe (si ha definido un nuevo informe) ni los criterios de informe modificados (si ha editado un informe existente).

- Guardar el informe.

  Haga clic en Guardar para guardar el informe. Después de guardar el informe, puede ejecutarlo desde la página Ejecutar informes (lista de informes). Una vez que ejecuta el informe en la página Ejecutar informes, puede ver el resultado de inmediato o posteriormente en la ficha Ver informes.

Para obtener información sobre la programación de un informe, consulte "Programación de informes" en la página 278.

Configuración del informe de atributos auditados

En el informe de atributos auditados (consulte la Tabla 15–1) pueden aparecer los cambos de nivel de atributo experimentados por los usuarios y las cuentas de Identity Manager. Sin embargo, el registro de auditoría estándar no genera suficientes datos de auditoría como para admitir una expresión de consulta completa.

El registro de auditoría estándar introduce *realmente* los atributos modificados en el campo `acctAttrChanges` del registro de auditoría, pero de manera que al consultar el informe sólo se encuentran los registros basados en el nombre del atributo cambiado. En la consulta del informe no se encuentra exactamente el valor del atributo.

Es posible configurar este informe para encontrar los registros que contienen modificaciones del atributo `lastname` especificando los parámetros siguientes:

```
Attribute Name = 'acctAttrChanges'
Condition = 'contains'
Value = 'lastname'
```

Nota – Por la forma en que se almacenan los datos en el campo `acctAttrChanges`, es necesario utilizar `Condition='contains'`. Este campo no admite varios valores. Básicamente, se trata de una estructura de datos que contiene los valores `before/after` de todos los atributos modificados con la sintaxis `attrname=value`. Por consiguiente, los valores anteriores permiten encontrar cualquier instancia de `lastname=` *xxx* en la consulta del informe.

También es posible encontrar los registros de auditoría que tienen un atributo específico con valor determinado solamente. Para esto, realice el procedimiento que se describe en la sección "Configuración de la ficha Auditoría" en la página 329. Seleccione la casilla Auditar todo el flujo de trabajo, haga clic en el botón Añadir atributo para elegir los atributos que deben quedar registrados para el informe y haga clic en Guardar.

A continuación, active la configuración de la plantilla de tareas (si no está activada). Para esto, realice el procedimiento que se describe en la sección "Habilitación de las plantillas de tarea" en la página 301. Haga clic en Guardar sin cambiar el valor predeterminado de la lista Tipos de procesos seleccionados.

El flujo de trabajo ahora puede suministrar los registros de auditoría que corresponden tanto al nombre de atributo como al valor. Aunque con este nivel de auditoría se obtiene mucha información, hay que tener en cuenta que se produce una notable pérdida de rendimiento y que los flujos de trabajo se ralentizan drásticamente.

Remediación y mitigación de infracciones del cumplimiento

En esta sección se describe la forma de utilizar la remediación de Identity Manager para proteger los activos críticos.

En los temas siguientes se explican los elementos del proceso de remediación de Identity Manager:

Acerca de la remediación

Cuando Identity Manager detecta un infracción del cumplimiento de directivas de auditoría sin resolver (mitigar), crea una solicitud de remediación que debe enviar un *remediador*. El remediador es el usuario designado que puede evaluar y responder a las infracciones de directivas de auditoría.

Escalación del remediador

Identity Manager permite definir tres niveles de escalación. Las solicitudes de remediación se envían inicialmente a los remediadores de nivel 1. Si el remediador de nivel 1 no responde a la solicitud de remediación antes de que expire el tiempo establecido, Identity Manager remite la infracción a los remediadores de nivel 2 y comienza un intervalo de espera nuevo. Si el remediador de nivel 2 tampoco responde antes del tiempo establecido, se pasa la solicitud al remediador de nivel 3.

Para llevar a cabo la remediación, debe designar al menos un designador dentro de la organización. Aunque se recomienda designar más de un remediador en cada nivel, es opcional. La existencia de varios remediadores evita que el flujo de trabajo se retrase o interrumpa.

Acceso seguro a la remediación

Las opciones de autorización están relacionadas con elementos de trabajo del tipo de autenticación (authType) `RemediationWorkItem`.

- Propietario del elemento de trabajo de remediación
- Administrador directo o indirecto del propietario del elemento de trabajo de remediación
- Administrador que controla la organización a la que pertenece el propietario del elemento de trabajo de remediación

De forma predeterminada, el comportamiento de las comprobaciones de autorización es uno de los siguientes:

- El propietario es el usuario que intenta realizar la acción.
- El propietario es una organización que controla el usuario que intenta realizar la acción.
- El propietario es un subordinado del usuario que intenta realizar la acción.

Las comprobaciones segunda y tercera se pueden configurar por separado cambiando estas opciones:

- **controlOrg**. Los valores válidos son true o false.
- **subordinate**. Los valores válidos son true o false.
- **lastLevel**. Último nivel de subordinación que se incluye en el resultado; -1 corresponde a todos los niveles. El valor entero de lastLevel es -1 de forma predeterminada, y hace referencia a los subordinados directos e indirectos.

Estas opciones se pueden agregar o modificar en:

`Formulario de usuario: Lista de remediación`

Proceso del flujo de trabajo de remediación

Identity Manager proporciona el flujo de trabajo de remediación estándar a fin de garantizar procesos de remediación para todas las exploraciones de directivas de auditoría.

El flujo de trabajo de remediación estándar genera una solicitud de remediación (elemento de trabajo de tipo revisión), que contiene información sobre la infracción del cumplimiento, y envía una notificación por correo electrónico a los remediadores de nivel 1 mencionados en la directiva de auditoría. Cuando un remediador mitiga la infracción, el flujo de trabajo cambia el estado del objeto de infracción del cumplimiento existente y el asigna una caducidad.

La infracción del cumplimiento solamente se puede identificar mediante la combinación del usuario, el nombre de la directiva y el nombre de la regla. Cuando el resultado de evaluar la directiva de auditoría es true, se crea una infracción del cumplimiento nueva por cada combinación de usuario/directiva/regla, si no existe una infracción para esta combinación. Si no existe una infracción para esa combinación y la infracción se encuentra en estado mitigado, el proceso del flujo de trabajo no se realiza. Si la infracción no está mitigada, su recuento de recurrencia aumenta.

Para obtener más información sobre los flujos de trabajo de remediación, consulte "Qué son las directivas de auditoría" en la página 440.

Respuestas de remediación

Cada remediador tiene tres opciones de forma predeterminada:

- **Remediar**. El remediador indica que se ha realizado alguna acción para solucionar el problema en el recurso.

  Cuando se modifica una infracción del cumplimiento, Identity Manager crea un evento de auditoría para registrar la remediación. Además, Identity Manager almacena el nombre del remediador y los comentarios introducidos.

  Nota – Después de la remediación, la infracción no se elimina hasta la siguiente exploración de auditoría. Si la directiva de auditoría se configura para permitir reexploraciones, el usuario se volverá a explorar en cuanto se remedie la infracción.

- **Mitigar**. El remediador permite la infracción y exime al usuario de la infracción durante un periodo de tiempo determinado.

Si la infracción se comete de forma deliberada (por ejemplo, hay un caso de pertenencia a dos grupos), puede mitigar la infracción durante un periodo de tiempo mayor. También puede mitigar la infracción durante un breve periodo de tiempo (por ejemplo, si el administrador del sistema del recurso está de vacaciones y no sabe cómo solucionar el problema).

Identity Manager almacena el nombre del remediador que mitiga la infracción, junto con la fecha de caducidad asignada a la exención y los comentarios introducidos.

Nota – Cuando Identity Manager detecta una exención caducada, cambia el estado de la infracción de mitigado a pendiente.

- **Reenviar**. El remediador reasigna a otra persona la responsabilidad de solucionar la infracción.

Ejemplo de remediación

La organización establece una regla según la cual un usuario no puede ser responsable de las cuentas por pagar y por cobrar, y se le informa de que un usuario está infringiendo esta regla.

- Si el usuario es un supervisor, responsable de ambas funciones hasta que la organización contrate a otra persona para desempeñar ese cargo, podrá mitigar la infracción y generar una exención durante un máximo de seis meses.
- Si el usuario está infringiendo la regla, puede solicitar al administrador de Oracle ERP que solucione el conflicto y luego remediar la infracción una vez que se haya resuelto el problema de ese recurso. También puede reenviar la solicitud de remediación al administrador de Oracle ERP.

Plantilla de remediación para correo electrónico

Identity Manager proporciona una plantilla de notificación por correo electrónico de infracciones de directiva (disponible mediante la selección de la ficha Configuración y, a continuación, Plantillas de correo electrónico). Puede configurar esta plantilla para notificar a los remediadores las infracciones pendientes. Para obtener más información, consulte "Personalización de plantillas de correo electrónico" en la página 106 en el Capítulo 4, "Configuración de objetos de administración de negocio".

Operaciones en la página Remediaciones

Seleccione Elementos de trabajo → Remediaciones para acceder a la página Remediaciones.

Puede utilizar esta página para:

- Ver infracciones pendientes.
- Priorizar las infracciones de directiva.
- Mitigar una o varias infracciones de directiva.
- Remediar una o varias infracciones de directiva.
- Reenviar una o varias infracciones de directiva.
- Editar usuarios desde un elemento de trabajo de remediación.

Visualización de infracciones de directiva

En la página Remediaciones puede consultar los detalles de las infracciones antes de realizar cualquier acción.

Dependiendo de sus capacidades o del lugar que ocupe en la jerarquía de capacidades de Identity Manager, podrá ver y realizar acciones en las infracciones asignadas a otros remediadores.

Los temas siguientes están relacionados con la visualización de infracciones:

- "Visualización de solicitudes pendientes" en la página 474
- "Visualización de solicitudes completadas" en la página 475
- "Actualización de la tabla" en la página 476

Visualización de solicitudes pendientes

Las solicitudes pendientes que se le asignan aparecen en la tabla Remediaciones de forma predeterminada.

Si quiere ver las solicitudes de remediación pendientes de otro remediador, puede utilizar la opción Lista de remediaciones para.

- Seleccione Mis informes directos para ver las solicitudes pendientes de usuarios de la organización que le informan directamente.
- Seleccione Buscar usuarios para introducir o localizar uno o varios usuarios, cuyas solicitudes pendientes desea ver. Introduzca un ID de usuario y haga clic en Aplicar para ver las solicitudes pendientes de ese usuario. También puede hacer clic en **...** (Más) para buscar un usuario. Después de localizar y seleccionar un usuario, haga clic en Descartar para cerrar la sección de búsqueda.

En la tabla resultante se proporciona la siguiente información sobre cada solicitud:

- **Remediador**. Nombre del remediador asignado. Esta columna sólo aparece cuando se visualizan las solicitudes de remediación de otros remediadores.
- **Usuario**. Usuario objeto de la solicitud.
- **Directiva/Solicitud de auditorí-a**. Acción solicitada al remediador.
- **Regla/Descripción de auditorí-a**. Comentarios de remediación relacionados con la solicitud.
- **Estado de infracción**. Estado actual de la infracción.
- **Gravedad**. Gravedad asignada a la solicitud (ninguna, baja, media, alta o crítica).
- **Prioridad**. Prioridad asignada a la solicitud (ninguna, baja, media, alta o urgente).
- **Fecha de la solicitud**: fecha y hora en que se envió la solicitud de remediación.

Nota – Cada usuario puede elegir un formulario personalizado para presentar los datos de remediación relacionados con ese remediador concreto. Para asignar un formulario personalizado, seleccione la ficha Cumplimiento en el formulario de usuario.

Visualización de solicitudes completadas

Para ver las solicitudes de remediación completadas, haga clic en la ficha Mis elementos de trabajo y luego en la ficha Historial. Se muestra la lista de elementos de trabajo remediados previamente.

En la tabla resultante (que genera un informe `AuditLog`) se proporciona la siguiente información sobre cada una de las solicitudes de remediación:

- **Tiempo**. Fecha y hora en que se resuelve la solicitud.
- **Sujeto**. Nombre del remediador que procesa la solicitud.
- **Acción**. Si el remediador ha mitigado o remediado la solicitud.
- **Tipo**. `Infracción de cumplimiento` o `Derecho de usuario`.
- **Nombre de objeto**. Nombre de la directiva de auditoría que se ha infringido.
- **Recurso**. ID de cuenta del remediador (o n/d).
- **ID**. ID de cuenta relacionado con la infracción de directiva.
- **Resultado**. Siempre `satisfactorio`.

Cuando se hace clic en una indicación de tiempo de la tabla, se abre la página Detalles de incidente de auditorí-a.

En la página Detalles de incidente de auditorí-a se proporciona información sobre la solicitud completada, con información sobre la remediación o la mitigación, los parámetros de evento (si procede) y los atributos auditables.

Actualización de la tabla

Para actualizar la información de la tabla Remediaciones, haga clic en Actualizar. La página Remediaciones actualiza la tabla con las nuevas solicitudes de remediación.

Priorización de infracciones de directiva

Puede priorizar las infracciones de directiva mediante la asignación de una prioridad, una gravedad o ambas. Utilice la página Remediaciones para priorizar las infracciones.

▼ Para editar la prioridad o la gravedad de las infracciones

1. **Seleccione una o varias infracciones en la lista.**
2. **Haga clic en Priorizar.**
   Aparece la página Priorizar infracciones de directiva.
3. **También puede definir la gravedad de la infracción. Las opciones disponibles son Ninguna, Baja, Media, Alta o Crítica.**
4. **Además, puede establecer la prioridad de la infracción. Las opciones disponibles son Ninguna, Baja, Media, Alta o Urgente.**
5. **Haga clic en Aceptar cuando termine de seleccionar opciones. Identity Manager devuelve la lista de remediaciones.**

Nota – Sólo se pueden definir valores de gravedad y prioridad en remediaciones de tipo IC (infracción de cumplimiento).

Mitigación de infracciones de directiva

En las páginas Remediaciones y Revisar infracción de directiva puede mitigar las infracciones de directiva.

Página Remediaciones

▼ Para mitigar las infracciones de directiva pendientes en la página Remediaciones

1. **Seleccione filas de la tabla para especificar las solicitudes que deben mitigarse.**
   - Active una o varias opciones separadas para especificar las solicitudes que se van a mitigar.

- Active la opción del encabezado de la tabla para mitigar todas las solicitudes incluidas en la tabla.

Identity Manager sólo permite introducir una serie de comentarios para describir un acción de mitigación. Es posible que no desee realizar una acción de mitigación en masa, a menos que las infracciones estén relacionadas y que un solo comentario sea aceptable para todas ellas.

Puede mitigar las solicitudes que incluyan infracciones del cumplimiento solamente. No se pueden mitigar otras solicitudes de mitigación.

2 Haga clic en Mitigar.

Aparece la página Mitigar infracción de directiva (o la página Mitigar varias infracciones de directiva).

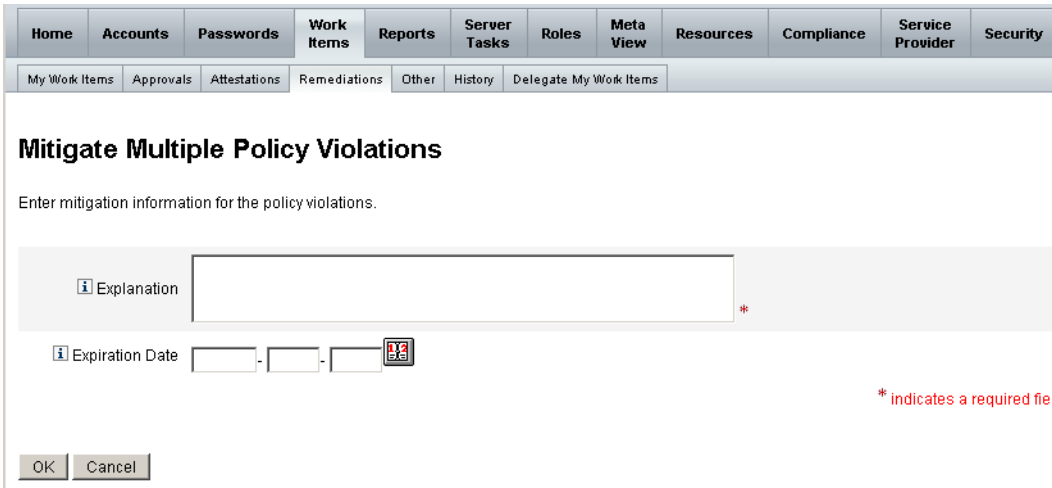


FIGURA 15–3 Página Mitigar infracción de directiva

3 Introduzca comentarios sobre la mitigación en el campo Explicación. (*imprescindible*)

Puesto que los comentarios permiten realizar un seguimiento de auditoría de esta acción, asegúrese de introducir información completa e importante. Por ejemplo, explique por qué está mitigando la infracción de directiva, la fecha y el motivo de la elección del periodo de exención.

4 Para proporciona la fecha de caducidad de la exención, introduzca la fecha (en formato `AAAA-MM-DD`) directamente en el campo Fecha de caducidad o haga clic en el botón de fecha y seleccione una fecha del calendario.

Nota – Si no introduce la fecha, la exención tendrá una validez indefinida.

---

5 Haga clic en Aceptar para guardar los cambios y regresar a la página Remediaciones.

Remediación de infracciones de directiva

▼ Para remediar una o varias infracciones de directiva

1 Utilice las casillas de la tabla para especificar las solicitudes que se van a remediar.

- Para esto, active una o varias casillas de la tabla.
- Active la casilla del encabezado de la tabla para remediar todas las solicitudes incluidas en la tabla.

  Cuando seleccione más de una solicitud, recuerde que Identity Manager sólo permite introducir una serie de comentarios para describir una acción de remediación. Es posible que no desee realizar una acción de mitigación en masa, a menos que las infracciones estén relacionadas y que un solo comentario sea aceptable para todas ellas.

2 Haga clic en Remediar.

3 Aparece la página Remediar infracción de directiva (o la página Remediar varias infracciones de directiva).

4 Introduzca los comentarios relacionados con la remediación en el campo Comentarios.

5 Haga clic en Aceptar para guardar los cambios y regresar a la página Remediaciones.

Nota – Las directivas de auditoría que se asignan directamente a un usuario (mediante una cuenta de usuario o asignación de organización) siempre vuelven a evaluarse cuando se remedia una infracción de dicho usuario.

Reenvío de solicitudes de remediación

Puede reenviar una o varias solicitudes de remediación a otro remediador.

▼ Para reenviar solicitudes de remediación

1 Utilice las casillas de la tabla para especificar las solicitudes que se van a reenviar.

- Active la casilla del encabezado de la tabla para reenviar todas las solicitudes de la tabla.
- Active casillas separadas de la tabla para reenviar una o varias solicitudes.

2 Haga clic en Reenviar.

Aparece la página Seleccionar y confirmar reenvío.

FIGURA 15–4 Página Seleccionar y confirmar reenvío

3 **Introduzca el nombre del remediador en el campo Remitir a y haga clic en Aceptar. También puede hacer clic en . . . (Más) para buscar el nombre de un remediador. Seleccione un nombre en la lista de búsqueda y haga clic en Definir para introducir ese nombre en el campo Remitir a. Haga clic en Descartar para cerrar la sección de búsqueda.**

Cuando vuelva a aparecer la página Remediaciones, el nombre del nuevo remediador aparecerá en la columna Remediador de la tabla.

Edición de un formulario de usuario de un elemento de trabajo de remediación

Si dispone de las capacidades de edición de usuarios oportunas, en el elemento de trabajo de remediación puede editar un usuario para remediar los problemas (descritos en el historial de derechos asociados).

Para editar un usuario, haga clic en Editar usuario en la página Solicitud de remediación de revisión. En la página Editar usuario que se abre aparece lo siguiente:

- Historial de derechos asociados con el usuario, para este elemento de trabajo
- Atributos del usuario

  Las opciones que se muestran aquí coinciden con las del formulario Editar usuario de la sección Cuentas.

Después de realizar cambios en el usuario, haga clic en Guardar.

Nota – Cuando se guardan los cambios, se ejecuta el flujo de trabajo de actualización de usuarios. Como este flujo de trabajo puede estar sujeto a aprobación, es posible que los cambios efectuados en las cuentas de usuario no se apliquen durante un periodo de tiempo después de guardarlos. Si la directiva de auditoría permite realizar reexploraciones y el flujo de trabajo de actualización de usuarios no ha terminado, puede detectarse la misma infracción en la exploración de directiva siguiente.

Revisiones de acceso periódicas y autenticación

Identity Manager proporciona un proceso para realizar revisiones de acceso que permiten a los administradores u otros responsables revisar y verificar los privilegios de acceso de los usuarios. Este proceso ayuda a identificar y administrar la acumulación de privilegios de usuario a lo largo del tiempo, además de contribuir a mantener el cumplimiento de la ley Sarbanes-Oxley, la ley GLBA y otras disposiciones de los reglamentos federales.

Las revisiones de acceso se pueden realizar conforme se necesitan, pero también puede planificarse para ejecutarlas periódicamente. Por ejemplo, se pueden programar trimestralmente, lo que permite realizar revisiones de acceso periódicas para mantener el nivel adecuado de privilegios de usuario. Como alternativa, cada revisión de acceso puede incluir exploraciones de directivas de auditoría.

Acerca de las revisiones de acceso periódicas

La *revisión de acceso periódica* es el proceso por el que se autentica que un conjunto de empleados tiene los privilegios adecuados en los recursos oportunos en un momento concreto.

La revisión de acceso periódica conlleva las siguientes actividades:

- **Exploraciones de revisión de acceso**. Exploraciones en las que se realizan evaluaciones de los *derechos de usuario* basadas en reglas para determinar si se requiere autenticación.
- **Autenticación**. Proceso por el que se responde a la solicitud de autenticación aprobando o rechazando los derechos de usuario.

Un *derecho de usuario* es un registro detallado de las cuentas de un usuario en una serie concreta de recursos.

Exploraciones de revisión de acceso

Para iniciar una revisión de acceso periódica, primero debe definir una exploración de acceso como mínimo.

La exploración de acceso define quién va a ser objeto de la exploración, los recursos que se incluirán en la exploración, las directivas de auditoría opcionales que se van a evaluar durante la exploración y las reglas que determinan los registros de derechos que se van a autenticar manualmente y por quién.

Proceso del flujo de trabajo de revisión de acceso

En general, el flujo de trabajo de revisión de acceso de Identity Manager:

- Crea una lista de usuarios, obtiene información de la cuenta de cada usuario y evalúa las directivas de auditoría opcionales.
- Crea registros de derechos de usuario.
- Determina si es necesario autenticar cada registro de derechos de usuario.
- Asigna elementos de trabajo a cada autenticador.
- Espera la aprobación de todos los autenticadores o el primer rechazo.
- Delega en el siguiente autenticador si no se obtiene respuesta a una solicitud en un periodo de tiempo determinado.
- Actualiza los registros de derechos de usuario con resoluciones.

Consulte la descripción de las capacidades de remediación en "Remediación de revisión de acceso" en la página 501.

Capacidades de administrador de remediación

Para realizar una revisión de acceso periódica y controlar los procesos de revisión, el usuario debe tener la capacidad Administrador de revisiones de acceso periódico de Auditor. Los usuarios que tienen la capacidad Administrador de exploraciones de acceso de Auditor pueden crear y administrar exploraciones de acceso.

Para asignar estas capacidades, edite la cuenta de usuario y modifique los atributos de seguridad. Para obtener más información sobre éstas y otras capacidades, consulte "Conceptos y administración de capacidades" en la página 216 en el Capítulo 6, "Administración".

Proceso de autenticación

La *autenticación* es el proceso de certificación que realiza uno o varios de los autenticadores designados para confirmar un derecho de usuario tal y como existe en una fecha determinada. Durante la revisión de acceso, el autenticador (o autenticadores) recibe por correo electrónico una notificación con las solicitudes de autenticación de revisión de acceso. El autenticador debe ser un usuario de Identity Manager, pero no hace falta que sea un administrador de Identity Manager.

Flujo de trabajo de autenticación

Identity Manager emplea un flujo de trabajo de autenticación que se inicia cuando una exploración de acceso identifica los registros de derechos que deben revisarse. La exploración de acceso determina la necesidad de efectuar la revisión basándose en las reglas definidas en la misma exploración.

La regla evaluada en la exploración de acceso determina si el registro de derechos de usuario tiene que autenticarse de forma manual o si se puede aprobar o rechazar automáticamente. Cuando el registro de derechos de usuario necesita autenticarse de forma manual, la exploración de acceso utiliza una segunda regla para determinar quiénes son los autenticadores adecuados.

Cada registro de derechos de usuario que se debe autenticar manualmente se asigna a un flujo de trabajo, con un elemento de trabajo por autenticador. La notificación sobre estos elementos de trabajo se puede enviar al autenticador mediante un flujo de trabajo ScanNotification, que agrupa los elementos en una notificación por autenticador y exploración. A menos que seleccione este flujo de trabajo, se enviará una notificación por derecho de usuario. Esto significa que un autenticador puede recibir varias notificaciones por exploración, y posiblemente en gran cantidad en función del número de usuarios explorados.

Acceso seguro a la autenticación

Estas opciones de autorización están relacionadas con elementos de trabajo del tipo de autenticación (authType) `AttestationWorkItem`.

- Propietario del elemento de trabajo
- Administrador directo o indirecto del propietario del elemento de trabajo
- Administrador que controla la organización a la que pertenece el propietario del elemento de trabajo
- Usuarios validados mediante las comprobaciones de autenticación

De forma predeterminada, el comportamiento de las comprobaciones de autorización es *uno* de los siguientes:

- El propietario es el usuario que intenta realizar la acción.
- El propietario está en la organización controlada por el usuario que intenta realizar la acción.
- El propietario es un subordinado del usuario que intenta realizar la acción.

Las comprobaciones segunda y tercera se pueden configurar por separado cambiando estas propiedades de formulario:

- `controlOrg`: los valores válidos son true o false.
- `subordinate`: los valores válidos son true o false.
- `lastLevel`: último nivel de subordinación que se incluye en el resultado; `-1` corresponde a todos los niveles.

El valor entero de `lastLevel` es `-1` de forma predeterminada, y hace referencia a los subordinados directos e indirectos.

Estas opciones se pueden agregar o modificar en:

```
Formulario de usuario: AccessApprovalList
```

Nota – Si define la seguridad de las autenticaciones en controlada por la organización, también se requiere la capacidad Autenticador de Auditor para modificar las autenticaciones de otros usuarios.

Autenticación delegada

De forma predeterminada, el flujo de trabajo de exploración de acceso respeta las delegaciones correspondientes a los elementos de trabajo del tipo Autenticación de revisión de acceso y Remediación de revisión de acceso, que crea el usuario para elementos de trabajo y notificaciones de autenticación. El administrador de exploración de acceso puede anular la selección de la opción Seguir delegación para que se ignoren las configuraciones de delegación. Si un autenticador ha delegado todos los elementos de trabajo a otro usuario, pero no se ha configurado la opción Seguir delegación para una exploración de revisión de acceso, el autenticador recibirá las notificaciones de solicitud de autenticación y los elementos de trabajo, *no* el usuario en el que se ha delegado.

Planificación de una revisión de acceso periódica

La revisión de acceso puede ser un proceso laborioso y largo para las empresas. El proceso de revisión de acceso periódica de Identity Manager ayuda a reducir al mínimo el coste y el tiempo que conlleva automatizar muchas partes del proceso. Sin embargo, algunos procesos siguen siendo largos. Por ejemplo, la obtención de datos de cuentas de usuario de una serie de ubicaciones de miles de usuarios es un proceso que puede durar una cantidad de tiempo considerable. La autenticación manual de registros también puede durar mucho. Una planificación adecuada mejora la efectividad del proceso y reduce en gran medida el esfuerzo que supone.

Para planificar una revisión de acceso periódica hay que tener en cuenta lo siguiente:

- La duración de la exploración puede variar mucho en función del número de usuarios y de recursos implicados.

  En una única revisión de acceso periódica de una organización grande, la exploración puede tardar uno o varios días en realizarse, mientras que la autenticación manual puede tardar en completarse una o varias semanas.

  Por ejemplo, en una organización con 50.000 usuarios y diez recursos, la exploración de acceso puede tardar aproximadamente un día en completarse, de acuerdo con los cálculos siguientes:

  1 seg/recurso * 50 K usuarios * 10 recursos / 5 subprocesos simultáneos = 28 horas

  Si los recursos están dispersos geográficamente, las latencias de red pueden incrementar la duración del proceso.
- El procesamiento paralelo mediante el uso de varios servidores de Identity Manager puede acelerar el proceso de revisión de acceso.

  La realización de exploraciones paralelas resulta más eficaz cuando las exploraciones no comparten recursos. Cuando defina una revisión de acceso, cree varias exploraciones, limite los recursos a un conjunto específico y utilice diferentes recursos en cada exploración. Cuando inicie la tarea, seleccione varias exploraciones y prográmelas para que se ejecuten de inmediato.
- La personalización del flujo de trabajo de autenticación y las reglas garantiza más control y puede ser más eficaz:

  Por ejemplo, personalice la regla de autenticador para que las tareas de autenticación se propaguen a varios autenticadores. El proceso de autenticación asigna elementos de trabajo y envía notificaciones como corresponde.
- Las reglas de escalación de autenticador ayudan a mejorar el tiempo de respuesta de las solicitudes de autenticación.

  Para configurar una cadena de escalación de autenticadores, defina la regla de autenticador de escalación predeterminado o utilice una regla personalizada. También tendrá que especificar los valores de tiempo de espera de escalación.
- Además, es necesario saber cómo utilizar las reglas de determinación de revisión para ahorrar tiempo, y establecer de modo automático los registros de derechos que deben revisarse manualmente.
- Especifique un flujo de trabajo de notificación en el nivel de exploración para agrupar la notificación de solicitudes de autenticación correspondientes a una exploración.

Ajuste de las tareas de exploración

Durante el proceso de exploración, varios subprocesos acceden a la vista del usuario, con lo que posiblemente acceden a los recursos en los que el usuario tiene cuentas. La evaluación de varias directivas y reglas de auditoría después de acceder a la vista podría dar lugar a infracciones del cumplimiento.

Para impedir que dos subprocesos actualicen la misma vista de usuario a la vez, el proceso bloquea en la memoria el nombre de usuario. Si no es posible establecer el bloqueo en 5 segundos (valor predeterminado), la tarea de exploración generará un error y se omitirá el usuario, con lo que se protegerán las exploraciones simultáneas en las que se procese el mismo conjunto de usuarios.

Puede editar los valores de varios "parámetros ajustables" que actúan como argumentos de tarea en la tarea de exploración:

- `clearUserLocks` (booleano). Si tiene el valor true, se liberan todos los bloqueos de usuarios actuales antes del inicio de la exploración.
- `userLock` (entero). Tiempo de espera (en milisegundos) cuando se intenta bloquear un usuario. El valor predeterminado es 5 segundos. Los valores negativos desactivan el bloqueo en esa exploración.
- `scanDelay` (entero). Tiempo de espera (en milisegundos) entre la distribución de subprocesos de exploración. El valor predeterminado es 0 (sin retraso). Si introduce un valor en este argumento, la exploración se ralentiza, pero el sistema responde mejor a otras operaciones.
- `maxThreads` (entero). Número de subprocesos simultáneos que se utilizan para procesar una exploración. El valor predeterminado es 5. Si los recursos tardan mucho en responder, puede aumentar este número para mejorar el rendimiento de la exploración.

Para cambiar los valores de estos parámetros, edite el formulario de definición de tarea correspondiente. Para obtener más información, consulte el Capítulo 2, "Identity Manager Forms" de *Sun Identity Manager Deployment Reference*.

Creación de una exploración de acceso

▼ Para definir la exploración de revisión de acceso

1. **Seleccione Cumplimiento → Administrar exploraciones de acceso.**
2. **Haga clic en Nuevo para que aparezca la página Crear exploración de acceso.**
3. **Asigne un nombre a la exploración de acceso.**

Nota – Los nombres de las exploraciones de acceso no deben contener estos caracteres:

’ (apóstrofo), . (punto), | (línea), [(corchete izquierdo),] (corchete derecho), , (coma), : (dos puntos), $ (símbolo del dólar), " (comillas), \ (barra diagonal inversa) y = (signo igual)

También se debe evitar el uso de estos caracteres: _ (subrayado), % (porcentaje), ^ (acento circunflejo) y * (asterisco).

4 Agregue una descripción explicativa en la identificación de la exploración (*opcional*).

5 Active la opción Derechos dinámicos para que los autenticadores tengan estas otras posibilidades:

Las opciones incluyen:

- Una autenticación pendiente se puede reexplorar inmediatamente para actualizar los datos de derechos y reevaluar la necesidad de autenticación.
- Una autenticación pendiente se puede enrutar a otro usuario para remediación. Después de la remediación, los datos de derechos se actualizan y reevalúan para determinar si se necesita autenticación.

6 Especifique el Tipo de ámbito de usuario (*imprescindible*).

Elija una de las opciones siguientes:

- **Según regla de condición de atributo**. Se exploran usuarios en función de la regla de ámbito de usuario seleccionada.

  Identity Manager ofrece varias reglas predeterminadas:

  - Todos los administradores

    Nota – Mediante el uso de Identity Manager IDE puede agregar reglas de definición de ámbitos de usuario. Para obtener información sobre Identity Manager IDE, visite `https://identitymanageride.dev.java.net/`.

  - Todos mis informes
  - Todos los no administradores
  - Mis informes directos
  - Usuarios sin administrador
- **Asignado a recursos**. Se exploran todos los usuarios que tienen una cuenta en uno o varios de los recursos seleccionados. Cuando se elige esta opción, la página muestra los recursos de ámbito de usuario para que pueda especificar recursos.

- **Según un rol específico**. Se exploran todos los miembros que tienen al menos un rol o todos los roles que ha especificado.
- **Miembros de organizaciones**. Elija esta opción para explorar todos los miembros de una o varias organizaciones seleccionadas.
- **Informa a administrador**. Se exploran todos los usuarios que rinden cuentas a los administradores seleccionados. El atributo de cuenta de Lighthouse de usuario de Identity Manager determina la jerarquía de administración.

  Si el ámbito de usuario es *organización* o *administración*, la opción Ámbito recursivo se encuentra disponible. Esta opción permite seleccionar usuarios de forma recursiva mediante la cadena de miembros controlados.

7 Si además elige explorar directivas de auditoría para detectar infracciones durante la exploración de revisión de acceso, seleccione las directivas de auditoría que deben aplicarse a esta exploración. Para esto, mueva las opciones que ha elegido en la lista Directivas de auditorí-a disponibles hasta la lista Directivas de auditorí-a actuales.

Al agregar directivas de auditoría a una exploración de acceso se obtiene el mismo resultado que cuando se realiza una exploración de auditoría en el mismo conjunto de usuarios. Sin embargo, las infracciones que detectan las directivas de auditoría se almacenan en el registro de derechos de usuario. Esta información puede facilitar la aprobación o el rechazo automáticos, ya que la regla puede utilizar la presencia o ausencia de infracciones en el registro de derechos de usuario como parte de su lógica.

8 Si ha explorado directivas de auditoría en el paso anterior, puede utilizar la opción Modo de directiva para especificar cómo determina la exploración de acceso las directivas de auditoría que se van a ejecutar con un usuario determinado. Los usuarios pueden tener directivas asignadas en el nivel de usuario, en el nivel de organización o ambos. De forma predeterminada, la exploración de acceso sólo aplica las directivas especificadas para la exploración cuando el usuario no tiene asignadas directivas.

a. Aplicar las directivas seleccionadas e ignorar otras asignaciones

b. Aplicar las directivas seleccionadas solamente si el usuario no tiene otras asignaciones

c. Aplicar las directivas seleccionadas además de otras asignaciones de usuario

9 (Opcional) Especificar propietario del proceso de revisión. Utilice esta opción para especificar el propietario de la tarea de revisión de acceso que se está definiendo. Cuando se especifica el propietario del proceso de revisión, cualquier autenticador que encuentre un posible conflicto a la hora de responder a una solicitud de autenticación puede *abstenerse* en lugar de aprobar o rechazar el derecho de usuario; la solicitud de autenticación se reenviará al propietario del proceso de revisión. Haga clic en el cuadro de selección (elíptico) para buscar las cuentas de usuario y realizar la selección.

10 Seguir delegación. Seleccione esta opción para activar la delegación para la exploración de acceso. Cuando marque esta opción, la exploración de acceso respetará las configuraciones de delegación. Esta opción está activada de forma predeterminada.

11 Restringir recursos destino. Seleccione esta opción para limitar la exploración a los recursos de destino.

Esta opción está directamente relacionada con la eficacia de la exploración de acceso. Si no limita los recursos de destino, cada registro de derechos de usuario incluirá información de las cuentas de todos los recursos a los que esté vinculado el usuario. Esto significa que se consultan todos los recursos asignados de cada usuario durante la exploración. Si utiliza esta opción para especificar un subconjunto de recursos, puede reducir en gran medida el tiempo de procesamiento que necesita Identity Manager para crear los registros de derechos de usuario.

12 Ejecutar remediación de infracción. Seleccione esta opción para que se active el flujo de trabajo de remediación de la directiva de auditoría cuando se detecte una infracción.

Cuando se selecciona esta opción, se ejecuta el flujo de trabajo de remediación de la directiva de auditoría cuya infracción se ha detectado.

Normalmente no debe seleccionarse esta opción, a menos que se trate de casos avanzados.

13 Flujo de trabajo de aprobación de acceso. Seleccione el flujo de trabajo de autenticación estándar predeterminado o un flujo de trabajo personalizado, si está disponible.

Este flujo de trabajo permite presentar el registro de derechos de usuario a los autenticadores apropiados (según la regla de autenticador) para que lo revisen. El flujo de trabajo de autenticación estándar predeterminado crea un elemento de trabajo por autenticador. Si se especifica la escalación en la exploración de acceso, este flujo de trabajo se encarga de asignar los elementos de trabajo que han estado inactivos durante mucho tiempo. Cuando no se especifique ningún flujo de trabajo, la autenticación de usuario permanecerá en estado pendiente de forma indefinida.

.

Nota – Para obtener más información sobre las reglas de Identity Auditor mencionadas en este paso y en los pasos siguientes, consulte el Capítulo 4, "Working with Rules" de *Sun Identity Manager Deployment Reference*.

---

14 Regla de autenticador. Seleccione la regla Autenticador predeterminado o una regla de autenticador personalizada, si existe.

La regla de autenticador en la que se introduce el registro de derechos de usuario, devuelve una lista con los nombres de los autenticadores. Cuando se selecciona Seguir delegación, la exploración de acceso cambia la lista de nombres por los nombres adecuados después de que cada usuario configure la información de delegación en la lista original de nombres. Si la delegación de un usuario de Identity Manager produce un ciclo de direccionamiento, la información de delegación se descarta y el elemento de trabajo se envía al autenticador inicial.

La regla de `Autenticador predeterminado` establece que el autenticador debe ser el administrador (idmManager) del usuario al que representa el registro de derechos, o la cuenta de configuración si el `idmManager` del usuario es nulo. Cuando sea necesario incluir a los propietarios de recursos y los administradores en la autenticación, tendrá que utilizar una regla personalizada.

15 Regla de escalación de autenticador. Utilice esta opción para especificar la regla de autenticador de escalación predeterminado o seleccionar una regla personalizada, si existe. También puede especificar el valor de Tiempo de espera de escalada de la regla. El valor predeterminado es 0 días.

Esta regla especifica la cadena de escalación que se utiliza con cualquier elemento de trabajo que haya superado el tiempo de espera de escalación. La regla de autenticador de escalación predeterminado delega las solicitudes en el administrador del autenticador designado (`idmManager`), o en el usuario Configurator si el valor `idmManager` del autenticador es nulo.

Puede especificar el tiempo de espera de escalación en minutos, horas o días.

El documento contiene información adicional sobre la regla de escalación de autenticador.

16 Regla de determinación de revisión. (*imprescindible*)

Seleccione una de las reglas siguientes para especificar la forma en que el proceso de exploración determinará la disposición de un registro de derechos:

- **Rechazar usuarios cambiados**. Rechaza automáticamente un registro de derechos de usuario si el último derecho de usuario de la misma definición de exploración de acceso no coincide y este derecho está aprobado. En caso contrario, fuerza una autenticación manual y aprueba todos los derechos de usuario que no han sufrido cambios con respecto al derecho de usuario previamente aprobado. De forma predeterminada, sólo se compara la parte correspondiente a las "cuentas" de la vista de usuario.
- **Revisar usuarios cambiados**. Fuerza la autenticación manual de cualquier registro de derechos de usuario si el último derecho de usuario de la misma definición de exploración de acceso no coincide y este derecho está aprobado. Aprueba todos los derechos de usuario que no han experimentado cambios con respecto al derecho de usuario aprobado anteriormente. De forma predeterminada, sólo se compara la parte correspondiente a las "cuentas" de la vista de usuario.
- **Revisar todos**. Fuerza la autenticación manual de todos los registros de derechos de usuario.

En las reglas Rechazar usuarios cambiados y Revisar usuarios cambiados se compara el derecho de usuario con la última instancia de la misma exploración de acceso en la que se ha aprobado el registro de derechos.

Si quiere cambiar este comportamiento, puede copiar y modificar las reglas para limitar la comparación a la parte que elija de la vista del usuario.

Esta regla puede devolver los siguientes valores:

- **-1**. No se requiere autenticación.
- **0**. La autenticación se rechaza automáticamente.
- **1**. Se requiere autenticación manual.
- **2**. La autenticación se aprueba automáticamente.
- **3**. La autenticación se remedia automáticamente.

  El documento contiene información adicional sobre la regla de determinación de revisión.

17 Regla de remediador. Seleccione la regla que se va a utilizar para determinar quién debe remediar un derecho de un determinado usuario en caso de remediación automática. La regla puede examinar los derechos e infracciones del usuario actual, y debe devolver una lista de usuarios que deben remediar. Si no se especifica ninguna regla, no se realizará ninguna remediación. Esta regla suele utilizarse cuando el derecho infringe el cumplimiento.

18 Regla de formulario de usuario de remediación. Seleccione la regla que se va a utilizar para seleccionar el formulario que deben utilizar los remediadores de autenticación para editar usuarios. Los remediadores pueden tener un formulario propio, que anula éste. Esta regla de formulario se configura cuando en la exploración se recopilan datos muy específicos que coinciden con los de un formulario personalizado.

19 Flujo de trabajo de notificación.

Seleccione una de las opciones siguientes para especificar el comportamiento de notificación de cada elemento de trabajo:

- **Ninguno**. Es el valor predeterminado. Con este valor, el autenticador recibe una notificación por correo electrónico por cada derecho de usuario que debe autenticar.
- **ScanNotification**. Esta opción agrupa las solicitudes de autenticación en una sola notificación. En la notificación se indica la cantidad de solicitudes de autenticación asignadas al destinatario.

  Si se ha especificado el propietario del proceso de revisión en la exploración de acceso, el flujo de trabajo ScanNotification también enviará una notificación a ese propietario al principio y al final de la exploración. Consulte "Creación de una exploración de acceso" en la página 485.

  El flujo de trabajo ScanNotification utiliza las plantillas de correo electrónico siguientes:

  - Aviso de inicio de exploración de acceso
  - Aviso de finalización de exploración de acceso
  - Aviso de autenticación masiva

    El flujo de trabajo ScanNotification se puede personalizar.

20 **Límite de infracción. Utilice esta opción para especificar el número máximo de infracciones de cumplimiento que puede emitir esta exploración antes de que se anule. El límite predeterminado es 1000. No existe ningún límite si el campo se deja vacío.**

Aunque el número de infracciones de directiva suele ser bajo en comparación con el número de usuarios durante las exploraciones de acceso o auditoría, la configuración de este valor podría evitar la repercusión que tendría una directiva defectuosa que incrementara el número de infracciones de forma significativa. Por ejemplo, imagínese la siguiente situación:

Si una exploración de acceso incluye 50.000 usuarios y genera de dos a tres infracciones por usuario, el coste de remediar cada infracción del cumplimiento podría repercutir negativamente en el sistema Identity Manager.

21 **Organizaciones. Seleccione las organizaciones para las que está disponible este objeto de exploración de acceso. Se trata de un campo obligatorio.**

Haga clic en Guardar para guardar la definición de exploración.

Eliminación de una exploración de acceso

Puede eliminar una o varias exploraciones de acceso. Para eliminar una exploración de acceso, seleccione Administrar exploraciones de acceso en la ficha Cumplimiento, elija el nombre de la exploración y haga clic en Eliminar.

Administración de revisiones de acceso

Después de definir una exploración de acceso, puede utilizarla o programarla como parte de una revisión de acceso. Tras iniciar la revisión de acceso, aparecen varias opciones para administrar el proceso de revisión.

Consulte las secciones siguientes para obtener más información sobre:

- "Inicio de una revisión de acceso" en la página 492
- "Programación de tareas de revisión de acceso" en la página 492
- "Administración del desarrollo de la revisión de acceso" en la página 493
- "Modificación de los atributos de exploración" en la página 494
- "Cancelación de una revisión de acceso" en la página 494
- "Eliminación de una revisión de acceso" en la página 495

Inicio de una revisión de acceso

Para iniciar una revisión de acceso desde la interfaz de administración, utilice uno de estos métodos:

- Haga clic en Iniciar revisión en la página Cumplimiento → Revisiones de acceso.
- Seleccione todas las tareas de revisión de acceso en la página Tareas del servidor → Ejecutar tareas.

En la página Iniciar tarea que aparece, especifique el nombre de la revisión de acceso. Seleccione exploraciones en la lista exploraciones de acceso disponibles y trasládelas a la lista Seleccionado.

Si selecciona más de una exploración, puede elegir una de las opciones de inicio siguientes:

- **inmediatamente**. La exploración comienza a ejecutarse inmediatamente después de hacer clic en el botón Iniciar. Si selecciona esta opción para varias exploraciones en la tarea de inicio, las exploraciones se ejecutarán en paralelo.
- **tras una espera**. Esta opción permite especificar el tiempo de espera que debe transcurrir antes de que se inicie la exploración, lo que depende del inicio de la tarea de revisión de acceso.

Nota – Puede iniciar varias exploraciones durante la sesión de revisión de acceso. Sin embargo, debe tener en cuenta que cada exploración puede incluir un gran número de usuarios y, por consiguiente, el proceso de exploración puede tardar varias horas en finalizar. Se recomienda planificar las exploraciones en función de esto. Por ejemplo, puede iniciar una exploración de ejecución inmediata y programar otras exploraciones de forma escalonada.

Haga clic en Iniciar para que el proceso de revisión de acceso comience.

Nota – El nombre que asigna a la revisión de acceso es importante. En algunos informes se pueden comparar las revisiones de acceso que se ejecutan de forma periódica y tienen el mismo nombre.

Cuando se inicia la revisión de acceso, aparece el diagrama del proceso del flujo de trabajo, donde se muestran los pasos del proceso.

Programación de tareas de revisión de acceso

Las tareas de revisión de acceso se pueden programar en la sección Tareas del servidor. Por ejemplo, para configurar revisiones de acceso periódicas, seleccione Administrar programa y defina el programa. Puede programar la tarea para que se realice cada mes o cada trimestre.

Para definir el programa, seleccione la tarea Revisión de acceso en la página Programar tareas y rellena la información de la página Crear programa de tareas.

Haga clic en Guardar para guardar la tarea programada.

Nota – Identity Manager conserva los resultados de las tareas de revisión de acceso durante una semana, de forma predeterminada. Si decide programar una revisión con una frecuencia más alta que la semanal, configure Opciones de resultados en Eliminar. Si no se configura de esta manera, la nueva revisión no se ejecutará debido a que todavía existe la tarea anterior.

Administración del desarrollo de la revisión de acceso

Utilice la ficha Revisiones de acceso para supervisar el desarrollo de la revisión de acceso. La ficha Cumplimiento proporciona acceso a esta función.

En la ficha Revisiones de acceso puede revisar el resumen de todas las revisiones de acceso activas y procesadas previamente. Por cada revisión de acceso de la lista se proporciona la siguiente información:

- **Estado**. Estado actual del proceso de revisión: inicializando, terminando, terminado, número de exploraciones en curso, número de exploraciones programadas, en espera de autenticación o completado.
- **Fecha de inicio**. Fecha (indicación de tiempo) de inicio de la tarea de revisión de acceso.
- **Usuarios totales**. Número total de usuarios que se van a explorar.
- **Detalles de derechos**. Columnas adicionales de la tabla en las que se proporcionan todos los derechos por estado. Se incluyen detalles, como pendiente, aprobado, rechazado, terminado, derechos remediados y derechos totales.

  En la columna Remediación se indica el número de derechos que se encuentran en el estado REMEDIANDO. Cuando se remedia un derecho, pasa al estado PENDIENTE; por consiguiente, el valor de esta columna es cero cuando concluye la revisión de acceso.

Si quiere consultar información más detallada sobre la revisión, puede seleccionar la revisión para acceder al informe de resumen.

En la Figura 15–5 se muestra un ejemplo de informe de resumen de revisión de acceso.

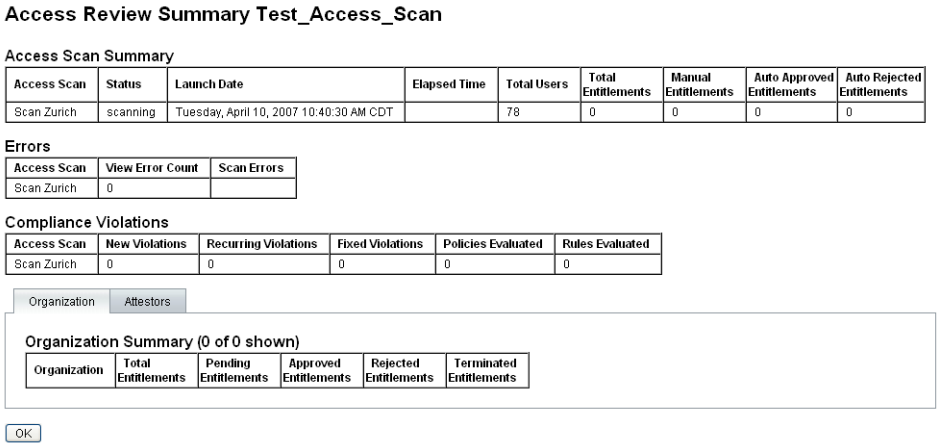


FIGURA 15–5 Página de informe de resumen de revisión de acceso

Haga clic en la ficha de formulario Organización o Autenticadores para ver la información de exploración clasificada por dichos objetos.

Si ejecuta el informe de resumen de revisión de acceso, también puede revisar y descargar la información de un informe.

Modificación de los atributos de exploración

Después de configurar una exploración de acceso, puede editarla para especificar nuevas opciones, como recursos de destino por explorar o directivas de auditoría para buscar infracciones mientras se ejecuta la exploración de acceso.

Para editar una definición de exploración, selecciónela en la lista de exploraciones de acceso y modifique los atributos en la página Editar exploración de revisión de acceso.

Para guardar los cambios en la definición, haga clic en Guardar.

Nota – El cambio del ámbito de una exploración de acceso puede modificar la información de los registros de derechos de usuario recién adquiridos, ya que puede afectar a la regla de determinación de revisión si esa regla compara los derechos de usuario con registros de derechos de usuario anteriores.

Cancelación de una revisión de acceso

En la página Revisiones de acceso, haga clic en Terminar para detener la revisión en curso seleccionada.

Al terminar la revisión, ocurre lo siguiente:

- Se cancela la programación de las exploraciones programadas.
- Se detienen las exploraciones activas.
- Se eliminan todos los flujos de trabajo y elementos de trabajo pendientes.
- Todas las autenticaciones pendientes se marcan como canceladas.
- No se modifican las autenticaciones completadas por usuarios.

Eliminación de una revisión de acceso

En la página Revisiones de acceso, haga clic en Eliminar para borrar la revisión seleccionada.

La revisión de acceso se puede eliminar si la tarea se encuentra en el estado *terminado* o *completado*. Las tareas de revisión de acceso que se están ejecutando no se pueden eliminar a menos que se terminen antes.

Al eliminar una revisión de acceso se borran todos los registros de derechos de usuario que ha generado la revisión. La operación de eliminación queda reflejada en el registro de auditoría.

Para eliminar una revisión de acceso, haga clic en Eliminar en la página Revisiones de acceso.

Nota – La cancelación y la eliminación de una revisión de acceso puede hacer que se actualice un gran número de objetos y tareas de Identity Manager, operación que puede tardar varios minutos en completarse. Para comprobar el desarrollo de la operación, puede consultar los resultados de la tarea en Tareas del servidor → Todas las tareas.

Administración de tareas de autenticación

Puede administrar las solicitudes de autenticación en la interfaz de usuario o administración de Identity Manager. En esta sección se proporciona información relacionada con la respuesta a solicitudes de autenticación y las tareas que incluye la autenticación.

Notificación de revisión de acceso

Durante la exploración, Identity Manager notifica a los autenticadores si las solicitudes de autenticación requieren aprobación. Si las responsabilidades de autenticación se han delegado, las solicitudes se envían al delegado. Cuando se definen varios autenticadores, cada uno de ellos recibe una notificación por correo electrónico.

Las solicitudes aparecen como elementos de trabajo de autenticación en la interfaz de Identity Manager. Los elementos de trabajo de autenticación pendientes se muestran cuando el autenticador asignado inicia una sesión en Identity Manager.

Visualización de solicitudes de autenticación pendientes

Los elementos de trabajo de autenticación se pueden ver en la sección Elementos de trabajo de la interfaz. Cuando se selecciona la ficha Autenticación en la sección Elementos de trabajo, se muestran todos los registros de derechos que requieren aprobación. En la página Autenticaciones también puede ver la lista de los registros de derechos correspondientes a todos los informes directos y a los usuarios especificados, que puede controlar de forma directa o indirecta.

Actuación en registros de derechos

Los elementos de trabajo de autenticación contienen los registros de derechos de usuario que deben revisarse. Los registros de derechos proporcionan información sobre los privilegios de acceso de usuario, los recursos asignados y las infracciones del cumplimiento.

A continuación se indican las posibles respuestas a una solicitud de autenticación:

- **Aprobar**. Permite confirmar que el derecho es correcto conforme a la fecha que aparece en el registro de derechos.
- **Rechazar**. El registro de derechos indica posibles discrepancias que no se pueden validar o remediar en este momento.
- **Reexplorar**. Se solicita una reexploración para volver a evaluar el derecho de usuario.
- **Reenviar**. Permite especificar un destinatario de la revisión diferente.
- **Abstener**. La autenticación para este registro no es apropiada y no se conoce un autenticador más adecuado. El elemento de trabajo de autenticación se reenvía al propietario del proceso de revisión. Esta opción sólo se encuentra disponible cuando se define el propietario del proceso de revisión en la tarea Revisión de acceso.

Si un autenticador no responde a una solicitud mediante una de estas acciones antes del tiempo de espera de escalación especificado, se enviará un aviso al siguiente autenticador incluido en la cadena de escalación. El proceso de notificación continúa hasta que se obtiene una respuesta.

El estado de autenticación se puede supervisar en la ficha Cumplimiento → Revisiones de acceso.

Remediación de bucle cerrado

Puede evitar que se rechacen derechos de usuario si:

- Marca un derecho como que requiere corrección mediante la solicitud de una corrección a otro usuario (remediación de solicitud). En este caso se crea un elemento de trabajo de remediación nuevo, que se asigna a uno o varios remediadores especificados.

  El nuevo remediador puede editar el usuario, ya sea mediante el uso de Identity Manager o de forma independiente, y luego marcar el elemento de trabajo como remediado cuando esté satisfecho con el resultado. En ese momento se vuelve a explorar y evaluar el derecho de usuario.
- Solicita reevaluar el derecho (reexploración). En tal caso, el derecho de usuario se volverá a explorar y evaluar. El elemento de autenticación original se cierra. Si el derecho sigue requiriendo autenticación conforme a las reglas definidas en la exploración de acceso, se creará un elemento de trabajo de autenticación nuevo.

Solicitud de remediación

Si se define mediante la exploración de acceso, puede dirigir una autenticación pendiente a otro usuario para su remediación.

Nota – Esta función se activa con la opción Derechos dinámicos de las páginas Crear o Editar exploración de acceso.

▼ Para solicitar remediación a otro usuario

1. **Seleccione uno o varios derechos en la lista de autenticaciones y haga clic en Solicitar remediación.**

   Aparece la página Seleccione y confirme la solicitud de remediación.

2. **Introduzca un nombre de usuario y haga clic en Añadir para incluir al usuario en el campo Remitir a. También puede hacer clic en ... (Más) para buscar usuarios. Seleccione el usuario en la lista de búsqueda y haga clic en Añadir para incluir al usuario en la lista Remitir a. Haga clic en Descartar para cerrar la sección de búsqueda.**

3. **Introduzca comentarios en el campo correspondiente y haga clic en Continuar.**

   Identity Manager regresa a la lista de autenticaciones.

Nota – La sección Historial del derecho de usuario específico muestra información detallada sobre la solicitud de remediación.

Reexploración de autenticaciones

Si la exploración de acceso lo establece, puede volver a explorar y evaluar las autenticaciones pendientes.

Nota – Esta función se activa con la opción Derechos dinámicos de las páginas Crear o Editar exploración de acceso.

▼ Para reexplorar una autenticación pendiente

1. **Seleccione uno o varios derechos en la lista de autenticaciones y haga clic en Reexplorar.**

   Aparece la página Reexplorar derechos de usuario.

2. **Introduzca comentarios sobre la acción de reexploración en la sección correspondiente y haga clic en Continuar.**

Reenvío de elementos de trabajo de autenticación

Puede remitir uno o varios elementos de trabajo de autenticación a otro usuario.

▼ Para reenviar autenticaciones

1. **Seleccione uno o varios elementos de trabajo en la lista de autenticaciones y haga clic en Reenviar.**

   Aparece la página Seleccionar y confirmar reenvío-.

2. **Introduzca un nombre de usuario en el campo Remitir a. Como alternativa, haga clic en ... (Más) para buscar un nombre de usuario.**

3. **Introduzca comentarios sobre la acción de reenvío en el área Comentarios.**

4. **Haga clic en Continuar.**

   Identity Manager regresa a la lista de autenticaciones.

Nota – El área Historial del derecho de usuario específico muestra información sobre la acción de reenvío.

Firma digital de acciones de revisión de acceso

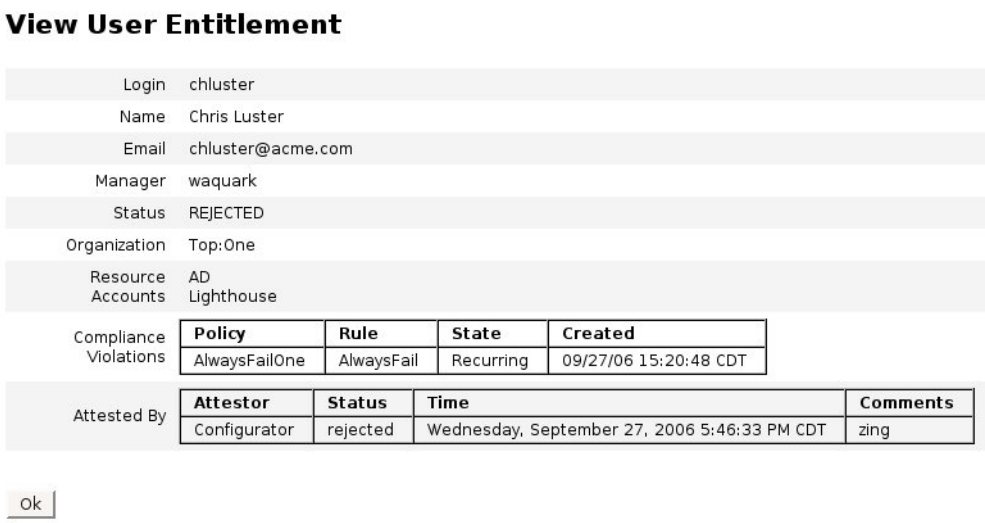
Puede configurar la firma digital para controlar las acciones de revisión de acceso. Para obtener información sobre la configuración de la firma digital, consulte "Firma de aprobaciones"

en la página 239. En los temas que se tratan aquí se explica la configuración de servidor y cliente que se necesita para agregar el certificado y el CRL a Identity Manager para firmar aprobaciones.

Informes de revisión de acceso

Identity Manager proporciona los siguientes informes, que puede utilizar para evaluar los resultados de una revisión de acceso:

- **Informe de cobertura de revisión de acceso**. Proporciona una lista de usuarios con coincidencias o diferencias de derechos de usuario, o ambas opciones, en formato de tabla, dependiendo de la forma en que se defina el informe. Este informe también puede contener columnas adicionales que muestran las revisiones de acceso que contienen coincidencias, diferencias o ambas cosas.
- **Informe de detalle de revisión de acceso**. Este informe presenta una tabla con la siguiente información:
  - **Nombre**. Nombre del registro de derechos de usuario.
  - **Estado**. Estado actual del proceso de revisión: inicializando, terminando, terminado, número de exploraciones en curso, número de exploraciones programadas, en espera de autenticación o completado.
  - **Autenticador**. Usuarios de Identity Manager asignados al registro en calidad de autenticador.
  - **Fecha de exploración**. Indicación de tiempo que se registra en el momento en que se realiza la exploración.
  - **Fecha de disposición**. Fecha (indicación de tiempo) en la que se autentica el registro de derechos.
  - **Organización**. Organización del usuario incluido en los registros de derechos.
  - **Administrador**. Administrador del usuario explorado.
  - **Recursos**. Recursos en los que el usuario tiene cuentas que se han registrado en este derecho de usuario.
  - **Infracciones**. Número de infracción detectadas durante la revisión.
  - Haga clic en un nombre del informe para abrir el registro de derechos de usuario. En los "Informes de revisión de acceso" en la página 499 se muestra un ejemplo de la información proporcionada en la vista del registro de derechos de usuario.



View User Entitlement

Login	chluster
Name	Chris Luster
Email	chluster@acme.com
Manager	waquark
Status	REJECTED
Organization	Top:One
Resource Accounts	AD Lighthouse

Compliance Violations

Policy	Rule	State	Created
AlwaysFailOne	AlwaysFail	Recurring	09/27/06 15:20:48 CDT

Attested By

Attestor	Status	Time	Comments
Configurator	rejected	Wednesday, September 27, 2006 5:46:33 PM CDT	zing

Ok

- **Informe de resumen de revisión de acceso**.

  En este informe, que también se describe en "Administración del desarrollo de la revisión de acceso" en la página 493 y se muestra en la Figura 15–5, aparece la siguiente información resumida sobre las exploraciones de acceso seleccionadas para el informe:

  - **Nombre de revisión**. Nombre de la exploración de acceso.
  - **Fecha**. Indicación de tiempo del inicio de la revisión.
  - **Recuento de usuarios**. Número de usuarios explorados para revisión.
  - **Recuento de derechos**. Número de registros de derechos generados.
  - **Aprobado**. Número de registros de derechos aprobados.
  - **Rechazado**. Número de registros de derechos rechazados.
  - **Pendiente**. Número de registros de derechos todavía pendientes.
  - **Cancelado**. Número de registros de derechos cancelados.

    Estos informes se pueden descargar en formato PDF (Portable Document Format) o CSV (valores separados por coma) desde la página Ejecutar informes.

Remediación de revisión de acceso

La remediación y mitigación de infracciones del cumplimiento, así como la remediación de revisión de acceso, se pueden administrar en la sección Remediaciones de la ficha Elementos de trabajo. No obstante, existen diferencias entre los dos tipos de remediación. En esta sección se explica el comportamiento exclusivo de la remediación de revisión de acceso, así como la diferencia que existe con las tareas de remediación y la información descritas en "Remediación y mitigación de infracciones del cumplimiento" en la página 470.

Acerca de la remediación de revisión de acceso

Cuando un autenticador solicita remediar un derecho de usuario, el flujo de trabajo de autenticación estándar crea una solicitud de remediación que debe controlar un remediador (el usuario designado al que se permite evaluar y responder a las solicitudes de remediación).

El problema sólo se puede remediar; no se puede mitigar. La autenticación no puede continuar hasta que el problema se resuelve.

Cuando las remediaciones son resultado de una revisión de acceso, el panel de control Revisión de accesos realiza un seguimiento de todos los autenticadores y remediadores involucrados en la revisión.

Escalación de solicitudes de remediación de revisión de acceso

Las solicitudes de remediación de revisión de acceso no se delegan más allá del remediador inicial.

Proceso del flujo de trabajo de remediación

La lógica de la remediación de revisión de acceso se define en el flujo de trabajo de autenticación estándar.

Cuando un autenticador solicita remediar un derecho de usuario, el flujo de trabajo de autenticación estándar:

- Genera una solicitud de remediación (del tipo `accessReviewRemediation`) que contiene información sobre el derecho de usuario que requiere remediación .
- Envía una notificación al remediador solicitado por correo electrónico.

El nuevo remediador puede editar el usuario, ya sea mediante el uso de Identity Manager o de forma independiente, y marcar el elemento de trabajo como remediado cuando esté satisfecho con el resultado. En ese momento se vuelve a explorar y evaluar el derecho de usuario.

Respuestas de remediación de revisión de acceso

El remediador de revisión de acceso dispone de tres opciones de respuesta de forma predeterminada:

- **Remediar**. Un remediador indica que se ha realizado alguna acción para solucionar el problema.

  El derecho de usuario se vuelve a explorar y evaluar. Si el derecho de usuario se vuelve a marcar por requerir autenticación, el autenticador original verá que el derecho de usuario vuelve a aparecer en la lista del elemento de trabajo Autenticaciones.

  Los detalles de la acción de solicitud de remediación aparecen en la sección Historial del derecho de usuario en concreto.

- **Reenviar**. Un remediador reasigna la responsabilidad de resolver la solicitud de remediación a otra persona.

  El área Historial del derecho de usuario específico muestra información sobre la acción de reenvío.

- **Editar usuario**. Un remediador elige editar directamente el usuario para remediar el problema.

  Este botón sólo se muestra cuando el remediador tiene permiso para modificar usuarios. Después de realizar cambios en el usuario y de hacer clic en Guardar, el remediador accede a la página de confirmación de remediación para introducir un comentario en el que se describa el cambio realizado en el usuario.

  Entonces se vuelve a explorar y evaluar el derecho de usuario. Si el derecho de usuario se vuelve a marcar por requerir autenticación, el autenticador original verá que el derecho de usuario vuelve a aparecer en la lista del elemento de trabajo Autenticaciones.

  La sección Historial del derecho de usuario específico muestra información detallada sobre la acción de edición.

Página Remediaciones

En la columna Tipo aparece UE (derecho de usuario) para todos los elementos de trabajo de remediación que son de revisión de acceso.

Acciones de remediación de revisión de acceso incompatibles

La funciones de priorización y mitigación no son compatibles con las remediaciones de revisión de acceso.

◆ ◆ ◆ CAPÍTULO 16

Exportador de datos

El Exportador de datos le permite escribir información sobre usuarios, roles y otros tipos de objetos en un almacén de datos externo.

En este capítulo encontrará información y procedimientos para configurar y mantener el Exportador de datos. La planificación e implementación detalladas del Exportador de datos se explican en el Capítulo 5, "Data Exporter" de *Sun Identity Manager Deployment Guide*.

El capítulo se ha organizado como sigue:

¿Qué es el Exportador de datos?

Identity Manager contiene y procesa datos importantes para administrar las identidades en todas las aplicaciones y sistemas distribuidos. Con el fin de elevar el rendimiento total, Identity Manager no conserva todos los datos que genera durante el abastecimiento normal y otras actividades cotidianas. Por ejemplo, de manera predeterminada Identity Manager no mantiene en estado intermedio las actividades de flujo de trabajo ni las instancias de tarea. Si es preciso capturar todos o algunos de los datos que Identity Manager suele descartar, puede habilitar la funcionalidad del Exportador de datos.

Cuando el Exportador de datos está habilitado, Identity Manager almacena cada cambio detectado en un objeto especificado (tipo de datos) como un registro de una tabla del depósito. Estos eventos se retienen en la cola hasta que una tarea los escribe en un almacén de datos externo. (Es posible configurar la frecuencia con que se exporta cada tipo de datos.) Los datos

exportados pueden seguir procesándose o utilizarse como base en consultas y transformaciones con herramientas de transformación, generación de informes y análisis comerciales.

La exportación de datos a un almacén de datos perjudica el rendimiento del servidor de Identity Manager, de ahí que sólo deba habilitarse cuando la información exportada se necesite por motivos comerciales.

Identity Manager también le permite crear y ejecutar consultas forenses, que realizan búsquedas en el almacén de datos para identificar los objetos de usuario o de rol que cumplen los criterios especificados. Para obtener más información, consulte "Configuración de consultas forenses" en la página 516.

Planificación de la implementación del Exportador de datos

Como el Exportador de datos está inhabilitado de manera predeterminada, hay que configurarlo para que sea operativo. Antes de iniciar la configuración del Exportador de datos hay que tomar varias decisiones:

- ¿Qué tipos de datos se van a exportar?
- ¿Con qué técnicas se capturará cada tipo de datos?
- ¿Con qué frecuencia se exportarán los datos de cada tipo?
- ¿Qué contendrá el esquema exportado de cada tipo?
- ¿Se necesitará una clase de fábrica personalizada de código de interfaz de almacén de datos (WIC)?

Cuando el Exportador de datos está habilitado, la configuración predeterminada exporta todos los atributos de todos los tipos de datos. Esto puede suponer una sobrecarga de proceso inútil para Identity Manager y el almacén de datos, al ocupar un espacio de almacenamiento que nunca se va a aprovechar. El almacenamiento de datos es un proceso conservador que tiende a capturar cualquier dato que pueda tener un posible uso futuro. No es necesario exportar todos los datos exportables. Puede configurar los tipos de datos que se deben exportar e impedir la exportación de determinados eventos.

Una vez tomadas las decisiones anteriores, siga estos pasos para implementar el Exportador de datos:

▼ Para implementar el Exportador de datos

1 **(Opcional) Personalice el esquema de exportación para los tipos seleccionados y regenere la DDL del almacén. Para obtener más información, consulte "Customizing Data Exporter" de *Sun Identity Manager Deployment Guide*.**

2. **Cree una cuenta de usuario en el RDBMS del almacén y cargue la DDL del almacén en dicho sistema. Para obtener más información, consulte "Customizing Data Exporter" de *Sun Identity Manager Deployment Guide*.**

3. **Configure el Exportador de datos como se explica en "Configuración del Exportador de datos" en la página 505.**

4. **Verifique si la configuración del Exportador de datos es correcta. Para obtener más información, consulte "Verificación del Exportador de datos" en la página 515.**

5. **(Opcional) Cree consultas forenses que busquen los datos escritos en el almacén de datos. Para obtener más información, consulte "Configuración de consultas forenses" en la página 516.**

6. **Mantenga el Exportador de datos mediante JMX y supervisando los archivos de registro. Para obtener más información, consulte "Mantenimiento del Exportador de datos" en la página 520.**

Configuración del Exportador de datos

En la página de configuración del Exportador de datos puede definir qué tipos de datos se retienen, especificar qué atributos se exportan y programar cuando se exportan los datos. Cada tipo de datos se puede configurar por separado.

▼ Para configurar el Exportador de datos

1. **En la interfaz de administración, seleccione Configurar en el menú principal. A continuación, haga clic en la ficha secundaria Almacén. Aparece la página Configuración del exportador de datos.**

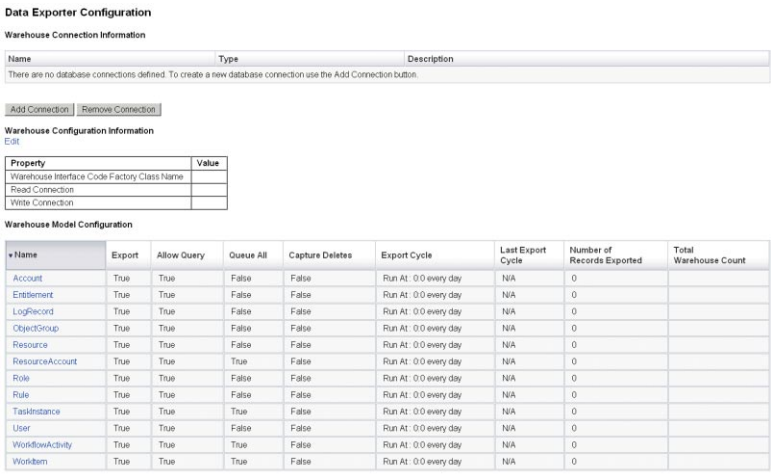


FIGURA 16–1 Configuración del exportador de datos

2 Para definir conexiones de lectura y escritura, pulse el botón Agregar conexión. Aparece la página Editar conexión a base de datos.

Rellene los campos de esta página y pulse Guardar para volver a la página Configuración del exportador de datos. Encontrará más información en "Definición de conexiones de lectura y escritura" en la página 507.

3 Para asignar la clase WIC y las conexiones de base de datos, pulse el vínculo Editar que aparece en la sección Información de configuración de almacén. Aparece la página Configuración del almacén de exportador de datos.

Rellene los campos de esta página y pulse Guardar para volver a la página Configuración del exportador de datos. Encontrará más información en "Definición de la información de configuración de almacén" en la página 509.

4 Haga clic en un vínculo de tipo de datos de la tabla Configuración de modelo de almacén. Aparece la página Configuración del tipo de exportador de datos.

Rellene las fichas Exportar, Atributos y Programar de esta página y pulse Guardar para volver a la página Configuración del exportador de datos. Para obtener más información, consulte "Configuración de modelos de almacén" en la página 510.

Repita este paso con cada tipo de datos.

5 Para configurar qué flujo de trabajo se ejecuta antes y después de exportar cada tipo de datos, haga clic en el vínculo Editar de la sección Automatización del exportador. Aparece la página Configuración de automatización del exportador de datos.

Rellene los campos de esta página y pulse Guardar para volver a la página Configuración del exportador de datos. Consulte más información.

6 **Para configurar el daemon de la tarea de exportación, pulse el vínculo Editar que aparece en la sección Configuración de tarea de almacén. Aparece la página Configuración del almacén de exportador de datos.**

Rellene los campos de esta página y pulse Guardar para volver a la página Configuración del exportador de datos. Para obtener más información, consulte "Configuración de la tarea de almacén" en la página 512.

Nota – La exportación es totalmente funcional una vez realizados estos pasos. Cuando la exportación está habilitada, los registros de datos empiezan a incluirse en la cola de exportación. Si no habilita la tarea de exportación, las tablas de la cola se saturarán y se suspenderá la inclusión en la cola. Normalmente resulta más eficaz exportar lotes pequeños (con más frecuencia) que grandes, pero la exportación está condicionada por la disponibilidad del propio almacén, que puede verse restringida por otras causas.

---

7 **Si lo desea, defina el tamaño máximo de la cola. Encontrará más información en "Modificación del objeto de configuración" en la página 514.**

Definición de conexiones de lectura y escritura

Identity Manager utiliza una conexión de escritura durante los ciclos de exportación. Mediante la conexión de lectura indica cuántos registros contiene actualmente el almacén (durante su configuración) y presta servicio a la interfaz de consultas forenses.

Las conexiones de almacén se pueden definir como un origen de datos de servidor de aplicaciones, una conexión JDBC, o una referencia a un recurso de base de datos. Si se define una conexión JDBC o un recurso de base de datos, al exportar los datos se usan pocas conexiones extensivamente durante las operaciones de escritura y después se cierran todas las conexiones. El Exportador de datos sólo utiliza conexiones de lectura durante la configuración del almacén y la ejecución de consultas forenses, conexiones que cierra en cuanto ha finalizado la operación.

El Exportador aplica el mismo esquema a las conexiones de escritura y lectura, lo que permite utilizar la misma información de conexión para ambas. Sin embargo, en caso de conexiones separadas, la implementación puede escribir en un conjunto de tablas de montaje de almacén, transformar dichas tablas en el verdadero almacén y después convertir las tablas del almacén en un subalmacén de datos donde leerá Identity Manager.

Puede editar el formulario de configuración de exportación de datos para impedir que Identity Manager lea el almacén. Este formulario contiene la propiedad `includeWarehouseCount` , que instruye a Identity Manager para que consulte el almacén y muestre el número de registros de cada tipo de datos. Para inhabilitar esta función, copie el formulario de configuración de exportación de datos, cambie el valor de la propiedad `includeWarehouseCount` a `true` e importe su formulario personalizado.

▼ Para definir conexiones de lectura y escritura

1 Pulse el botón Agregar conexión en la página Configuración del exportador de datos.

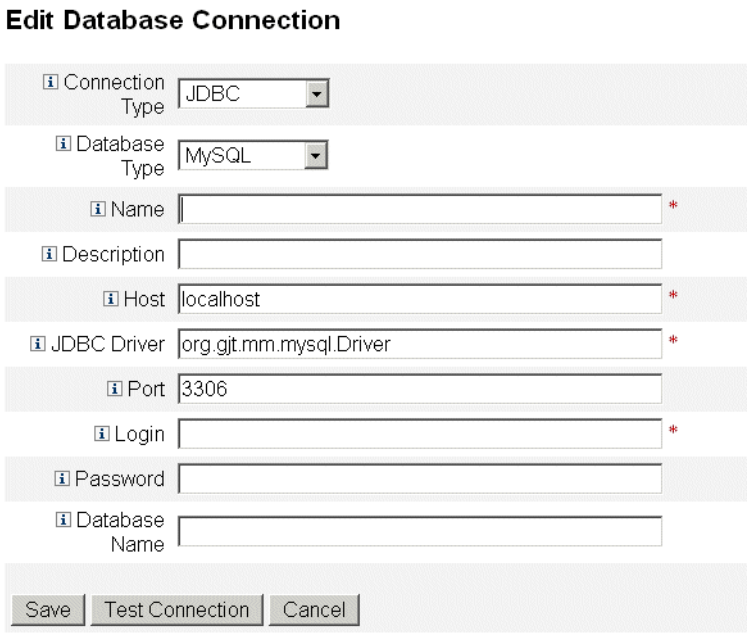


FIGURA 16–2 Configuración del exportador de datos

2 Elija una opción en el menú desplegable Tipo de conexión para indicar cómo debe establecer Identity Manager las conexiones de lectura o escritura con el almacén de datos.

- **JDBC**. Conecta a una base de datos a través de la interfaz de programación de aplicaciones Java Database Connectivity (JDBC). El código de interfaz de almacén proporciona la agrupación de conexiones.
- **Recurso**. Utiliza la información de conexión definida en un recurso. El código de interfaz de almacén proporciona la agrupación de conexiones.
- **Origen de datos**. Utiliza el servidor de aplicaciones subyacente para administrar y agrupar las conexiones. Este tipo de conexión solicita conexiones al servidor de aplicaciones.

  Los campos de la página varían según la opción elegida en el menú desplegable **Tipo de conexión**. La configuración de la conexión a base de datos se explica detalladamente en la ayuda en línea.

3 **Pulsar Guardar para guardar los cambios de configuración y regresar a la página Configuración del exportador de datos.**

Repita este procedimiento si va a utilizar conexiones de lectura y escritura distintas.

Definición de la información de configuración de almacén

Para configurar el almacén, debe seleccionar una conexión de lectura, otra de escritura y una clase de fábrica de código de interfaz de almacén (WIC). La clase de fábrica WIC proporciona la interfaz entre Identity Manager y el almacén. Identity Manager incluye una implementación predeterminada del código, pero puede crear el suyo propio. Para obtener más información sobre la configuración de clases de fábrica personalizadas, consulte el Capítulo 5, "Data Exporter" de *Sun Identity Manager Deployment Guide*.

El archivo `jar` que contiene la clase de fábrica y todos los archivos `jar` auxiliares deben aparecer en el directorio `$WSHOME/exporter` del servidor de Identity Manager donde se ejecuta la tarea de exportación y en cualquier servidor donde se configure el Exportador de datos. Sólo un servidor de Identity Manager puede exportar datos en un momento dado.

▼ Para definir información de configuración de almacén

1 **En la página Configuración del exportador de datos, pulse el vínculo Editar que aparece en la sección Información de configuración de almacén.**

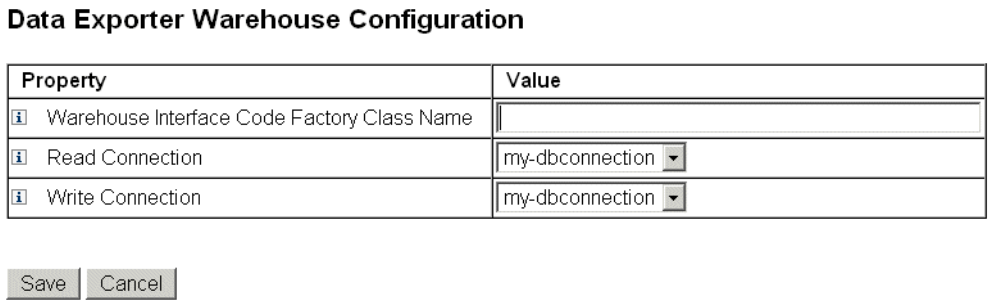


FIGURA 16–3 Configuración del exportador de datos

2 **Especifique un valor en el campo Nombre de clase de fábrica de código de interfaz de almacén. Si el integrador no ha creado una clase personalizada, introduzca el valor** `com.sun.idm.warehouse.base.Factory`**.**

3 **Especifique las conexiones en los menús desplegables Leer conexión y Escribir conexión.**

4 **Pulsar Guardar para guardar los cambios de configuración y regresar a la página Configuración del exportador de datos.**

Configuración de modelos de almacén

Cada tipo de datos exportable tiene un conjunto de opciones que sirven para controlar si ese tipo se exporta y cuándo. La exportación de datos aumenta la carga de los servidores de Identity Manager, por lo que conviene habilitarla únicamente para los tipos de datos que interesen a la empresa.

En la tabla siguiente se describen los distintos tipos de datos exportables.

TABLA 16–1 Tipos de datos admitidos

Tipo de datos	Descripción
`Account`	Un registro que contiene la vinculación entre un usuario y una cuenta de recursos.
`AdminGroup`	Un grupo de permisos de Identity Manager disponibles en todos los grupos de objetos.
`AdminRole`	Los permisos asignados a uno o más grupos de objetos.
AuditPolicy	Una colección de reglas que se evalúan en un objeto de Identity Manager para averiguar si se cumple una directiva de negocio.
`ComplianceViolation`	Un registro que contiene el incumplimiento de una directiva de auditoría por parte de un usuario.
`Entitlement`	Un registro que contiene una lista de autenticaciones para un usuario concreto.
`LogRecord`	Un registro que contiene un único registro de auditoría.
`ObjectGroup`	Un contenedor de seguridad modelado como una organización.
`Resource`	Un sistema/aplicación donde se abastecen cuentas.
`ResourceAccount`	Un conjunto de atributos que forman una cuenta en un determinado recurso.
`Role`	Un contenedor lógico para el acceso.
`Rule`	Un bloque lógico que puede ser ejecutado por Identity Manager.
`TaskInstance`	Un registro que indica un proceso completado o en ejecución.
`User`	Un usuario lógico que incluye cero o más cuentas.
`WorkflowActivity`	Una actividad individual de un flujo de trabajo de Identity Manager.

TABLA 16–1 Tipos de datos admitidos *(Continuación)*

Tipo de datos	Descripción
`WorkItem`	Una acción manual de un flujo de trabajo de Identity Manager.

▼ Para configurar modelos de almacén

1 **Haga clic en un vínculo de tipo de datos dentro de la página Configuración del exportador de datos.**

2 **En la ficha Exportar, indique si se exporta el tipo de datos. Si no desea exportar este tipo de datos, quite la marca de la casilla de verificación Exportar y pulse Guardar. De lo contrario, seleccione las demás opciones que necesite en esta ficha Exportar.**

- **Permitir consulta**. Controla si el modelo se puede consultar.
- **Todo en cola**. Captura todos los cambios que sufren los objetos de este tipo. Si se marca esta opción, puede sobrecargarse considerablemente el proceso del Exportador. Utilícela con moderación.
- **Capturar eliminaciones**. Registra todos los objetos eliminados de este tipo. Si se marca esta opción, puede sobrecargarse considerablemente el proceso del Exportador. Utilícela con moderación.

3 **La ficha Atributos permite seleccionar los atributos que pueden especificarse en una consulta forense y los que pueden aparecer en los resultados de la consulta. No es posible eliminar los atributos predeterminados de la interfaz de administración. Encontrará instrucciones para cambiar los atributos predeterminados en el Capítulo 1, "Working with Attributes" de *Sun Identity Manager Deployment Guide*.**

Los nombres de atributo nuevos deben tener las características siguientes:

- `attrName`: El atributo es de nivel superior y escalar.
- `attrName[]`: Es un atributo de nivel superior valorado con una lista cuyos elementos son escalares.
- `attrName['`*key*`']`: El atributo contiene un valor de asignación, que conviene incluir con la clave especificada.
- `attrName[].` *name2*: Es un atributo de nivel superior valorado con una lista cuyos elementos son estructuras. *name2* es el atributo de la estructura al que se debe acceder.

Nota – Si desea exportar atributos a la tabla `EXT_RESOURCEACCOUNT_ACCTATTR` , debe marcar la casilla Auditar para cada atributo que quiera exportar.

---

4 **Especifique con qué frecuencia se exporta la información asociada al tipo de datos en la ficha Programar. Los ciclos son relativos a la media noche en el servidor. Un ciclo de 20 minutos se produciría a la hora exacta, 20 minutos después y 40 minutos después. Si un intento de exportar**

dura más que el ciclo programado, se omite el ciclo siguiente. Por ejemplo, si se ha definido un ciclo de 20 minutos para que comience a media noche, pero la exportación dura 25 minutos, la próxima exportación empezará a las 12:40. No se producirá la exportación programada inicialmente para las 12:20.

Configuración de la automatización del exportador

Identity Manager permite especificar los flujos de trabajo que se ejecutan antes y después de exportar datos.

El flujo de trabajo de inicio de ciclo puede servir para impedir una exportación si se produce un evento que justifique una cancelación. Por ejemplo, si una aplicación que lee o escribe en las tablas de montaje requiere acceso exclusivo a las tablas al mismo tiempo que una exportación programada, habrá que cancelar dicha exportación. El flujo de trabajo debe devolver el valor 1 para cancelar la exportación. Identity Manager crea un registro de auditoría donde se indica que se ha omitido la exportación y cuáles son los resultados del error. Si el flujo de trabajo devuelve 0 y no se produce ningún error, el tipo de datos se exportará.

El flujo de trabajo de ciclo completo se ejecuta una vez exportados todos los registros. Este flujo de trabajo suele activar otra aplicación para procesar los datos exportados. Una vez completado este flujo de trabajo, el Exportador comprueba si hay otro tipo de datos para exportar.

Encontrará ejemplos de flujo de trabajo en el archivo `$WSHOME/sample/web/exporter.xml` . El subtipo (`subtype`) de un flujo de trabajo del Exportador es `DATA_EXPORT_AUTOMATION`, mientras que el tipo de autorización (`authType`) es `WarehouseConfig`.

▼ Para configurar la automatización del exportador

1. **En la página Configuración del exportador de datos, pulse el vínculo Editar que aparece en la sección Automatización del exportador.**
2. **Si lo desea, en el menú desplegable Flujo de trabajo de inicio de ciclo puede seleccionar un flujo de trabajo para ejecutarlo antes de exportar.**
3. **Si lo desea, en el menú desplegable Flujo de trabajo de inicio de ciclo puede seleccionar un flujo de trabajo para ejecutarlo después de exportar.**

Configuración de la tarea de almacén

No hace falta ejecutar la tarea de exportación en un servidor dedicado, pero quizá le interese si prevé exportar grandes volúmenes de datos. La tarea de exportación transfiere los datos eficazmente desde Identity Manager al almacén y acapara el máximo posible de la CPU durante

la operación de exportación. Si no utiliza un servidor dedicado, le conviene evitar que el servidor controle el tráfico interactivo, ya que el tiempo de respuesta se ralentizará rotundamente durante las exportaciones largas.

▼ Para configurar la información de configuración del almacén

1 **En la página Configuración del exportador de datos, pulse el vínculo Editar que aparece en la sección Configuración de tarea de almacén.**

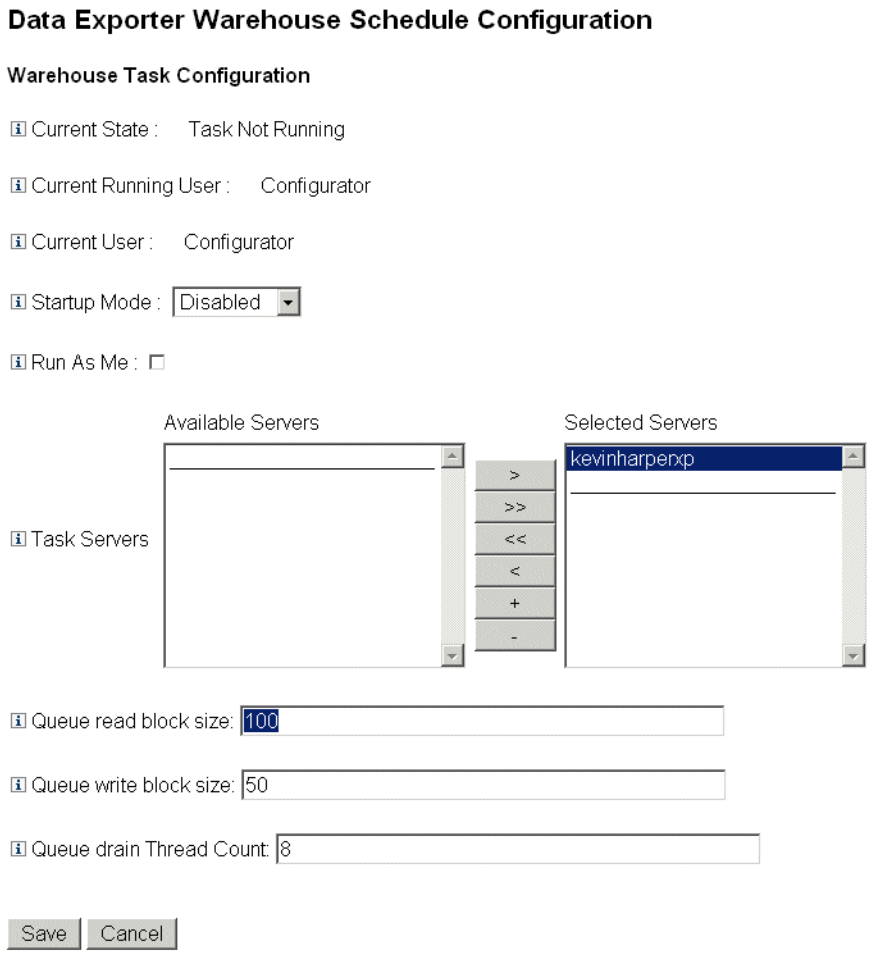


FIGURA 16–4 Configuración de la programación del almacén

2 **Seleccione una opción en el menú desplegable Modo de inicio para indicar qué tarea del almacén comienza automáticamente cuando se inicia Identity Manager. Inhabilitado significa que la tarea se debe comenzar manualmente.**

3 **Marque la casilla Ejecutar como para que la tarea del Exportador se ejecute en su cuenta administrativa.**

4 **Seleccione los servidores donde se puede ejecutar la tarea. Aunque es posible especificar varios servidores, sólo se puede ejecutar una única tarea del almacén a la vez. Si se detiene el servidor donde se ejecuta la tarea, el Programador la reiniciará automáticamente en otro servidor de la lista (si está disponible).**

5 **Especifique el número de registros que se leen de la cola a un búfer de memoria antes de escribir en el campo de tamaño de bloque de lectura de la cola. El valor predeterminado de este campo es adecuado para la mayoría de las exportaciones. Eleve este valor si el servidor del depósito de Identity Manager es más lento que el servidor del almacén.**

6 **Especifique el número de registros que se escriben en el almacén durante una única transacción en el campo de tamaño de bloque de escritura de la cola.**

7 **Indique el número de subprocesos de Identity Manager que se realizan para leer los registros de la cola en el campo Queue drain Thread Count. Eleve este número si la tabla de la cola contiene muchos registros de distintos tipos. Redúzcalo si la tabla de la cola tiene pocos tipos de datos.**

8 **Pulsar Guardar para guardar los cambios de configuración y regresar a la página Configuración del exportador de datos.**

Modificación del objeto de configuración

Cuando el Exportador de datos está configurado y en funcionamiento, todos los tipos de datos que se configuren para la cola se capturarán en la tabla interna de la cola. Esta tabla carece de un límite superior predeterminado, pero es posible configurarlo editando el objeto de configuración `Data Warehouse Configuration`. Este objeto tiene anidado un objeto denominado `warehouseConfig`. Incluya la línea siguiente en el objeto `warehouseConfig`:

```
<Attribute name='maxQueueSize' value='YourValue'/>
```

El valor de `maxQueueSize` puede ser cualquier entero positivo menor que 2^{31}. El Exportador de datos inhabilita la inclusión en la cola cuando se alcanza dicho límite. Los datos generados no se pueden exportar hasta que se ha vaciado la cola.

Durante el funcionamiento normal de Identity Manager se pueden generar varios millares de registros modificados por hora, de manera que la tabla de la cola crecerá vertiginosamente. Como la tabla de la cola se encuentra en el depósito de Identity Manager, este crecimiento

consumirá espacio de tablas en el RDBMS, con el consiguiente riesgo de que se agote dicho espacio. Si el espacio de tablas es limitado, quizá sea necesario restringir la cola.

Para supervisar el tamaño de la tabla de la cola, use Data Queue JMX Mbean. Para obtener más información, consulte "Supervisión del Exportador de datos" en la página 520.

Verificación del Exportador de datos

Una vez configurado correctamente, el Exportador de datos actúa en segundo plano enviando los datos al almacén según los intervalos configurados. Para ejecutar el Exportador cuando le interese, utilice la tarea Iniciador del exportador de almacén de datos.

▼ Para usar el Iniciador del exportador de almacén de datos

1. **Inhabilite la tarea de almacén. Para obtener más información, consulte "Configuración de la tarea de almacén" en la página 512.**
2. **Seleccione Tareas de servidor en el menú principal. A continuación, haga clic en la ficha secundaria Ejecutar tareas. Aparece la página Tareas disponibles.**
3. **Pulse el vínculo Iniciador del exportador de almacén de datos. Aparece la página Iniciar tarea.**
4. **Marque la casilla Opciones de depuración para ver otras opciones.**
5. **Marque la casilla No hacer caso de LastMods iniciales para que el Exportador omita la marca de fecha y hora del último sondeo ("last polled"), con la que determina qué registros del depósito de Identity Manager se han exportado ya. Con esta opción marcada, se exportan todos los registros del depósito de Identity Manager que tienen los tipos seleccionados.**
6. **Elija los tipos de datos que desea exportar en la lista Exportar una vez. Si no especifica ningún tipo de la lista Exportar una vez, la tarea de exportación ejecuta un daemon y exporta basándose en la programación previamente definida. Si elige uno o varios tipos de datos, Identity Manager los exporta de inmediato y cierra la tarea de exportación.**
7. **Defina los valores que le interesen de los demás campos.**
8. **Pulse Ejecutar para iniciar la tarea.**

Configuración de consultas forenses

Las consultas forenses permiten a Identity Manager leer datos que se han incluido en el almacén de datos. Pueden identificar objetos de usuario o de rol basándose en valores actuales o históricos del usuario, del rol, o de tipos de datos relacionados. Una consulta forense es análoga a un informe Buscar usuario o Buscar rol, con la diferencia de que los criterios de coincidencia pueden evaluarse con datos históricos, ya que permite buscar atributos con tipos de datos distintos a los del usuario o rol consultados.

La finalidad de una consulta forense es emprender una acción con los resultados utilizando Identity Manager. La consulta forense no constituye una herramienta de informes genérica.

Una consulta forense puede plantear preguntas como éstas:

- ¿Quién ha tenido acceso al sistema X entre las horas A y B y quién ha aprobado ese acceso?
- ¿Cuántas solicitudes de abastecimiento se han procesado durante las últimas 48 horas y cuánto se ha tardado con cada solicitud?

Los resultados de las consulta forenses no se pueden guardar. Los informes genéricos sobre los datos del almacén deben realizarse con herramientas comerciales de creación de informes.

Creación de consultas

Una consulta forense puede buscar objetos de usuario o de rol. Se pueden efectuar consultas forenses muy complejas, seleccionando una o más condiciones de atributo sobre tipos de datos relacionados. Las consultas forenses sobre usuarios pueden utilizar atributos de búsqueda con los tipos de datos Usuario, Cuenta, Cuenta de recursos, Rol, Derecho y Elemento de trabajo. Las consultas forenses sobre roles pueden utilizar atributos de búsqueda con los tipos de datos Rol, Usuario y Elemento de trabajo.

Dentro de un mismo tipo de datos, todas las condiciones de atributo se unen lógicamente (con el operador Y), de modo que han de cumplirse todas las condiciones para que haya una coincidencia. De manera predeterminada, se aplica el operador Y a las coincidencias se unen lógicamente entre los tipos de datos, pero si marca la casilla Utilizar O, se les aplica el operador O.

El almacén puede contener varios registros para un solo objeto de usuario o rol, y una misma consulta puede devolver múltiples coincidencias para el mismo usuario o rol. Para facilitar la distinción entre estas coincidencias, cada tipo de datos puede restringirse a un rango de fechas, de manera que sólo se consideren coincidencias los registros a partir del rango especificado. Cada tipo de datos relacionados se puede restringir a un rango de fechas, lo que permite realizar consultas del tipo:

```
find all Users with Resource Account on ERP1 between May and July 2005
who were attested by Fred Jones between June and August 2005
```

El rango de fechas va de una medianoche a otra. Por ejemplo, del 3 de mayo de 2007 al 5 de mayo de 2007 hay un rango de 48 horas. Por tanto, no se incluiría ningún registro del 5 de mayo.

Los operandos (valores de comparación) de cada condición de atributo deben especificarse dentro de la definición de la consulta. El esquema restringe algunos atributos a un conjunto limitado de posibles valores, mientras que otros atributos carecen de restricciones. Por ejemplo, la mayoría de los campos de fecha sólo admiten el formato `AAAA-MM-DD HH:mm:ss`.

Nota – Dado el gran volumen potencial de los datos del almacén y la complejidad de la consulta, puede tardarse mucho en obtener resultados. Si sale de la página de consulta mientras se ejecuta una consulta forense, no podrá ver los resultados.

▼ Para crear una consulta forense

1 **En la interfaz de administración, seleccione Cumplimiento en el menú principal.**

Aparece la página Directivas de auditoría (ficha Administrar directivas).

2 **Haga clic en la ficha secundaria Consulta forense.**

Aparece la página Buscar en almacén de datos.

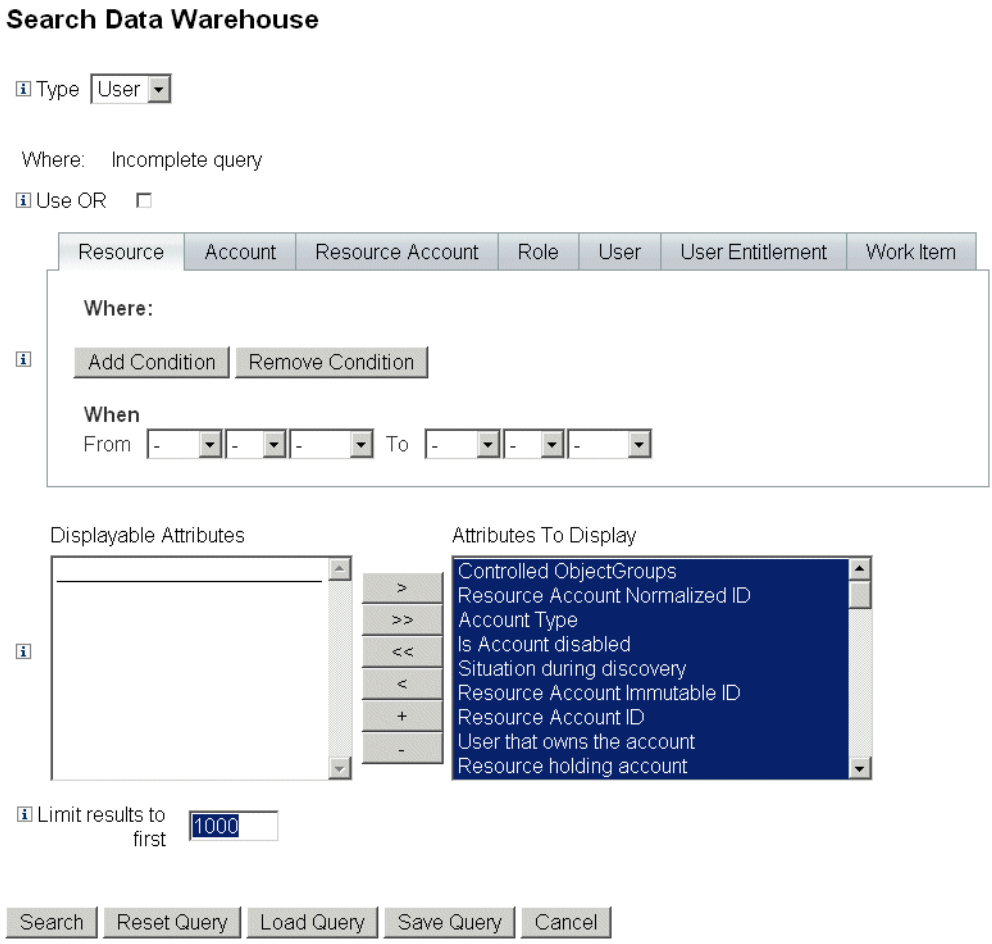


FIGURA 16–5 Buscar en almacén de datos

3 Indique si se deben buscar registros de usuario o de rol en el menú desplegable Tipo.

4 Marque la casilla Utilizar O para que Identity Manager aplique el operador lógico O a los resultados de cada tipo de datos consultado. El sistema aplica el operador lógico Y de manera predeterminada a los resultados.

5 Seleccione una ficha correspondiente a un tipo de datos que vayan a aparecer en la consulta forense.

a. Pulse Agregar condición. Aparece un conjunto de menús desplegables.

b. **Seleccione un operando (condición para verificar) en el menú desplegable de la izquierda y el tipo de comparación en el de la derecha. A continuación, introduzca una cadena o un entero para la búsqueda. La lista de posibles operandos se define en el esquema externo. Todos los operandos se describen en la ayuda en línea.**

c. **Si lo desea, seleccione un rango de fechas para restringir el ámbito de la consulta.**

   Incluya otras condiciones necesarias para el tipo de datos seleccionado. Repita este paso con todos los tipos de datos que deban formar parte de la definición de la consulta forense.

6 **Seleccione los atributos disponibles que desea mostrar en los resultados de la consulta forense.**

7 **Especifique un valor en el campo Limitar resultados al primero. Cuando se emplean condiciones de diversos tipos de datos, el límite se aplica a la subconsulta de cada tipo y el resultado final es la intersección de todas las subconsultas. En consecuencia, el resultado final puede excluir algunos registros debido al límite de una subconsulta.**

8 **Haga clic en Buscar para ejecutar la consulta forense enseguida o Guardar consulta para poder reutilizarla. La reutilización de las consultas forenses se explica en "Cómo guardar una consulta forense" en la página 519.**

Cómo guardar una consulta forense

Después de configurar una consulta y, opcionalmente, ejecutarla para comprobar si produce los resultados deseados, es posible guardarla para ejecutarla en el futuro.

▼ Para guardar una consulta forense

1 **En la página Buscar en almacén de datos, elija Guardar consulta. Aparece la página Guardar consulta forense.**

2 **Indique un nombre y una descripción para la consulta.**

3 **Marque la casilla Guardar valores de condición para guardar los valores de las condiciones (cadenas y enteros) que ha introducido en la página Buscar en almacén de datos. Si no marca esta casilla, la consulta forense guardada servirá como plantilla, con lo cual deberá introducir valores cada vez que ejecute la consulta.**

4 **Cualquier persona puede ejecutar una consulta guardada, pero de forma predeterminada sólo su autor puede modificarla. Para que otros usuarios puedan modificar su consulta, marque la casilla Permitir que otros alteren esta consulta.**

5 **Como la consulta devuelve objetos de usuario o de rol, puede indicar qué atributos de los objetos aparecen en los resultados. Si quiere ver atributos no incluidos en la lista Atributos para mostrar, puede ir a la página Configuración del exportador de datos y agregar nuevos atributos visualizables al tipo de usuario o rol.**

Carga de consultas

Es posible cargar cualquier consulta guardada por cualquier usuario, pero sólo puede alterar las consultas creadas por usted o que otros usuarios hayan marcado como modificables por cualquier persona.

▼ Para cargar una consulta forense

1 **En la página Buscar en almacén de datos, elija Cargar consulta. Aparece la página Cargar consulta forense. La columna Resumen de la consulta indica Consulta incompleta si la consulta se ha guardado como una plantilla.**

2 **Marque la casilla situada a la izquierda de la consulta y haga clic en Cargar consulta.**

Mantenimiento del Exportador de datos

A continuación se explica cómo efectuar un seguimiento del estado del Exportador de datos. Esta información se ha dividido en los temas siguientes:

- "Supervisión del Exportador de datos" en la página 520
- "Supervisión del registro" en la página 521

Supervisión del Exportador de datos

Una vez que el Exportador está configurado y funcionando, tiene la posibilidad de supervisarlo para garantizar su funcionamiento continuo. El Exportador posee diversos beans JMX que sirven para conocer su comportamiento. Los beans JMX incluyen datos estadísticos sobre las velocidades medias de lectura/escritura para el Exportador, el tamaño actual/máximo de la cola de memoria interna y el tamaño de la cola persistente. El Exportador también produce registros de auditoría durante la exportación: uno por cada ciclo de cada tipo de datos. El registro de auditoría incluye el número de registros exportados de ese tipo y la duración de la exportación.

El Exportador de datos cuenta con los siguientes beans de administración JMX que lo supervisan.

TABLA 16–2 Beans de administración JMX

Nombre del bean	Descripción
DataExporter	Contiene el número de exportaciones que hay actualmente en la cola y el límite superior de la cola.
DataQueue	Contiene el número de exportaciones que hay actualmente en caché en la cola y la frecuencia de llegada a la caché.
ExporterTask	Contiene el número de lecturas de exportación (desde Identity Manager), de escrituras de exportación (en el almacén), las velocidades de lectura y escritura (registros/segundo) y el número de errores.

El Exportador de datos se puede configurar para incluir en una tabla de cola los registros de exportación de la cola durante el funcionamiento normal de Identity Manager. Como la cola debe poder ampliarse hasta un gran número de registros y sobrevivir al reiniciar el servidor, una tabla del depósito de Identity Manager actúa como copia de seguridad de la cola. Dado que escribir en el depósito ralentizaría las operaciones normales de Identity Manager, la cola utiliza una pequeña caché de memoria para alojar los registros hasta que puedan permanecer en el depósito.

Los atributos del MBean DataQueue se pueden ajustar para mostrar el máximo número de registros que hay en la cola en memoria (en un único servidor de Identity Manager). En un sistema equilibrado, el número de registros en la caché de memoria debería ser reducido y tender rápidamente a cero. Si observa que este número aumenta (en millares) o no devuelve cero al cabo de unos segundos, conviene que estudie el rendimiento de escritura del depósito.

El MBean ExportTask contiende dos recuentos de errores: uno de lectura y otro de escritura. Estos recuentos deben ser cero, pero pueden producirse errores por muy diversos motivos, sobre todo durante la escritura. El error de escritura más frecuente se debe a que los datos exportados no caben en las columnas de la tabla de almacén, normalmente por desbordamiento de cadena. Algunos datos de cadena exportados carecen de límites, mientras que las columnas de la tabla requieren un límite superior.

Supervisión del registro

Identity Manager tiene dos conjuntos de objetos que crecen sin límites: el registro de auditoría y el registro del sistema. El Exportador de datos solucionar algunos problemas de mantenimiento relacionados con las tablas de registro.

Registros de auditoría

Identity Manager escribe registros de auditoría inmutables en el archivo de registro de auditoría para llevar un seguimiento histórico de las operaciones que realiza. Identity Manager utiliza estos registros en determinados informes y los datos de dichos registros pueden verse en la

interfaz de administración. Sin embargo, como el registro de auditoría crece ilimitadamente y a una velocidad moderada, el implementador debe establecer cuándo se trunca el registro de auditoría. Con anterioridad al Exportador de datos, si se quería preservar los registros antes de truncar, no había más remedio que volcar las tablas desde el depósito. Si el Exportador de datos está habilitado y configurado para exportar registros del registro, los antiguos registros se conservan en el almacén y Identity Manager puede truncar las tablas de auditoría en la medida necesaria.

Registros del sistema

Los registros del sistema poseen la misma propiedad inmutable que los registros de auditoría, pero no suelen generarse con tanta frecuencia. El Exportador de datos no exporta los registros del sistema. Para truncar el registro del sistema y preservar los antiguos registros, debe volcar las tablas en el depósito.

◆ ◆ ◆ CAPÍTULO 17

Administración de Service Provider

En este capítulo se proporciona la información necesaria para administrar Service Provider en Sun Identity Manager. Para utilizar esta información resulta útil conocer los directorios LDAP (Protocolo de acceso a directorios ligeros) y la administración de federación. Para obtener una explicación más extensa de la implementación de Sun Identity Manager Service Provider (Service Provider), consulte *Sun Identity Manager Service Provider 8.1 Deployment*.

Este capítulo contiene los temas siguientes:

Descripción de las funciones de Service Provider

En un entorno de proveedor de servicios es necesario ser capaz de administrar el aprovisionamiento de todos los usuarios finales, incluidos los usuarios de las extranet y las intranet. Las funciones de Service Provider permiten a los administradores de la organización clasificar las cuentas de identidad en dos categorías distintas: usuarios de Identity Manager y usuarios de Service Provider. En Identity Manager, los usuarios de Service Provider están incluidos en cuentas de usuario configuradas como usuario de Service Provider.

Las capacidades de aprovisionamiento de usuario y auditoría de Identity Manager se extienden a las implementaciones del proveedor de servicios para ofrecer las siguientes funciones:

Páginas de usuario final mejoradas

Se proporcionan páginas de usuario final mejoradas que se pueden personalizar en función de la implementación de Service Provider.

Directiva de contraseña e ID de cuenta

Puede definir las directivas de ID de cuenta y contraseña que se aplicarán a los usuarios y las cuentas de recursos de Service Provider, así como a otros usuarios de Identity Manager.

Se activa el código de comprobación de directivas correspondiente a los usuarios que tienen la directiva de cuentas del sistema Service Provider, que se ha añadido a la tabla principal de directivas.

Sincronización de Identity Manager y Service Provider

La sincronización de las cuentas de Identity Manager y Service Provider se puede configurar para que se ejecute en cualquier servidor Identity Manager o en los servidores seleccionados solamente.

Al igual que ocurre con Identity Manager, la sincronización de Service Provider se puede detener y reiniciar fácilmente con las opciones Acciones de recurso de la página Recursos. Consulte "Iniciar y detener la sincronización" en la página 563.

Los formularios de entrada para sincronización de usuarios de Identity Manager y Service Provider son distintos. Consulte "Interfaz de usuario final" en la página 559.

Integración de Access Manager

Puede utilizar Sun Access Manager 7 2005Q4 para realizar la autenticación en las páginas de usuario final de Service Provider. Si se configura la integración con Access Manager, esta aplicación garantiza el acceso de los usuarios autenticados a las páginas de usuario final.

Service Provider necesita que se introduzca el nombre de usuario para efectuar la auditoría. Actualice el archivo `AMAgent.properties` para agregar el ID de usuario a los encabezados HTTP; por ejemplo:

```
com.sun.identity.agents.config.response.attribute.mapping[uid] = HEADER_speuid
```

El filtro de autenticación de las páginas de usuario final incluye el valor del encabezado HTTP en la sesión HTTP, donde debe estar el resto del código.

Configuración inicial

Si quiere configurar las funciones de Service Provider, lleve a cabo los siguientes procedimientos para editar los objetos de configuración de Identity Manager en el servidor de directorio.

- Editar configuración principal
- Editar la configuración de búsqueda de usuarios

Nota –

Antes de continuar, asegúrese de que tiene lo siguiente:

- Recurso LDAP definido. El recurso de ejemplo Directorio de usuario final de Service Provider se importa de forma predeterminada. Puede configurar varios recursos si la información de usuario y configuración se va a almacenar en directorios diferentes.
- El esquema debe incluir la asignación para un objeto XML.

  Si quiere, puede configurar la directiva de cuentas de Service Provider.
- El contexto base configurado para el recurso del directorio sólo se aplica a los usuarios almacenados en el directorio.

Editar configuración principal

▼ Para editar objetos de configuración de una implementación Service Provider

1 En la interfaz del administrador, haga clic en la opción Service Provider del menú.

2 Haga clic en Editar configuración principal.

Se abre la página de configuración de Service Provider.

3 Rellene el formulario de configuración de Service Provider.

Utilice las instrucciones que se proporcionan en las secciones siguientes:

- “Configuración de directorio” en la página 526
- “Formularios de usuario y directiva” en la página 529
- “Base de datos de transacciones” en la página 530
- “Configuración de eventos objeto de seguimiento” en la página 531
- “Índices de cuenta de sincronización” en la página 532
- “Configuración de llamadas” en la página 534

Configuración de directorio

En la sección Configuración de directorio, introduzca información para configurar el directorio LDAP y especifique los atributos de Identity Manager correspondientes a los usuarios del proveedor de servicios.

En la Figura 17–1 se muestra esta sección de la página de configuración de Service Provider, así como la sección de formularios de usuario y directiva que se explica en la sección siguiente.

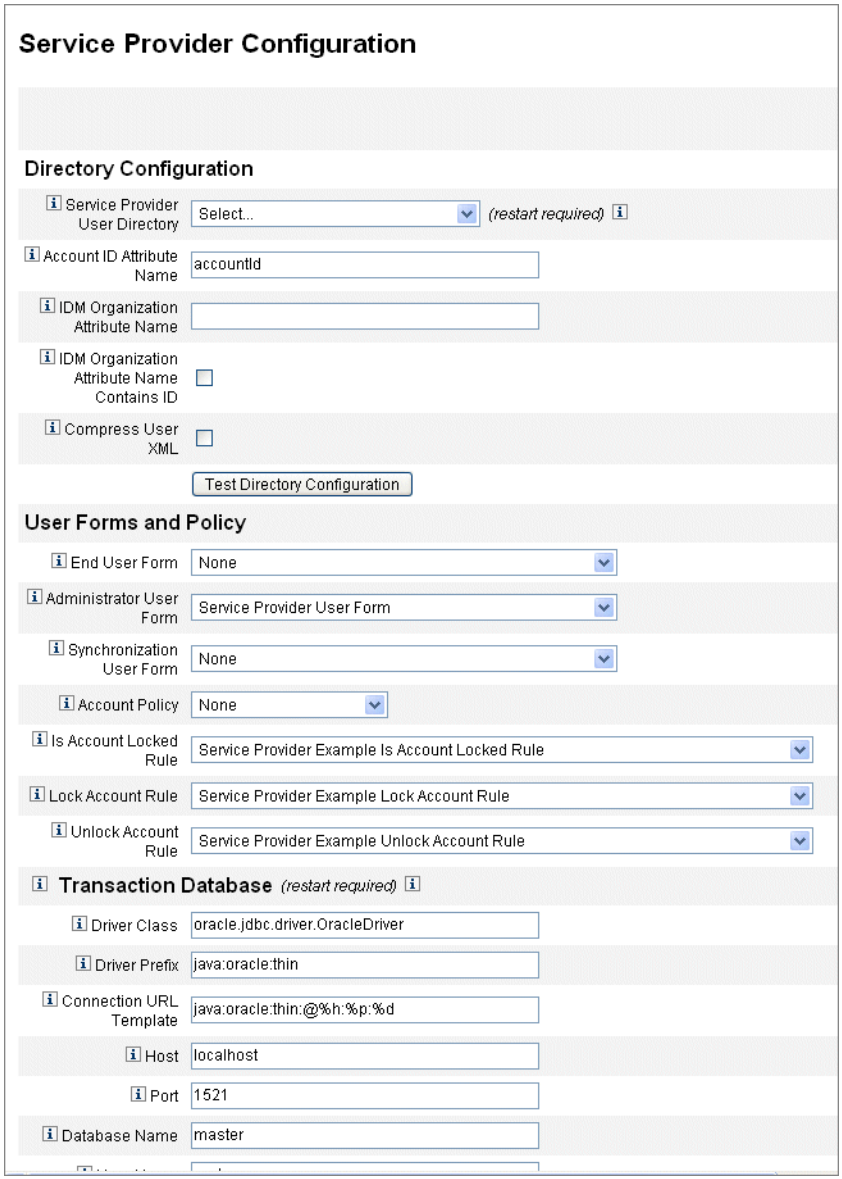


FIGURA 17–1 Configuración de Service Provider (directorio, formularios de usuario y directiva)

▼ Para rellenar el formulario de configuración del directorio

1 **Seleccione el directorio de usuario final de Service Provider en la lista.**

Seleccione el recurso del directorio LDAP en el que están almacenados los datos de todos los usuarios de Service Provider.

2 **Introduzca el nombre del atributo de ID de cuenta.**

Se trata del nombre del atributo de la cuenta LDAP, que contiene un identificador corto único para la cuenta. Se considera el nombre del usuario para la autenticación y el acceso de la cuenta a través de la API. El nombre del atributo debe definirse en el mapa del esquema.

3 **Especifique el nombre del atributo de la organización IDM.**

Se trata del nombre del atributo de la cuenta LDAP que contiene el nombre o ID de una organización dentro de Identity Manager al que pertenece la cuenta LDAP. Se usa para la administración delegada de cuentas de LDAP. El nombre de atributo debe definirse en el mapa de esquema de recurso LDAP y es el nombre de atributo del sistema Identity Manager (el nombre a la izquierda del mapa de esquema).

Nota – Especifique el nombre del atributo de la organización de Identity Manager (y El nombre del atributo de la organización IDM contiene el ID, en caso necesario) si quiere activar la administración delegada por medio de la autorización de la organización.

---

4 **Si decide seleccionar El nombre del atributo de la organización IDM contiene el ID, active esta opción.**

Seleccione esta opción si el atributo del recurso LDAP que hace referencia a la organización de Identity Manager al que pertenece la cuenta de LDAP contiene el ID de la organización de Identity Manager, en lugar de su nombre.

5 **Si decide seleccionar Comprimir XML de usuario, active esta opción.**

Seleccione esta opción para comprimir el XML de usuario almacenado en el directorio.

6 **Haga clic en Configuración de directorio de prueba para verificar los valores introducidos en la configuración.**

Nota – Puede comprobar que la configuración de directorio, transacción y auditoría se adecua a sus necesidades. Para probar completamente las tres configuraciones, haga clic en los botones de prueba.

Formularios de usuario y directiva

En la sección de formularios de usuario y directiva, mostrada en la Figura 17–1 anterior, especifique los formularios y las directivas que se van a utilizar en la administración de usuarios del proveedor de servicios.

▼ Para especificar formularios y directivas para la administración de usuarios de Service Provider

1. **Seleccione Formulario del usuario final en la lista.**

   Este formulario se usa en cualquier lugar, excepto en las páginas del administrador delegado y durante la sincronización. Si se selecciona Ninguno, no se usará ningún formulario predeterminado de usuario.

2. **Seleccione Formulario del usuario administrador en la lista.**

   Se trata del formulario de usuario predeterminado que se utiliza en los contextos de administrador. Se incluyen las páginas de edición de cuentas de Service Provider. Si se selecciona Ninguno, no se usará ningún formulario predeterminado de usuario.

   Nota – Si no selecciona un formulario de usuario del administrador, los administradores no podrán crear ni editar los usuarios de Service Provider Edition en Identity Manager

3. **Seleccione un Formulario de usuario de sincronización de la lista.**

   Este es el formulario predeterminado que se utiliza cuando no se especifica ninguno para un recurso donde se ejecuta sincronización de Service Provider. Si se especifica un formulario de entrada en una directiva de sincronización de un recurso, se utilizará dicho formulario. Los recursos suelen requerir distintos formularios de entrada para la sincronización. En tal caso, deberá definir el formulario de usuario de sincronización para cada recurso, en vez de seleccionar un formulario de la lista.

4. **Seleccione una Directiva de cuentas de la lista.**

   En las opciones se incluyen las directivas de cuentas de identidad definidas mediante Configurar > Directivas.

5. **Seleccione Es una regla de cuenta bloqueada en la lista.**

   Seleccione una regla para ejecutarla en la vista de usuario de Service Provider que permita determinar si una cuenta está bloqueada.

6. **Seleccione una Regla de bloqueo de cuenta.**

   Seleccione una regla para ejecutarla en la vista de usuario de Service Provider que permita definir atributos en la vista que hagan que la cuenta se bloquee.

7 Seleccione una Regla de desbloqueo de cuenta.

Seleccione una regla para ejecutarla en la vista de usuario de Service Provider que permita definir atributos en la vista que hagan que la cuenta se desbloquee.

Base de datos de transacciones

Esta sección de la página de configuración de Service Provider, que se muestra en la Figura 17–2, se utiliza para configurar una base de datos de transacciones. Estas opciones sólo son necesarias cuando se utiliza el almacén persistente de transacciones JDBC. Si cambia cualquiera de estos valores, debe reiniciar el servidor para que se apliquen los cambios.

La tabla de base de datos correspondiente a las transacciones se tiene que configurar con arreglo al esquema mostrado en las secuencias de comandos DDL `create_spe_tables` (situadas en el directorio de `ejemplo` de la instalación de Identity Manager). Quizá haya que personalizar la secuencia de comandos adecuada para el entorno de destino.

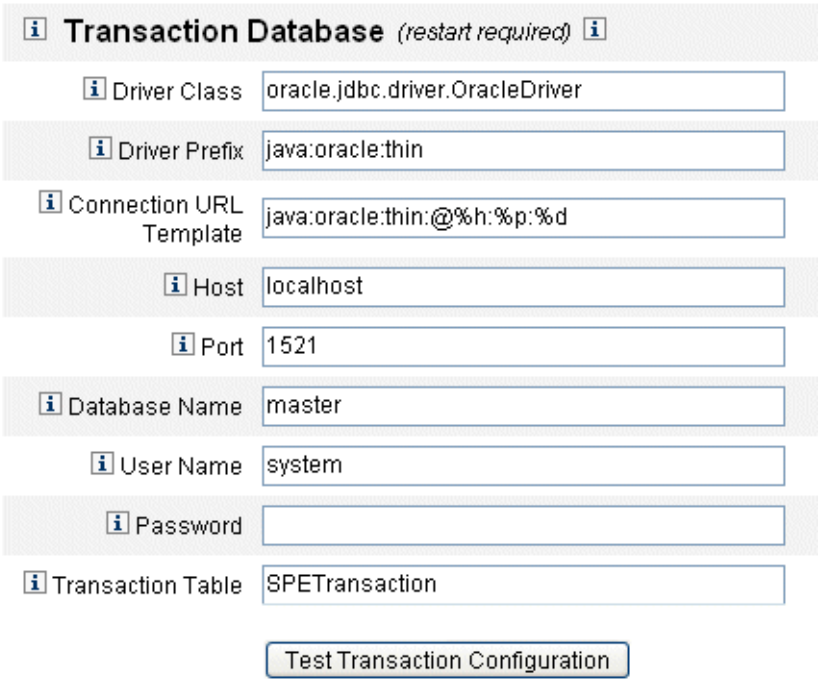


FIGURA 17–2 Configuración de Service Provider (base de datos de transacciones)

▼ Para configurar una base de datos de transacciones

1 **Indique la siguiente información de la base de datos:**

- **Clase del controlador**. Especifique el nombre de la clase del controlador JDBC.
- **Prefijo del controlador**. Este campo es opcional. Si se especifica, se consultará al administrador de controladores JDBC antes de registrar un nuevo controlador.
- **Plantilla URL de conexión**. Este campo es opcional. Si se especifica, se consultará al administrador de controladores JDBC antes de registrar un nuevo controlador.
- **Host**. Introduzca el nombre de host en el que se está ejecutando la base de datos.
- **Puerto**. Introduzca el número de puerto al que está conectado el servidor de base de datos.
- **Nombre de la base de datos**. Introduzca el nombre de la base de datos que se utilizará.
- **Nombre de usuario**. Introduzca el ID de un usuario de base de datos con permiso para leer, actualizar y eliminar filas de las tablas de transacciones y auditoría de la base de datos seleccionada.
- **Contraseña**. Introduzca la contraseña del usuario de base de datos.
- **Tabla de transacciones**. Introduzca el nombre de la tabla de la base de datos seleccionada que se utilizará para almacenar las transacciones pendientes.

2 **Si es preciso, haga clic en Configuración de transacción de prueba para verificar la información introducida.**

Continúe con la sección siguiente de la página de configuración de Service Provider para configurar eventos objeto de seguimiento.

Configuración de eventos objeto de seguimiento

Si la recopilación de eventos está activada, permite realizar un seguimiento de las estadísticas en tiempo real; por consiguiente, ayuda a mantener los niveles de servicio previstos o acordados. La recopilación de eventos está activada de forma predeterminada, como se muestra en la Figura 17–3. La recopilación se desactiva cuando se quita la marca de selección de la casilla Habilitar colección de eventos.

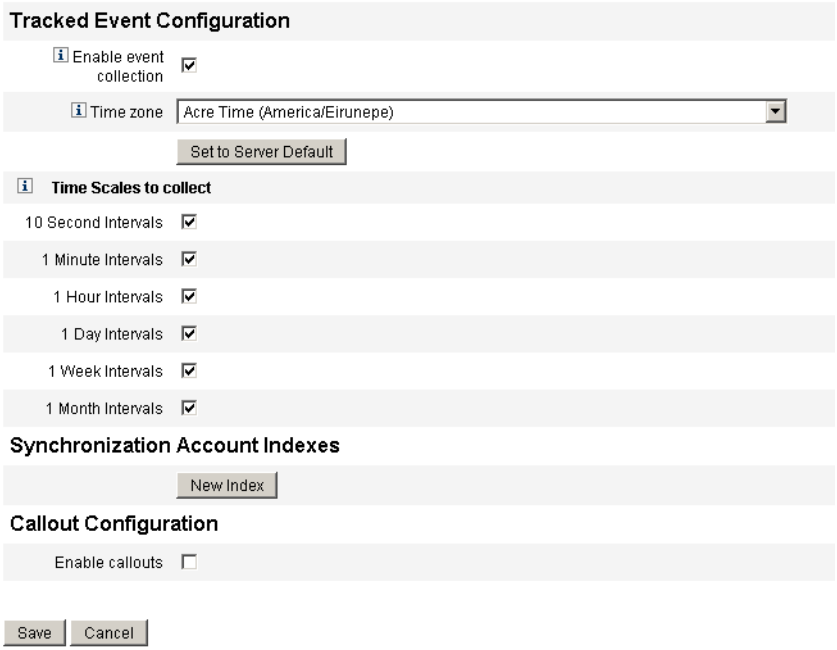


FIGURA 17–3 Configuración de Service Provider (configuración de eventos objeto de seguimiento, índices de cuenta y llamadas)

▼ Para especificar una zona horaria e intervalos de recopilación de eventos objeto de seguimiento de Service Provider

1 Seleccione la zona horaria en la lista.

Seleccione la zona horaria para utilizarla al registrar eventos, o Definido en la configuración predeterminada del servidor para usar la zona horaria definida en el servidor.

2 Seleccione las opciones de Escalas de tiempo para recopilación.

La recopilación tiene lugar en los siguientes intervalos de tiempo: cada 10 segundos, cada minuto, cada hora, a diario, semanal o mensualmente. Desactive los intervalos de tiempo en los que no quiere que se recopilen eventos.

Índices de cuenta de sincronización

Cuando se sincronizan recursos en una implementación de Service Provider, puede que sea preciso definir índices de cuenta para correlacionar correctamente los eventos enviados por el recurso a los usuarios incluidos en el directorio de Service Provider.

De forma predeterminada, los eventos de los recursos deben contener un atributo de ID de cuenta (accountId) cuyo valor coincida con el mismo atributo del directorio. En algunos recursos no se envía este atributo de forma coherente. Por ejemplo, la eliminación de eventos de ActiveDirectory sólo contiene la GUID de cuenta generada en ActiveDirectory.

Los recursos que no incluyen el atributo de ID de cuenta (accountId) deben contener el valor de cualquiera de los atributos siguientes.

- **guid**. Este atributo suele contener un identificador único generado por el sistema.
- **identidad**. Este atributo suele coincidir con el atributo de ID de cuenta (accountId) de todos los recursos, excepto los recursos LDAP, en los que la identidad será el DN completo.

Si necesita establecer la correlación mediante el uso de guid o identidad, debe definir un índice de cuenta para esos atributos. El índice es la serie formada por uno o varios atributos de usuario de directorio que pueden utilizarse para almacenar identidades específicas de recursos. Una vez que las identidades se almacenan en el directorio, se pueden utilizar en filtros de búsqueda para correlacionar los eventos de sincronización.

Para definir índices de cuenta, primero determine los recursos que se utilizarán en la sincronización y cuáles de ellos necesitan un índice. Luego edite la definición de los recursos del directorio de Service Provider y agregue atributos al mapa de esquema de la GUID o atributos de identidad para cada recurso de Active Sync. Por ejemplo, si realiza la sincronización desde ActiveDirectory, puede definir un atributo denominado AD-GUID asignado a un atributo de directorio no utilizado, como un gestor.

▼ Para definir atributos de índice para un recurso

Después de definir todos los atributos de índice en el recurso de Service Provider, lleve a cabo los pasos siguientes:

1. **En la sección Índices de cuenta de sincronización de la página de configuración, haga clic en el botón Nuevo índice.**

   El formulario se amplía para abarcar un campo de selección de recursos, seguido de dos campos de selección de atributos. Los campos de selección de atributos permanecen vacíos hasta que se selecciona un recurso.

2. **Seleccione un recurso de la lista.**

   Los campos de atributos presentan ahora los valores definidos en el mapa de esquema del recurso seleccionado.

3. **Seleccione el atributo de índice adecuado para el atributo Guid o el atributo de identidad completa.**

   Por lo general no es necesario definir ambos. Cuando se definen los dos, el programa intenta establecer la correlación utilizando la GUID en primer lugar, y luego la identidad completa.

4 **Para definir atributos de índice de otros recursos, puede hacer clic en Nuevo índice otra vez.**

5 **Para eliminar un índice, haga clic en el botón Eliminar situado a la derecha del campo de selección de recursos.**

Al eliminar un índice sólo se quita de la configuración; no se modifican los usuarios del directorio existente que puedan tener valores almacenados en los atributos de índice.

Nota – Al eliminar un índice sólo se quita de la configuración; no se modifican los usuarios del directorio existente que puedan tener valores almacenados en los atributos de índice.

Configuración de llamadas

Seleccione esta opción en la sección Configuración de llamadas para activar las llamadas. Cuando están activadas, aparecen las asignaciones de llamadas, que permiten seleccionar las llamadas anteriores y posteriores a la operación de cada tipo de transacción de la lista.

Las opciones de llamadas anteriores y posteriores a la operación se configuran en Ninguno de forma predeterminada.

Cuando seleccione las llamadas posteriores a la operación, utilice la opción Esperar a la llamada posterior a la operación para especificar la espera de la transacción hasta que se haya completado el procesamiento de la llamada posterior a la operación. De esta forma se garantiza que las transacciones dependientes se ejecuten sólo una vez completada correctamente la llamada posterior a la operación.

Nota – Después de seleccionar opciones en todas las secciones de la página de configuración de Service Provider, haga clic en Guardar para completar la configuración.

Editar la configuración de búsqueda de usuarios

La página que se muestra en la Figura 17–4 permite configurar los valores predeterminados de las búsquedas que realicen los administradores delegados en la página Administrar los usuarios de Service Provider. Aunque estos valores predeterminados se aplican a todos los usuarios de la página Administrar los usuarios de Service Provider, pueden anularse por sesión.

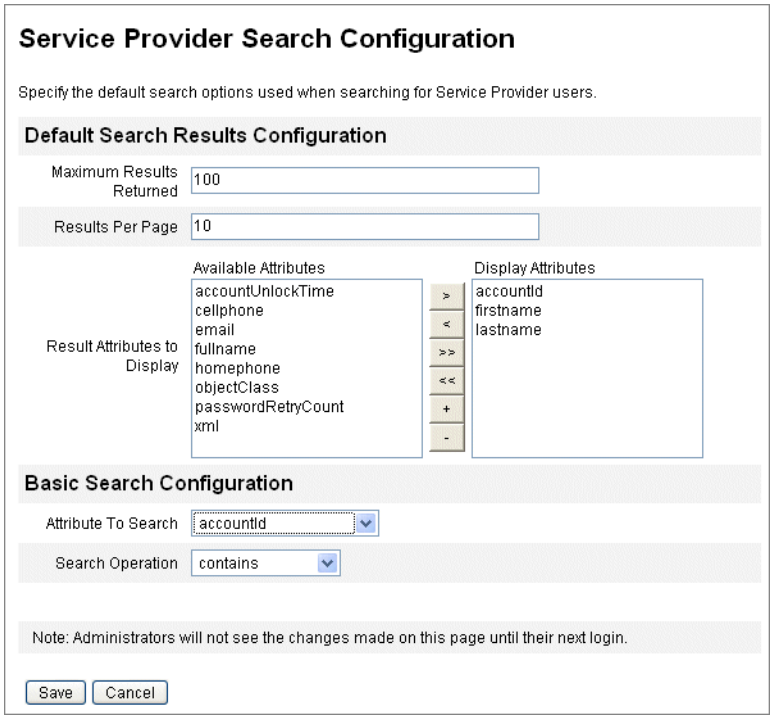


FIGURA 17–4 Configuración de búsqueda

▼ Para configurar los valores predeterminados de búsqueda de usuarios de Service Provider

1. **Haga clic en Service Provider en la barra de menús.**
2. **Haga clic en Editar configuración de búsquedas de usuario.**
3. **Introduzca un valor en Número máximo de resultados (valor predeterminado 100).**
4. **Introduzca un valor en Resultados por página (valor predeterminado 10).**
5. **Utilice las teclas de flecha para seleccionar la opción Atributos disponibles, que está situada junto a Atributos de resultado para mostrar.**
6. **Seleccione el Atributo para buscar en la lista.**
7. **Seleccione la Operación de búsqueda en la lista.**

8 **Haga clic en Guardar.**

Nota – los cambios realizados en la configuración de búsqueda no se aplicarán hasta que cierre la sesión y vuelva a iniciarla.

Estos objetos de configuración no están disponibles si el directorio de Service Provider no está configurado.

Administración de transacciones

Una transacción encapsula una única operación de configuración como, por ejemplo, la creación de un nuevo usuario o la asignación de nuevos recursos. Para asegurarse de que estas transacciones se completan cuando los recursos no están disponibles, se escriben en el almacén persistente de transacciones.

En los temas siguientes de esta sección se incluyen los procedimientos para administrar las transacciones del proveedor de servicios:

Configuración de las opciones predeterminadas de ejecución de la transacción

Estas opciones controlan el modo de ejecución de las transacciones, incluido el procesamiento síncrono o asíncrono y cuándo se mantienen en el almacén persistente de transacciones. Pueden sustituirse en la vista IDMXUser o a través de la forma empleada para el proceso. Para obtener más información, consulte *Sun Identity Manager Service Provider 8.1 Deployment*.

▼ Para configurar transacciones de Service Provider

1 **Haga clic en Service Provider → Editar configuración de transacciones.**

Aparece la página de configuración de transacciones de Service Provider.

En la Figura 17–5 se muestra la sección Opciones predeterminadas de ejecución de la transacción.

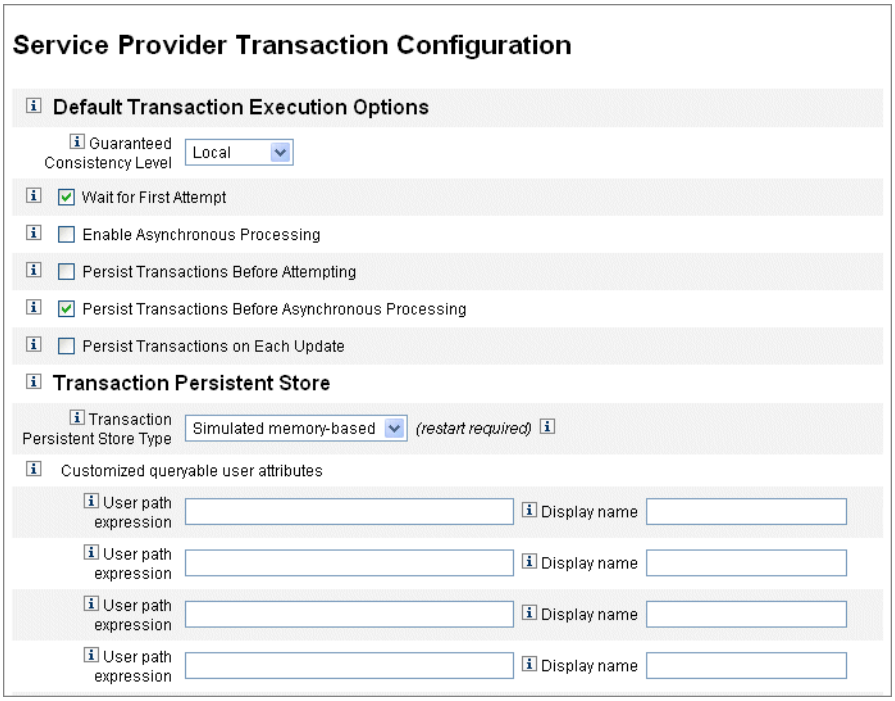


FIGURA 17–5 Configuración de transacciones

2 **Seleccione opciones adecuadas en Nivel de coherencia garantizada para especificar el nivel de coherencia de transacción de las actualizaciones de usuario.**

Las opciones incluyen:

- **Ninguno**. No se garantiza el ordenamiento de actualizaciones de recursos para un usuario.
- **Local**. Se garantiza que las actualizaciones de los recursos de un usuario que se está procesando en el mismo servidor estén en orden.
- **Completa**. Se garantiza el ordenamiento de todas las actualizaciones de recursos para un usuario en todos los servidores. Para ello, es necesario que todas las transacciones se mantengan antes de intentar la transacción o antes del procesamiento asíncrono.

3 **Active las opciones predeterminadas de ejecución de la transacción conforme necesite.**

Las opciones incluyen:

- **Espere al primer intento**. Determina el modo en el que el control regresa al llamador cuando se comprueba un objeto de vista IDMXUser. Si la opción está activada, la operación de comprobación se bloqueará hasta que la transacción de configuración haya realizado un único intento. Si se desactiva un proceso asíncrono, la transacción puede tener éxito o no cuando se devuelve el control. Si el procesamiento asíncrono está activo, se seguirá intentando la transacción en segundo plano. Si se desactiva la opción, la operación de comprobación devolverá el control al llamante antes de intentar la transacción de configuración. Plantéese activar esta opción.
- **Habilitar procesamiento así-ncrono**. Controla si el procesamiento de las transacciones de configuración continúa después de la devolución de la llamada de comprobación.

  La habilitación del procesamiento asíncrono permite que el sistema reintente las transacciones. También mejora el resultado porque permite que se ejecuten de forma asíncrona los subprocesos de trabajo configurados en "Establecer la configuración avanzada de procesamiento de transacciones" en la página 540. Si selecciona esta opción, utilice los formularios de entrada para sincronización para configurar los intervalos de reintento y los intentos de aprovisionamiento o actualización de recursos.

  Cuando seleccione Habilitar procesamiento así-ncrono, introduzca un valor en Tiempo de espera de reintento. Dicho valor establece el límite de tiempo máximo en milisegundos que el servidor intentará completar una transacción de configuración fallida. Esta configuración complementa los parámetros de reintento de los recursos individuales, incluido el directorio LDAP de usuarios de Service Provider. Por ejemplo, si se llega a este límite antes de que se alcancen los límites de reintentos del recurso, se anulará la transacción. Si el valor es negativo, sólo se limita el número de reintentos por los parámetros de los recursos individuales.
- **Mantener las transacciones antes de intentarlo**. Si se activa, las transacciones de configuración se escriben en el almacén persistente de transacciones antes de intentar ejecutarlas. Al activar esta opción puede producirse una sobrecarga innecesaria, ya que la mayorí-a de las transacciones de configuración se realizarán correctamente al primer intento. Plantéese desactivar esta opción, a menos que la opción Espere al primer intento se encuentre desactivada. Esta opción no está disponible cuando se selecciona el nivel de coherencia Completa.
- **Mantener las transacciones antes del procesamiento asíncrono**(*opción predeterminada*). Si se activa, las transacciones de configuración se escriben en el almacén persistente de transacciones antes de procesarlas de forma asíncrona. Si se ha activado la opción Espere al primer intento, se mantendrán las transacciones que deben reintentarse antes de que el control se devuelva al llamador. Si, por el contrario, se ha desactivado esta opción, se mantendrán siempre las transacciones antes de intentar ejecutarlas. Se recomienda la habilitación de esta opción. Esta opción no está disponible cuando se selecciona el nivel de coherencia Completa.

- **Mantener las transacciones en cada actualización** Si se activa esta opción, se mantendrán las transacciones de configuración después de cada intento de reintento. Esto puede ayudar a identificar los problemas, ya que el almacén persistente de transacciones, en el que pueden realizarse búsquedas desde la página de búsqueda de transacciones, está siempre actualizado.

Configuración del almacén persistente de transacciones

Las opciones de la página de configuración de transacciones de Service Provider hacen referencia al almacén persistente de transacciones. Puede configurarse el tipo de almacén, así como los atributos adicionales que permiten consulta y que aparecerán en el almacén, como se muestra en la figura siguiente.

FIGURA 17–6 Configuración del almacén persistente de transacciones de Service Provider

▼ Para definir las opciones de la página de configuración de transacciones de Service Provider

1 Seleccione el Tipo de almacén persistente de transacciones de la lista que desee.

Si se selecciona la opción Base de datos, el RDBMS establecido en la página de configuración principal de Service Provider se utilizará para el mantenimiento de las transacciones de configuración. De este modo, se garantiza que las transacciones que deben reintentarse no se pierdan con el reinicio de un servidor. Para seleccionar esta opción, se necesita la configuración del RDBMS en la página de configuración principal de Service Provider. Si se selecciona la opción Basado en memoria simulada, las transacciones que deben reintentarse se almacenarán en la memoria solamente, y se perderán al reiniciar el servidor. Active la opción Base de datos para los entornos de producción.

Nota – No es conveniente utilizar el almacén persistente de transacciones basado en la memoria en entornos de clúster.

Cuando cambie el Tipo de almacén persistente de transacciones, tendrá que reiniciar todas las instancias de Identity Manager en ejecución para que se aplique el cambio.

2 **Si lo desea, introduzca los atributos de usuario personalizados y que permiten consulta.**

Seleccione los atributos adicionales del objeto IDMXUser para mostrarlos en los resúmenes de las transacciones. Estos atributos permiten consultas desde la página de transacción de búsqueda y se muestran en los resultados de la búsqueda.

Los atributos incluyen:

- **Expresión de la ruta del usuario**. Introduzca una expresión de ruta en el objeto IDMXUser.
- **Nombre exhibido**. Seleccione el nombre de visualización correspondiente a la expresión de ruta. El nombre que se muestra aparece en la página de búsqueda de la transacción.

Establecer la configuración avanzada de procesamiento de transacciones

Estas opciones avanzadas controlan el funcionamiento interno del administrador de transacciones. No cambie la configuración predeterminada, a menos que un análisis de rendimiento indique que no es óptima. Todas las entradas son obligatorias.

En la Figura 17–5 se muestra la sección Configuración avanzada de procesamiento de transacciones de la página Editar configuración de transacciones.

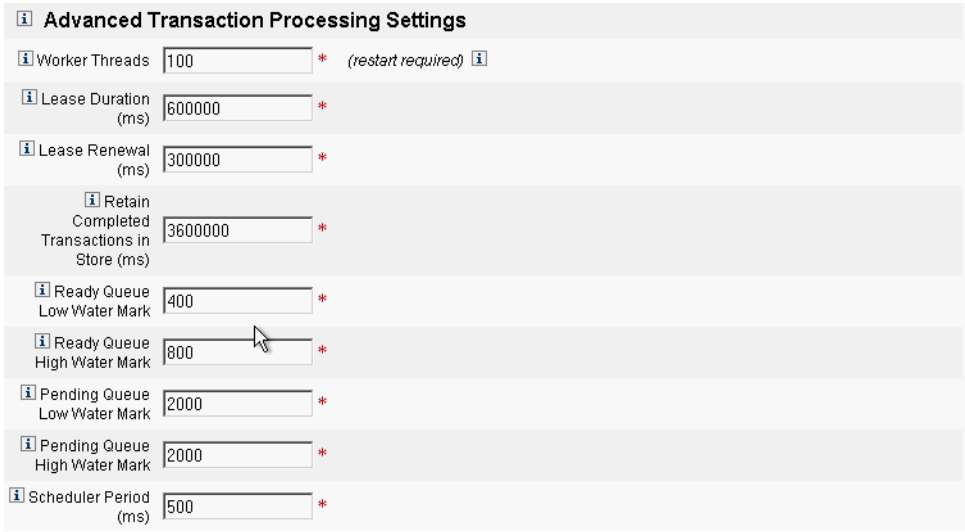


FIGURA 17–7 Configuración avanzada de procesamiento de transacciones

▼ Para especificar la configuración avanzada de procesamiento de transacciones

1 **Introduzca el número de subprocesos de trabajo que desee (valor predeterminado 100).**

Se trata del número de subprocesos utilizado para el procesamiento de las transacciones. Este valor limita el número de transacciones que pueden procesarse simultáneamente. Estos subprocesos se asignan de forma estática al inicio.

Nota – Cuando cambia la configuración de subprocesos de trabajo, tendrá que reiniciar todas las instancias de Identity Manager que se estén ejecutando para que se aplique el cambio.

---

2 **Introduzca la Duración de la concesión (ms) que desee (valor predeterminado 600000).**

Esta opción controla durante cuánto tiempo un servidor debe bloquear una transacción que se está reintentando. La concesión puede renovarse como sea pertinente. Sin embargo, si el servidor no se cierra de forma correcta, ningún otro servidor podrá bloquear la transacción hasta que caduque la concesión del servidor original. La duración mínima debe ser de un minuto. Si establece un valor menor, puede repercutir sobre la carga del almacén persistente de transacciones.

3 **Introduzca la Renovación de la concesión (ms) que desee (valor predeterminado 300000).**

Esta opción controla el momento en que se debe renovar la concesión de una transacción bloqueada. Se renovará cuando quede el intervalo de tiempo especificado en milisegundos en la concesión.

4 **Introduzca el tiempo que desee en Retener las transacciones completadas en el almacén (ms) (valor predeterminado 360000).**

Indica el número de milisegundos de espera antes de la eliminación de las transacciones completadas del almacén persistente de transacciones. Salvo que las transacciones se hayan configurado para mantenerse inmediatamente, el almacén persistente de transacciones no mantendrá todas las transacciones completadas.

5 **Introduzca la Marca de agua inferior de la cola de transacciones preparadas que desee (valor predeterminado 400).**

Cuando la cola de transacciones preparadas para la ejecución del programador de transacciones cae por debajo de este lí-mite, se vuelve a cargar con transacciones preparadas hasta el lí-mite de la marca de agua superior.

6 **Introduzca la Marca de agua superior de la cola de transacciones preparadas (valor predeterminado 800).**

Cuando la cola de transacciones preparadas para la ejecución del programador de transacciones cae por debajo del lí-mite de la marca de agua inferior definido, se vuelve a cargar con transacciones preparadas hasta este lí-mite.

7 **Introduzca la Marca de agua inferior de la cola de transacciones pendientes{ (valor predeterminado 2000).**

La cola de transacciones pendientes del programador de transacciones contiene las transacciones fallidas que están pendientes de reintentarse. Si el tamaño de la cola supera la marca de agua superior, todas las transacciones que superen la marca de agua inferior se vaciarán en el almacén persistente de transacciones.

8 **Introduzca la Marca de agua superior de la cola de transacciones pendientes (valor predeterminado 2000).**

La cola de transacciones pendientes del programador de transacciones contiene las transacciones fallidas que están pendientes de reintentarse. Si el tamaño de la cola supera la marca de agua superior, todas las transacciones que superen la marca de agua inferior se vaciarán en el almacén persistente de transacciones.

9 **Introduzca el Tiempo del programador (ms) (valor predeterminado 500).**

Esta opción permite especificar la frecuencia con que debe ejecutarse el programador de transacciones (milisegundos). Cuando se ejecuta, el programador de transacciones desplaza las transacciones preparadas para ejecutar de la cola de elementos pendientes a la cola de elementos preparados y realiza otras tareas periódicas, como las transacciones persistentes del almacén persistente de transacciones.

10 **Haga clic en Guardar para aceptar la configuración.**

Supervisión de transacciones

Las transacciones de Service Provider se escriben en el almacén persistente de transacciones. Puede buscar transacciones en el almacén persistente de transacciones para ver el estado en que se encuentran.

Nota – Mediante la página Editar configuración de transacciones (consulte Administración de transacciones), el administrador puede controlar el momento en que deben mantenerse las transacciones. Por ejemplo, pueden mantenerse inmediatamente, incluso antes del primer intento.

En la página de búsqueda de transacciones puede especificar las condiciones de búsqueda que permiten filtrar las transacciones que se van a mostrar en función de criterios específicos relacionados con el evento de transacción, como usuario, tipo, estado, ID de transacción, estado actual y éxito o fallo de la transacción. Entre ellas, se incluyen las transacciones que aún se están reintentando, así como las que ya se han completado. Las transacciones que todavía no se han completado se pueden cancelar para evitar que se vuelvan intentar.

▼ Para buscar transacciones

1 **En la interfaz del administrador, haga clic en Tareas del servidor → Transacciones de proveedor de servicios.**

Se abre la página de búsqueda de transacciones de Service Provider, en la que puede especificar las condiciones de búsqueda.

Nota – La búsqueda devuelve sólo transacciones que cumplen *todas* las condiciones seleccionadas abajo. Es similar a la página Cuentas → Buscar usuarios.

---

2 **Configure la búsqueda.**

Elija una o varias de las opciones siguientes:

- **Nombre de usuario**. Permite buscar las transacciones que sólo se aplican a los usuarios con el ID de cuenta especificado.

  Nota – Si ha configurado atributos del usuario personalizados y que permiten consulta en la página de configuración de Service Provider, aparecerán aquí. Por ejemplo, puede realizar una búsqueda por apellido o nombre completo si se han configurado como atributos del usuario personalizados que permiten consulta.

- **Tipo**. Permite buscar transacciones del tipo o los tipos seleccionados.

- **Estado**. Permite buscar transacciones que se encuentran en el estado o los estados seleccionados:
  - **No se ha intentado**: transacciones que aún no se han intentado ejecutar.
  - **Reintento pendiente**: transacciones que se han intentado ejecutar una o varias veces y han generado uno o varios errores. Estas transacciones se reintentarán hasta el lí-mite de reintentos configurado para los recursos individuales.
  - **Satisfactorio**: transacciones que se han completado correctamente.
  - **No satisfactorio**: transacciones que se han completado con uno o varios fallos.
- **Intentos**. Permite buscar transacciones en función del número de veces que se han intentado ejecutar. Las transacciones que han fallado se reintentarán hasta el lí-mite de reintentos configurado para los recursos individuales.
- **Enviado**. Permite buscar transacciones en función del momento en que se envían inicialmente, en incrementos de horas, minutos o dí-as.
- **Completada**. Permite buscar transacciones en función del momento en que se han completado, en incrementos de horas, minutos o dí-as.
- **Estado cancelado**. Permite buscar transacciones en función de si se han cancelado o no.
- **ID de transacción**. Permite buscar transacciones en función de su ID único. Utilí-cela para encontrar transacciones en función del ID que ha introducido y que aparece en todos los registros de auditorí-a.
- **Ejecución**. Permite buscar transacciones en función del servidor Service Provider en el que se ejecutan. El identificador del servidor se basa en el nombre del equipo correspondiente, salvo que se haya sustituido en el archivo`Waveset.properties`.
- **Limite los resultados de búsqueda al primer número de entradas seleccionado en la lista.** Sólo se devolverán los resultados hasta el lí-mite especificado. No se realizan indicaciones si se dispone de resultados adicionales.

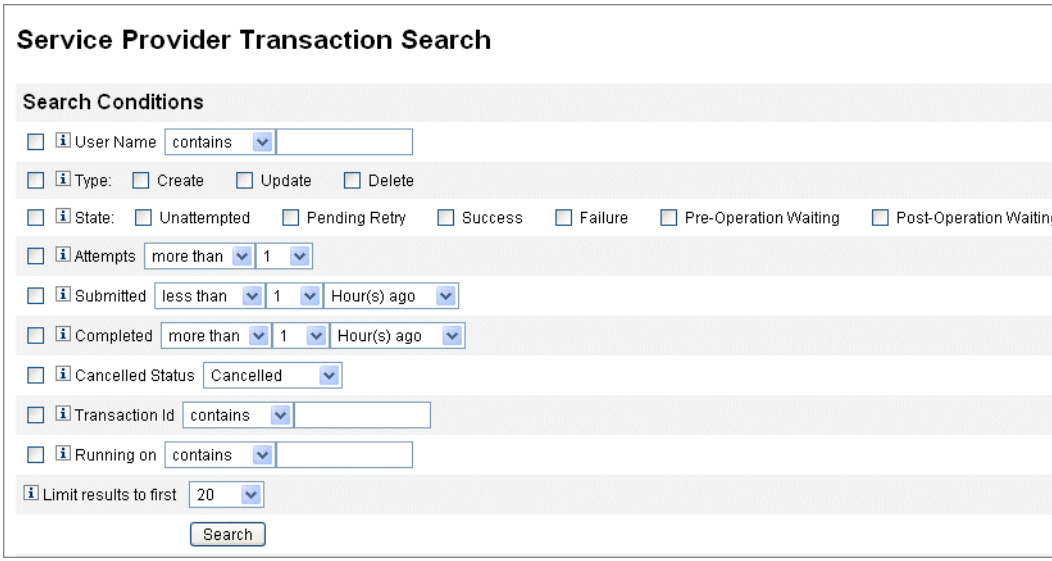


FIGURA 17–8 Buscar transacciones

3 **Haga clic en Buscar.**

Se mostrarán los resultados de búsqueda.

4 **Puede hacer clic en Descargar todas las transacciones coincidentes en la parte inferior de la página de resultados para guardar los resultados en un archivo con formato XML.**

Nota – Para cancelar las transacciones que aparecen en los resultados de búsqueda, seleccione la transacción en los resultados y haga clic en Cancelar selección. Las transacciones completadas o ya canceladas no se pueden cancelar.

Administración delegada para usuarios de Service Provider

La administración delegada para usuarios de Service Provider se activa mediante el uso de *roles de administración* de Identity Manager o mediante el modelo de autorización basado en la organización.

Delegación mediante la autorización de la organización

Identity Manager permite delegar las obligaciones administrativas mediante el modelo de autorización basado en la organización, de forma predeterminada.

Tenga en cuenta lo siguiente cuando cree administradores delegados en un modelo de autorización basado en la organización:

- Los administradores de Service Provider son usuarios de Identity Manager con capacidades específicas y organizaciones controladas.
- Los valores de atributo de la organización de los usuarios pueden ser el nombre de la organización de Identity Manager o el ID de objeto. Esto depende de cómo se configure el campo El nombre del atributo de la organización contiene el ID de Identity Manager en la pantalla de configuración principal de Identity Manager.
- Puede crear una jerarquía de Identity Manager e incluir las organizaciones en esa jerarquía en función de como quiera delegar la administración de esas organizaciones. Utilice identificadores específicos para las organizaciones en lugar de nombres de organización.
- La organización a la que pertenecen los usuarios de Service Provider se toma de los atributos de usuario del servidor de directorio.
  - Debe definir los atributos en el mapa del esquema del recurso del servidor de directorio.
  - Los atributos se comparan con la lista de la organización del administrador por *coincidencia exacta*. El valor almacenado en el directorio debe coincidir con el nombre de las organizaciones, en lugar de con la jerarquía entera. Si un administrador controla `Top:orgA:sub1`, entonces `sub1` debe tener el valor almacenado en el atributo de la organización para el usuario de Service Provider.
  - Si el atributo no se define o no coincide con una organización de Identity Manager, el usuario de Service Provider se considera un miembro de la organización principal (Top). Esto exige que los administradores de Service Provider tengan capacidades de usuario de Service Provider en `Top` para administrar los usuarios.

  La configuración del atributo determina el alcance de las búsquedas realizadas por los administradores de Service Provider.
- Para crear una cuenta de administrador delegado, cree un administrador de Identity Manager y luego agregue capacidades de administrador de Service Provider. Existen capacidades específicas de las tareas de Service Provider que se pueden asignar al usuario (mediante la ficha de seguridad de la página de edición de usuarios). Las organizaciones controladas especifican los usuarios de Service Provider que puede modificar el administrador. Todos los administradores de Identity Manager tendrán acceso a los recursos que estén a disposición de los usuarios de Service Provider.

Nota – Para obtener más información sobre la administración delegada de Identity Manager, consulte "Administración delegada" en la página 202 en el Capítulo 6, "Administración".

Delegación mediante la asignación de roles de administración

Para garantizar que los usuarios de Service Provider tengan capacidades precisas y un ámbito de control, utilice el rol de administración de usuarios de Service Provider. Los roles de administración se pueden configurar para asignarse de forma dinámica a uno o varios usuarios de Identity Manager o Service Provider al inicio de la sesión.

Puede definir y asignar reglas a roles de administración que determinen las capacidades (como `Crear usuario de Service Provider`) otorgadas a los usuarios que tienen asignado el rol de administración.

Para utilizar la delegación de roles de administración con usuarios del proveedor de servicios, debe activar esta opción en el objeto de configuración del sistema Identity Manager ("Edición de objetos de configuración de Identity Manager" en la página 118).

Cuando se activa la delegación mediante la asignación de roles de administración, no es necesario definir Nombre del atributo de la organización IDM en la configuración de Service Provider.

Activación de la delegación de roles de administración de Service Provider

Para activar la delegación de roles de administración del proveedor de servicios (administración delegada de Service Provider), abra el objeto de configuración del sistema para modificarlo ("Edición de objetos de configuración de Identity Manager" en la página 118) y defina la siguiente propiedad en `true`:

`security.authz.external.`*app name*`.`*object type*

donde *nombre apl* es la aplicación Identity Manager (como la interfaz del administrador) y *tipo de objeto* corresponde a los `usuarios de Service Provider`.

Esta propiedad se puede activar por aplicación Identity Manager (por ejemplo, para la interfaz del administrador o la interfaz de usuario) y por tipo de objeto. En la actualidad sólo se admite el tipo de objeto `Usuarios de Service Provider`. El valor predeterminado es `false`.

Por ejemplo, si quiere activar la administración delegada de Service Provider para los administradores de Identity Manager, defina los siguientes atributos en "true" en el objeto de configuración del sistema.

```
security.authz.external.Administrator Interface.Service Provider Users
```

Cuando la administración delegada de Service Provider está desactivada (definida en false) para una aplicación Identity Manager o Service Provider determinada, se utiliza el modelo de autorización basado en la organización.

Si está activada, los eventos objeto de seguimiento capturan información acerca del número y la duración de las reglas de autorización ejecutadas. Estas estadísticas están disponibles en el panel de control.

Configuración de un rol de administración de usuarios de Service Provider

Para configurar un rol de administración de usuarios de Service Provider, cree un rol de administración y especifique el ámbito de control, las capacidades y a quién se debe asignar.

Nota – Antes de crear un rol de administración de usuarios de Service Provider, defina el contexto de búsqueda, el filtro de búsqueda, el filtro tras la búsqueda, las capacidades y las reglas de asignación de usuarios del rol de administración

Para utilizar las reglas siguientes, tiene que especificar el atributo `authType` de la regla:

- SPEUsersSearchContextRule
- SPEUsersSearchFilterRule
- SPEUsersAfterSearchFilterRule
- CapabilitiesOnSPEUserRule
- UserIsAssignedAdminRoleRule
- SPEUserIsAssignedAdminRoleRule

Identity Manager ofrece reglas de ejemplo que se pueden utilizar para crear las reglas de los roles de administración de usuarios de Service Provider. Las reglas se encuentran disponibles en el archivo `sample/adminRoleRules.xml` del directorio de instalación de Identity Manager.

Para obtener más información sobre la creación de estas reglas en su entorno, consulte *Sun Identity Manager Service Provider 8.1 Deployment*.

▼ Para configurar un rol de administración de usuarios de Service Provider

1. **En la interfaz del administrador, haga clic en la opción Seguridad del menú y luego en Roles de administrador.**

   Se abre la página Roles de administrador.

2. **Pulse Nuevo.**

   Se abre la página Crear rol de Admin.

3. **Especifique el nombre del rol de administración y seleccione Usuarios de Service Provider como tipo.**

4 Especifique las opciones Ámbito de control, Capacidades y Asignar a usuarios como se describe en las secciones siguientes.

Especificación del ámbito de control

El ámbito de control del rol de administración de usuarios del proveedor de servicios establece los usuarios del proveedor que puede ver un administrador de Identity Manager, un usuario final de Identity Manager o un usuario final del proveedor de servicios de Identity Manager. Se aplica cuando se realiza una petición para que aparezca la lista de usuarios de Service Provider en el directorio.

En el ámbito de control de roles de administración de usuarios de Service Provider, puede especificar una o varias configuraciones:

- **Contexto de búsqueda de usuarios**. Especifique si se va a utilizar una regla o una cadena de texto para iniciar una búsqueda.

  Si se especifica Ninguno, el contexto de búsqueda predeterminado será el contexto base establecido en el recurso de Identity Manager, configurado como directorio de usuarios de Service Provider.

- **Filtro de búsqueda de usuarios**. Especifique si se va a aplicar una regla o una cadena de texto al filtro de búsqueda.

  La cadena de texto especificada o devuelta por la regla seleccionada debe ser una cadena de filtro de búsqueda conforme a LDAP que represente el conjunto de usuarios, dentro del contexto de búsqueda, que controlarán los usuarios que tengan este rol de administrador asignado. El filtro indicado se combinará con el de búsqueda especificado por el usuario para garantizar que los usuarios que devuelve la búsqueda no incluyen aquéllos que los usuarios asignados a este rol de administrador no pueden enumerar.

- **Regla de filtro tras búsqueda de usuarios**. Seleccione la regla que se aplicará después de utilizar el filtro de búsqueda de usuarios.

  Esta regla se ejecuta después de realizar la búsqueda LDAP inicial en el directorio de usuarios de Service Provider y evalúa los resultados para determinar los nombres distinguidos (dn) a los que puede acceder el usuario solicitante.

  Este tipo de regla se puede utilizar cuando es necesario determinar si un usuario debe encontrarse en el ámbito de control del usuario solicitante mediante atributos de usuario no LDAP (por ejemplo, pertenencia a un grupo) o cuando se utiliza un repositorio distinto del directorio de usuarios de Service Provider (por ejemplo, una base de datos Oracle o RACF) para elegir el filtro.

Especificación de capacidades

En la opción Capacidades del rol de administración de usuarios de Service Provider se especifican las capacidades y los derechos que tiene el usuario solicitante con respecto al usuario de Service Provider al que se pide acceder. Se aplica cuando se realiza una petición para ver, crear, modificar o eliminar un usuario de Service Provider.

En la ficha Capacidades, seleccione la Regla de capacidades que quiere aplicar a este rol de administración.

Asignación de roles de administración a usuarios

Los roles de administración de usuarios de Service Provider se pueden asignar dinámicamente a usuarios del proveedor de servicios especificando una regla, que se evaluará al iniciar la sesión para determinar si se asignará el rol de administrador al usuario de autenticación.

Haga clic en la ficha Asignar a usuarios y seleccione la regla de asignación que se va a aplicar.

Nota – Para activar la asignación dinámica de roles de administración a usuarios en cada interfaz de inicio de sesión (por ejemplo, la interfaz de usuario y la interfaz del administrador), configure los siguientes objetos de configuración del sistema ("Edición de objetos de configuración de Identity Manager" en la página 118) en `true`:

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.` *logininterface*

El valor predeterminado para todas las interfaces es `false`.

Delegación de roles de administración de usuarios de Service Provider

De forma predeterminada, los usuarios de Service Provider pueden asignar (o *delegar*) los roles de administración de usuarios que se les han concedido a otros usuarios de Service Provider incluidos en su ámbito de control.

De hecho, cualquier usuario de Identity Manager que pueda editar los usuarios de Service Provider puede asignar los roles de administración de usuarios de Service Provider que se le han concedido a los usuarios del proveedor de servicios que estén en su ámbito de control.

Los roles de administración de usuarios de Service Provider también pueden incluir una lista de *Asignadores*, que pueden asignar el rol de administración con independencia del ámbito de control. Estas asignaciones directas garantizan que haya al menos una cuenta de usuario conocida con capacidad para asignar el rol de administración.

Administración de usuarios de Service Provider

En esta sección se describen los procedimientos y la información que se requieren para administrar usuarios de Service Provider mediante Identity Manager.

Se tratan los temas siguientes:

Organizaciones de usuarios

Con Service Provider, el valor de un atributo de un usuario determina la organización a la que se asigna. Esto se especifica mediante el campo El nombre del atributo de la organización contiene el ID de Identity Manager de la pantalla de configuración principal de Service Provider (consulte "Configuración inicial" en la página 525). Sin embargo, los nombres de esas organizaciones deben coincidir con el valor del atributo de usuario asignado en el servidor de directorio.

Si el nombre del atributo de la organización de Identity Manager se ha definido, en las páginas Crear usuario y Editar usuario aparece una lista de selección múltiple con las organizaciones disponibles. Se muestran los nombres de organización cortos de forma predeterminada. Puede modificar el formulario de usuario de Service Provider para que presente la ruta completa de la organización.

Además, puede elegir el atributo que se convertirá en el atributo de nombre de la organización. El atributo de nombre de la organización se utiliza en las páginas de administración de usuarios de Service Provider para limitar la búsqueda y administración de un usuario por los administradores.

Nota – Existen directivas de contraseña e ID de cuenta para Service Provider y cuentas de recursos.

La directiva de cuentas del sistema Service Provider se encuentra disponible en la tabla principal de directivas.

Crear usuarios y cuentas

Todos los usuarios de proveedores de servicios deben tener una cuenta en el directorio de Service Provider. Si un usuario tiene cuentas en otros recursos, los vínculos con estas cuentas se almacenan en la entrada del directorio del usuario, con lo que la información sobre estas cuentas está disponible cuando se visualiza el usuario.

Nota – Se proporciona un ejemplo de formulario de usuario de Service Provider para crear y editar usuarios. Este formulario se puede personalizar para que cumpla los requisitos de la administración de usuarios en el entorno de Service Provider. Para obtener más información, consulte el Capítulo 2, "Identity Manager Forms" de *Sun Identity Manager Deployment Reference*.

▼ Para crear una cuenta de Service Provider

1. **En la interfaz del administrador, haga clic en la opción Cuentas de la barra de menús.**

2. **Haga clic en la ficha Administrar los usuarios de Service Provider.**

3. **Haga clic en Crear usuario.**

Nota – Cuando se utiliza el formulario de usuario predeterminado de Service Provider, la aparición de los campos depende de los atributos configurados en la tabla Atributos de cuenta (mapa del esquema) del recurso de directorio de Service Provider. Además, cuando asigne recursos al usuario (como un administrador delegado) tendrá que consultar las nuevas secciones que se han añadido a la presentación, en las que puede especificar los valores de atributo de esos recursos. También puede personalizar los campos.

4. **Especifique valores de atributo para los recursos conforme sea necesario.**

   En los valores de atributo se incluyen:

   - **ID de cuenta** (*imprescindible*)
   - **password**
   - **confirmación** (confirmación de contraseña)
   - **nombre** (*imprescindible*)
   - **apellido** (*imprescindible*)
   - **fullname**
   - **email**
   - **teléfono fijo**
   - **teléfono móvil**
   - **nº de intentos de contraseña**
   - **tiempo de desbloqueo de cuenta**

5. **Utilice las teclas de flecha para asignar los recursos que desee de la lista disponible.**

6. **En Estado de la cuenta se indica si la cuenta está bloqueada o desbloqueada. Haga clic en esta opción para bloquear o desbloquear la cuenta.**

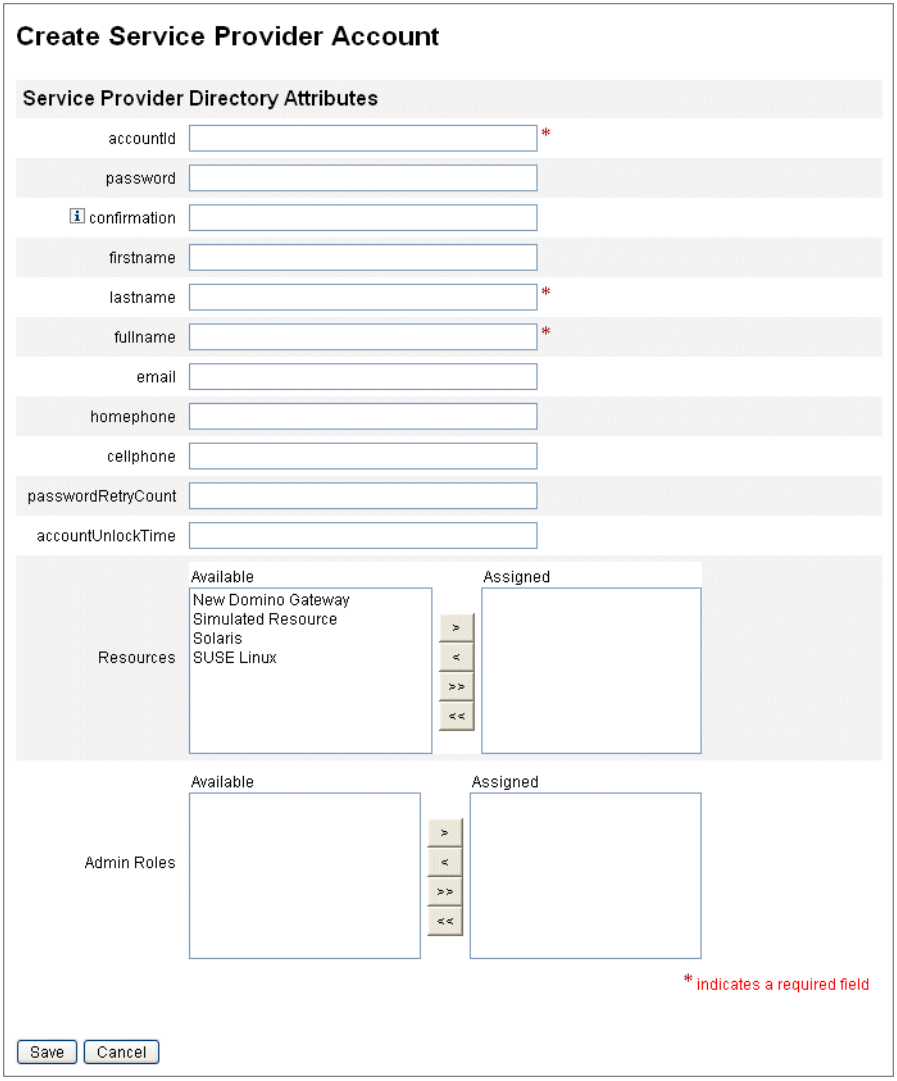


FIGURA 17–9 Crear usuarios y cuentas de Service Provider

Nota – Este formulario se rellena automática con valores correspondientes a atributos de cuentas de recursos basados en los atributos definidos para la cuenta del directorio. Por ejemplo, si el recurso define `firstName`, en el producto se introduce el valor de `firstName` de la cuenta del directorio. Sin embargo, las modificaciones realizadas en estos atributos no se propagan a las cuentas de recursos una vez que el formulario se rellena inicialmente. Si quiere, puede personalizar el formulario de usuario de ejemplo de Service Provider.

---

7 Haga clic en Guardar para crear la cuenta de usuario.

Buscar usuarios de Service Provider

Service Provider incluye una función de búsqueda que se puede configurar para facilitar la administración de cuentas de usuario. En la búsqueda sólo se encuentran los usuarios incluidos en su ámbito (conforme a lo definido por la organización, y posiblemente por otros factores).

Para realizar una búsqueda básica de usuarios del proveedor de servicios, haga clic en Administrar los usuarios de Service Provider en la sección Cuentas de la interfaz de Identity Manager; a continuación, introduzca el valor de la búsqueda y haga clic en Buscar.

En los temas siguientes se explican las funciones de búsqueda de Service Provider:

- "Búsqueda avanzada" en la página 554
- "Resultado de la búsqueda" en la página 555
- "Vincular cuentas" en la página 556
- "Eliminar, anular asignación o desvincular cuentas" en la página 557
- "Establecer opciones de búsqueda" en la página 558

Búsqueda avanzada

Para realizar una búsqueda avanzada de usuarios de Service Provider, utilice las instrucciones siguientes.

▼ Para realizar una búsqueda avanzada de usuarios de Service Provider

1 En la página Búsqueda de usuarios de Service Provider, haga clic en Avanzado.

2 Elija el atributo de la lista que desee.

3 Elija la operación que desee en la lista.

Está especificando un conjunto de condiciones para filtrar los usuarios devueltos por la búsqueda e indicando que los usuarios devueltos deben cumplir todas las condiciones especificadas.

4 Introduzca el valor de búsqueda que desee y haga clic en Buscar.

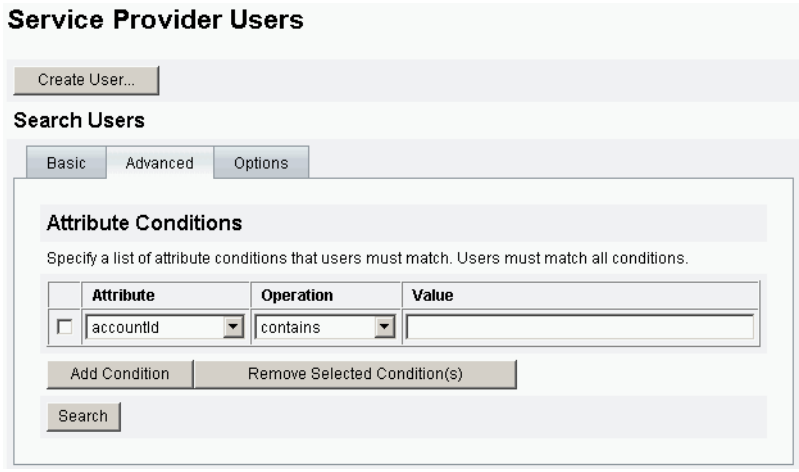


FIGURA 17–10 Buscar usuarios

Con las opciones siguientes puede agregar o eliminar condiciones de atributo:

- Haga clic en Añadir condición y especifique un atributo nuevo.
- Seleccione la condición y haga clic en Eliminar la condición seleccionada.

Resultado de la búsqueda

Los resultados de la búsqueda de Service Provider se muestran en una tabla como la que aparece en la Figura 17–11. Los resultados ordenarse por cualquier atributo haciendo clic en el encabezado de columna del atributo. La presentación de resultados depende de los atributos seleccionados.

Los botones de flecha permiten desplazarse hasta las distintas páginas de resultados (primera, anterior, siguiente o última). Si introduce un número en el cuadro de texto y pulsa Intro, puede mostrar directamente una página específica.

Para editar un usuario, haga clic en el nombre de usuario en la tabla.

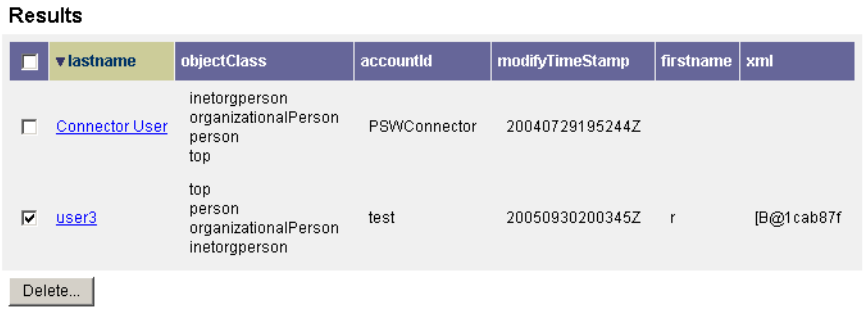


FIGURA 17–11 Ejemplo de resultados de la búsqueda

La página de resultados de la búsqueda permite eliminar usuarios o desvincular cuentas de recursos. Para esto es preciso seleccionar uno o varios usuarios y hacer clic en el botón Eliminar. Se mostrará la página de usuario de eliminación, que incluye opciones adicionales (consulte "Eliminar, anular asignación o desvincular cuentas" en la página 557).

Vincular cuentas

Service Provider se puede instalar en entornos en los que los usuarios tienen cuentas en varios recursos. La función de vinculación de cuentas de Service Provider permite asignar cuentas de recursos existentes a usuarios de Service Provider de forma progresiva. La directiva de vinculación de Service Provider, que define una regla de correlación de vínculos, una regla de confirmación de vínculos y una opción de verificación de vínculos, controla este proceso,

▼ Para vincular cuentas de usuario

1. **En la interfaz del administrador, haga clic en la opción Recursos de la barra de menús.**
2. **Seleccione el recurso que desee.**
3. **Seleccione Editar directiva de vinculación de proveedor de servicios en el menú Acción de recurso.**
4. **Seleccione una regla de correlación de vínculos. Esta regla permite buscar cuentas en los recursos que pueda tener el usuario.**
5. **Seleccione una regla de confirmación de vínculos. Esta regla permite eliminar cualquier cuenta de recursos de la lista de posibles cuentas que selecciona la regla de correlación de vínculos.**

Nota – Si la regla de correlación de vínculos selecciona una cuenta solamente, no se necesita la regla de confirmación de vínculos.

---

6 **Seleccione Se necesita verificar el ví-nculo para vincular la cuenta del recurso de destino al usuario de Service Provider.**

Eliminar, anular asignación o desvincular cuentas

▼ Para eliminar, anular la asignación o desvincular cuentas de usuario

1 **Haga clic en Cuentas en la barra de menús.**

2 **Haga clic en Administrar los usuarios de Service Provider.**

3 **Realice una búsqueda básica o avanzada.**

4 **Seleccione el usuario o los usuarios que desee.**

5 **Haga clic en el botón Eliminar.**

6 **Seleccione una de las opciones globales.**

Las opciones incluyen:

- **Eliminar todas las cuentas de recursos**

  Nota – Aunque al eliminar un recurso se elimina también la cuenta, la asignación de recurso continúa existiendo. Una actualización posterior del usuario volverá a crear la cuenta. La eliminación implica siempre una desvinculación de la cuenta de recurso.

- **Anular asignación de todas las cuentas de recursos**

  Nota – Al anular la asignación de un recurso, se elimina también dicha asignación de recurso. Asimismo, esta anulación implica siempre una desvinculación de la cuenta de recurso. Sin embargo, la cuenta de recurso no se elimina al anular la asignación de un recurso.

- **Desvincular todas las cuentas de recurso**

  Nota – La desvinculación elimina el vínculo entre un usuario y la cuenta de recurso, pero no la propia cuenta. Como tampoco se elimina la asignación de recurso, una actualización posterior del usuario volverá a vincular la cuenta o creará una cuenta nueva en el recurso.

7 **También, puede seleccionar una acción para una o varias de las cuentas de recursos en las columnas Eliminar, Anular asignación o Desvincular.**

8 **Una vez que seleccione las cuentas de usuario que desee, haga clic en Aceptar.**

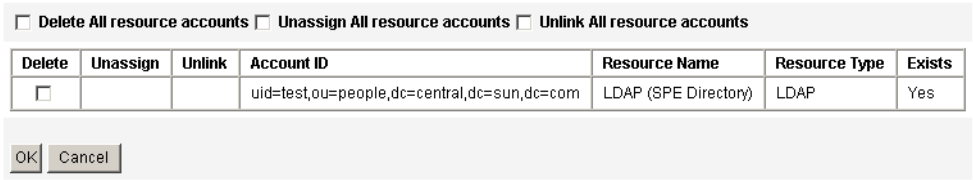


FIGURA 17–12 Eliminar, anular asignación o desvincular cuentas

Establecer opciones de búsqueda

▼ Para definir las opciones de búsqueda de los usuarios de Service Provider

1 **En la interfaz de administración, seleccione Cuentas en la barra de menús.**

2 **Haga clic en Service Provider.**

3 **Haga clic en Opciones.**

Nota – Estas opciones sólo son válidas para la sesión actual. Estas opciones afectan al modo en que se muestran los resultados de la búsqueda, tanto en una búsqueda básica como avanzada. Asimismo, algunos valores de configuración sólo se aplican en nuevas búsquedas.

---

4 **Introduzca el Número máximo de resultados.**

5 **Introduzca el Número de resultados por página.**

6 **Seleccione la opción que desee en el campo Mostrar atributos de Atributos disponibles mediante las teclas de flecha.**

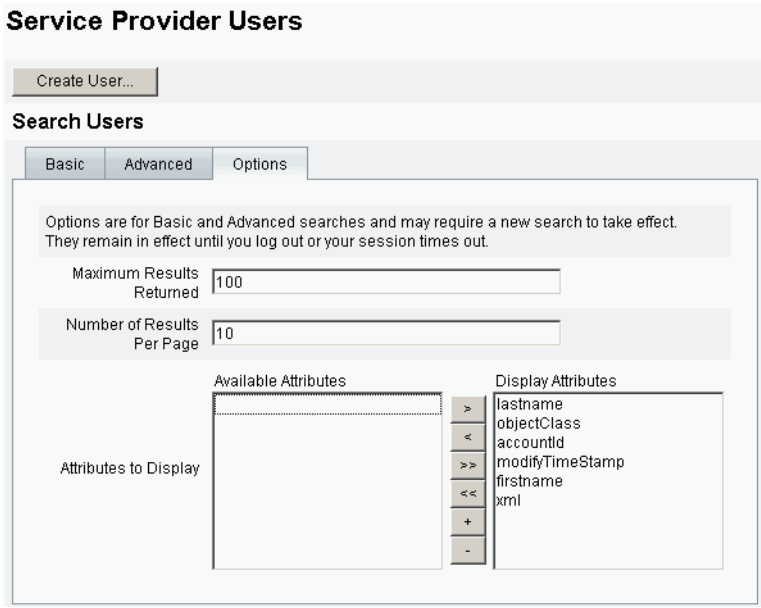


FIGURA 17–13 Establecer opciones de búsqueda para usuarios de Service Provider

Interfaz de usuario final

En las página de usuario final de ejemplo se ofrecen ejemplos de registro y autoservicio típicas de los entornos xSP. Estos ejemplos son extensibles y se pueden personalizar. Puede cambiar el estilo de la interfaz, modificar las reglas de desplazamiento entre páginas o mostrar mensajes regionales específicos de la implementación. Para obtener más información sobre la personalización de las páginas de usuario final, consulte *Sun Identity Manager Service Provider 8.1 Deployment*.

Además de auditar los eventos de autoservicio y registro, se puede enviar una notificación al usuario afectado mediante el uso de plantillas de correo electrónico. También se ofrecen ejemplos de uso de las directivas de ID de cuenta y contraseña, así como de bloqueo de cuentas. Los desarrolladores de aplicaciones pueden aprovechar los formularios de Identity Manager. El servicio de autenticación modular implementado como filtro de servlet que se puede ampliar o sustituir en caso necesario. Esto permite la integración con sistemas de administración de acceso, como Sun Access Manager.

Páginas de usuario final de ejemplo

Las páginas de usuario final de ejemplo permiten al usuario registrar y mantener información básica de usuario mediante una serie de pantallas de fácil desplazamiento, además de recibir notificación de sus acciones por correo electrónico.

Las páginas de ejemplo incluyen las siguientes funciones:

- Inicio (y cierre) de sesión, incluida autenticación mediante preguntas de desafío
- Registro e inscripción
- Cambio de contraseña
- Cambio de nombre de usuario
- Cambio de preguntas de desafío
- Cambio de dirección de notificación
- Gestión de olvido del nombre de usuario
- Gestión de olvido de la contraseña
- Notificación por correo electrónico
- Auditoría

Nota – Identity Manager utiliza una tabla de validación para el registro. Sólo pueden registrarse los usuarios incluidos en la tabla. Por ejemplo, cuando se registra el usuario Betty Childs, se localiza la entrada Betty Childs con dirección de correo electrónico bchilds@example.com en la tabla de validación y se permite el registro.

Estas páginas se pueden personalizar fácilmente en la implementación.

Para esto, realice lo siguiente:

- Cambie la información de personalización.
- Modifique las opciones de configuración (por ejemplo, el número de intentos de acceso fallidos).
- Agregue o elimine páginas.

Para obtener más información sobre la personalización de las páginas, consulte *Sun Identity Manager Service Provider 8.1 Deployment*.

Registro de nuevos usuarios

Los usuarios nuevos tienen que registrarse. Durante la operación, los usuarios pueden configurar el inicio de sesión, las preguntas de desafío y la información de notificación.

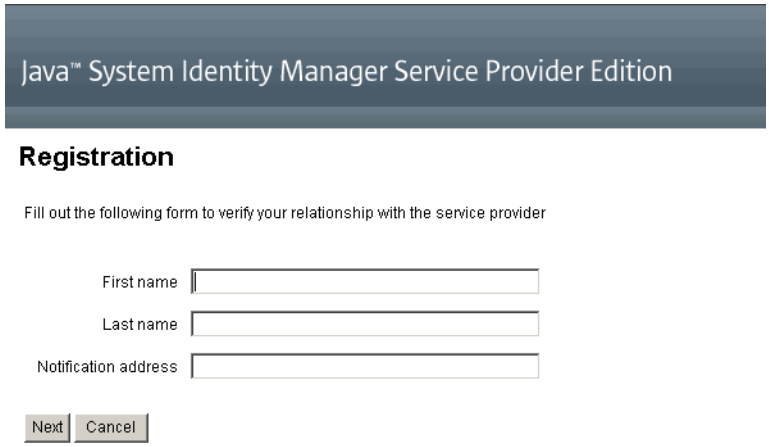


FIGURA 17–14 Página de registro

Pantallas principal y de perfil

En la Figura 17–15 se muestra la ficha principal del usuario final y la página de perfil. El usuario puede cambiar el ID de inicio de sesión y la contraseña, administrar la notificación y crear preguntas de desafío.

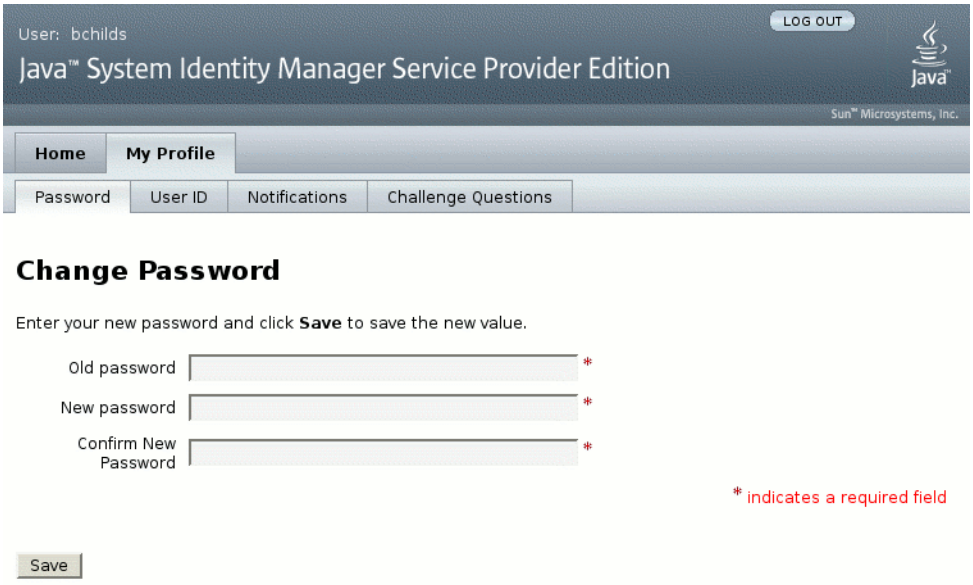


FIGURA 17–15 Página Mi perfil

Sincronización de usuarios de Service Provider

La sincronización de usuarios de Service Provider se activa mediante la directiva de sincronización. Para sincronizar los cambios de atributos en recursos con Identity Manager para usuarios de proveedores de servicios, debe configurar la sincronización de Service Provider.

En los temas siguientes se explica la forma de activar la sincronización en una implementación del proveedor de servicios:

- "Configurar la sincronización" en la página 562
- "Supervisar la sincronización" en la página 563
- "Iniciar y detener la sincronización" en la página 563
- "Migrar usuarios" en la página 564

Nota – La sincronización de Service Provider se configura desde la lista de recursos de la sección Recursos de Identity Manager.

Configurar la sincronización

Para configurar la sincronización de Service Provider. edite la directiva de sincronización de los recursos que se describen en "Para editar o configurar la sincronización" en la página 266.

Cuando edite la directiva de sincronización, tendrá que especificar las siguientes opciones para activar los procesos de sincronización en los usuarios de proveedores de servicios.

- Seleccione Usuarios de Service Provider como Tipo de objeto destino.
- En la sección Ajustes de programación, seleccione Habilitar sincronización.

Para especificar otras opciones que convengan al entorno que utiliza, siga las instrucciones que se incluyen en "Para editar o configurar la sincronización" en la página 266. Las tareas de sincronización de Service Provider tienen una duración predeterminada de 1 minuto.

Nota – La regla y el formulario de confirmación deben utilizar la vista de IDMXUser, en lugar de la vista de entrada de usuario de Identity Manager (consulte *Sun Identity Manager Service Provider 8.1 Deployment* para obtener más información).

Esto se debe a que las reglas de confirmación acceden a una vista de usuario cada vez que se identifica a un usuario en la regla de correlación, lo que afecta al rendimiento de la sincronización.

Haga clic en Guardar para guardar la definición de la directiva. Si la sincronización no está desactivada en la directiva, se programa como se ha especificado. Cuando se desactiva la sincronización, el servicio de sincronización se detiene (en caso de que esté funcionando). Si está activada, la sincronización se inicia al reiniciar el servidor Identity Manager o cuando se selecciona iniciar Service Provider en la sección de acciones de recursos de sincronización.

Supervisar la sincronización

Identity Manager ofrece los métodos siguientes para supervisar la sincronización de Service Provider.

- El estado de la sincronización aparece en el campo de descripción de la lista de recursos.
- Utilice la interfaz JMX para supervisar las unidades de sincronización.

Iniciar y detener la sincronización

La sincronización de Service Provider se activa de forma predeterminada cuando se configura Identity Manager para una implementación del proveedor de servicios.

▼ Para desactivar la sincronización activa de Service Provider

1 **En la interfaz del administrador, haga clic en la opción Recursos del menú.**

Se abre la página con la lista de recursos.

2 **En la sección Service Provider, seleccione el recurso y haga clic en Editar directiva de sincronización para editar la directiva.**

3 **Quite la marca de la casilla Habilitar sincronización.**

4 **Haga clic en Guardar.**

La sincronización se detiene cuando se guarda la directiva.

Para detener la sincronización sin desactivarla, seleccione Detención de Service Provider en la acción del recurso de sincronización.

Nota – Si utiliza la acción del recurso para detener la sincronización, sin desactivarla, se volverá a iniciar cuando se ponga en marcha cualquier servidor Identity Manager.

Migrar usuarios

Esta función de Service Provider contiene un ejemplo de tarea de migración de usuarios y de las secuencias de comandos asociadas. Mediante esta tarea, los usuarios de Identity Manager se migran al directorio de usuarios de Service Provider. En esta sección se describe la forma de utilizar la tarea de migración de ejemplo. Es conveniente que modifique este ejemplo para adaptarlo a sus circunstancias.

▼ Para migrar usuarios de Identity Manager existentes

1 **En la interfaz del administrador, haga clic en la opción Tareas del servidor del menú.**

Se abre la página Buscar tareas.

2 **Haga clic en Ejecutar tareas en el menú secundario.**

3 **Haga clic en Migración SPE.**

4 **Introduzca un nombre de tarea único.**

5 **Seleccione un recurso de la lista.**

Este es un recurso de Identity Manager que representa al servidor de directorio Service Provider. Los vínculos con este recurso encontrados en los usuarios de Identity Manager no se migran.

6 **Introduzca un atributo de identidad.**

Este es el atributo de usuario de Identity Manager que contiene la identidad exclusiva abreviada del usuario del directorio.

7 **Seleccione una regla de identidad de la lista.**

Esta es una regla opcional que puede calcular el nombre del usuario del directorio a partir de los atributos del usuario de Identity Manager. La regla de identidad puede calcular un nombre simple (normalmente UID), que luego se procesa mediante la plantilla de identidad del recurso para formar el nombre distinguido (DN) del servidor de directorio. La regla también puede devolver un DN con todas las especificaciones que evita utilizar la plantilla de ID.

8 **Haga clic en Iniciar para empezar a ejecutar la tarea de migración en segundo plano.**

Configuración de los eventos de auditoría de Service Provider

En una implementación de Service Provider, el sistema de registro de auditoría de Identity Manager examina los eventos relacionados con las actividades de los usuarios de la extranet. Identity Manager proporciona el grupo de configuración de auditoría (activado de forma predeterminada) que especifica los eventos de auditoría de los usuarios de Service Provider que se registran. Consulte la Figura 17–16.

Para obtener más información sobre el registro de auditoría y la modificación de eventos en el grupo de configuración de auditoría de Service Provider, consulte el Capítulo 10, “Registro de auditoría”.

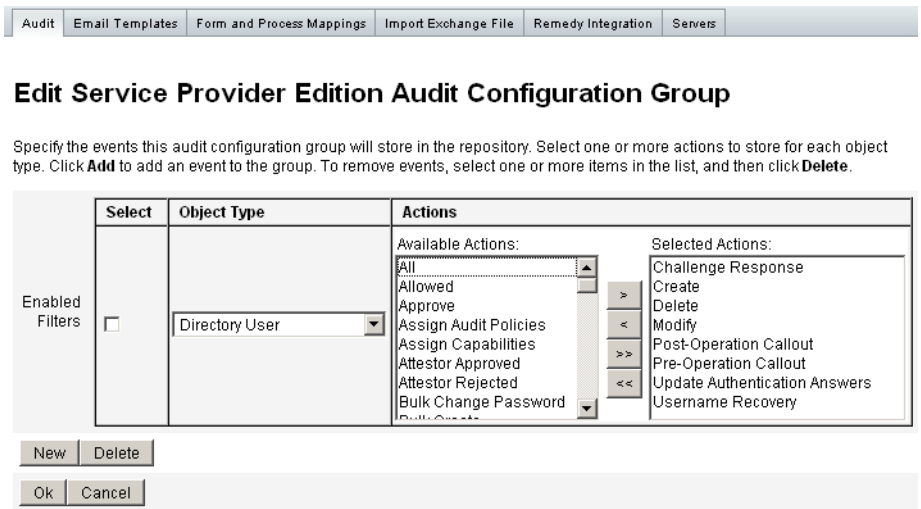


FIGURA 17–16 Página de edición del grupo de configuración de auditoría de Service Provider

◆ ◆ ◆ APÉNDICE A

Referencia de `lh`

Este apéndice contiene información que facilita el uso de la interfaz de línea de comandos de Identity Manager y la ejecución de los comandos de Identity Manager.

La información se ha organizado en estos temas:

Sintaxis de comandos de `lh`

Utilice la sintaxis siguiente para invocar la interfaz de línea de comandos de Identity Manager y ejecutar comandos de Identity Manager:

```
lh { $class | $command } [ $arg [$arg... ] ]
```

donde:

- `clase` debe ser un nombre de clase completo, como `com.waveset.session.WavesetConsole`.
- `comando` debe ser uno de los siguientes comandos:
  - `assessment` puede utilizarse durante las actualizaciones. Ofrece comandos secundarios que informan sobre todos los objetos modificados y todas las versiones instaladas de Identity Manager. Encontrará información detallada en *Sun Identity Manager 8.1 Upgrade*.
  - `config` inicia el Editor de procesos de negocio.
  - `console` inicia la consola de Identity Manager.
  - `genReports` genera un conjunto de datos aleatorios que sirven para demostrar la funcionalidad de informes de Identity Manager.

- import importa un objeto de Identity Manager. Con la opción -s se especifica el modo estricto. Cuando el modo estricto está habilitado, hay menos tolerancia al verificar las referencias durante la importación.
- js invoca un programa JavaScript.
- js también invoca un programa JavaScript.
- msgtool genera un catálogo de mensajes personalizado basado en WPMessages.properties. Este catálogo puede manipularse para efectuar cambios personalizados en texto o lenguajes.
- script ejecuta JavaScript o BeanShell.
- setRepo configura el depósito de índices de Identity Manager.
- setup inicia el proceso de configuración de Identity Manager, que permite establecer la clave de licencia, el depósito de índices de Identity Manager e importar archivos de configuración.
- spml inicia el navegador SPML.
- syslog [opciones] extrae registros del archivo de registro del sistema. Los detalles se explican en "Comando syslog" en la página 570.
- waveset actúa como alias del comando console. Consulte console, más arriba.
- xmlparse valida XML para objetos de Identity Manager.
- xpress [opciones] *Nombre de archivo* evalúa una expresión. Una opción válida es -trace (habilita la salida de seguimiento).

Notas sobre el uso

Tenga en cuenta los factores siguientes cuando utilice comandos de lh.

- Para obtener ayuda sobre el uso de los comandos, escriba lh sin argumentos.
- Al configurar las variables de entorno de ruta de acceso para el comando de lh:
  - Defina la ubicación de JAVA_HOME en el directorio de JRE que contiene un directorio bin con el ejecutable de Java. Esta ubicación varía según la instalación.

    Si tiene JRE estándar de Sun (sin JDK), una ubicación típica del directorio es C:\Archivos de programa\Java\jre1.5.0_14 (o similar). Este directorio contiene el directorio de bin con el ejecutable de Java. En tal caso, defina JAVA_HOMEen to C:\Archivos de programa\Java\jre1.5.0_14.

    Una instalación completa de JDK tiene varios ejecutables de Java. En tal caso, defina JAVA_HOME en el directorio jre integrado, que contiene el archivo bin/java.exe correcto. Con una instalación típica, defina JAVA_HOME en C:\java\jdk1.5.0_14\jre .
  - Defina la variable WSHOME en el directorio de instalación de Identity Manager así:

    ```
    set WSHOME=<path_to_identity_manager_directory>
    ```

Por ejemplo, para definir la variable en el directorio de instalación predeterminado, escriba:

```
set WSHOME=C:\Program Files\tomcat\webapps\idm
```

Nota – El valor de la variable WSHOME *no* debe contener los siguientes caracteres:

- Comillas (“ “)

  No utilice comillas aunque la ruta de acceso al directorio de implementación de la aplicación contenga espacios.
- Barra inclinada inversa (\) al final de la ruta.

En sistemas UNIX, también debe exportar las variables de la ruta escribiendo:

```
export WSHOME
export JAVA_HOME
```

- Para ejecutar el comando en modo de 64 bits, deje sin comentarios la línea FLAGS="$FLAGS -d64" en la secuencia de comandos de lh.
- Para iniciar la interfaz de línea de comandos de Identity Manager
  - Escriba lo siguiente en la línea de comandos de Windows.

    ```
    %WSHOME%\bin\lh
    ```
  - Escriba lo siguiente en una línea de comandos de UNIX.

    ```
    $WSHOME/bin/lh
    ```

Ejemplos de comandos de lh

- lh com.waveset.session.WavesetConsole
- lh console
- lh console– u $user– p *RutaAcontraseña*.txt
- lh setup -U *Administrador* -P *RutaAcontraseña*.txt
- lh setRepo– c -A *Administrador* -C *RutaAcontraseña* .txt
- lh setRepo– t *ArchivosLocales* – f $WSHOME

Comando syslog

Esta sección ofrece información sobre el comando syslog, incluidos:

Uso del comando syslog

Utilice la sintaxis siguiente para invocar el comando syslog:

```
syslog [options]
```

Opciones del comando syslog

Utilice las opciones siguientes para incluir o excluir información.

TABLA A–1 Opciones del comando syslog

Opción	Descripción
-d *Número*	Muestra los registros de los *Número* días anteriores (valor predeterminado=1).
-E	Muestra sólo los registros con nivel de gravedad de error o superior.
-F	Muestra sólo los registros con nivel de gravedad de fatal o superior.
-i *LogID*	Muestra sólo los registros con un determinado ID de registro del sistema. Los ID de registro del sistema aparecen en algunos mensajes de error y hacen referencia a una determinada entrada del registro del sistema.
-W	Muestra sólo los registros con nivel de gravedad de advertencia o superior (valor predeterminado).
-X	Incluye la causa comunicada del error, si está disponible.

◆ ◆ ◆ APÉNDICE B

Esquema de base de datos de registros de auditoría

Este apéndice proporciona información sobre los valores de esquema de datos de auditoría para los tipos de base de datos compatibles y las asignaciones de base de datos de registros de auditoría.

Tipo de base de datos Oracle

Tabla B–4 se enumeran los valores de esquema de datos para el tipo de base de datos Oracle.

TABLA B–1 Valores de esquema de datos para el tipo de base de datos Oracle

Columna de base de datos	Valor
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)

TABLA B–1 Valores de esquema de datos para el tipo de base de datos Oracle *(Continuación)*

Columna de base de datos	Valor
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) o CLOB (Consulte la nota [1] al final de la tabla.)
acctAttrChanges	VARCHAR(4000) o CLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)

TABLA B–1 Valores de esquema de datos para el tipo de base de datos Oracle *(Continuación)*

Columna de base de datos	Valor
sequence	CHAR(19)
xmlSize	NUMBER(19,0)
xml	BLOB

Nota – El límite de longitud de estas columnas es configurable. El tipo de datos predeterminado es VARCHAR, mientras que el límite de tamaño predeterminado se indica entre paréntesis. Consulte "Configuración del registro de auditoría" en la página 358 para obtener información sobre cómo ajustar el límite de tamaño.

Tipo de base de datos DB2

Tabla B–2 se enumeran los valores de esquema de datos para el tipo de base de datos DB2.

TABLA B–2 Valores de esquema de datos para el tipo de base de datos DB2

Columna de base de datos	Valor
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)

TABLA B–2 Valores de esquema de datos para el tipo de base de datos DB2 *(Continuación)*

Columna de base de datos	Valor
message	VARCHAR(255) o CLOB (Consulte la nota [1] al final de la tabla.)
acctAttrChanges	CLOB(16M)
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
sequence	CHAR(19)
xmlSize	DECIMAL(19,0)
xml	CLOB(16M)

Nota – El límite de longitud de estas columnas es configurable. El tipo de datos predeterminado es VARCHAR, mientras que el límite de tamaño predeterminado se indica entre paréntesis. Consulte "Configuración del registro de auditoría" en la página 358 para obtener información sobre cómo ajustar el límite de tamaño.

Tipo de base de datos MySQL

Tabla B–3 se enumeran los valores de esquema de datos para el tipo de base de datos MySQL.

TABLA B–3 Valores de esquema de datos para el tipo de base de datos MySQL

Columna de base de datos	Valor
id	VARCHAR(50) BINARY NOT NULL
name	VARCHAR(128) BINARY NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(255)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) o CLOB (Consulte la nota [1] al final de la tabla.)
acctAttrChanges	TEXT
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)

TABLA B–3 Valores de esquema de datos para el tipo de base de datos MySQL *(Continuación)*

Columna de base de datos	Valor
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
sequence	CHAR(19)
xmlSize	BIGINT
xml	MEDIUMTEXT

Nota – El límite de longitud de estas columnas es configurable. El tipo de datos predeterminado es VARCHAR, mientras que el límite de tamaño predeterminado se indica entre paréntesis. Consulte "Configuración del registro de auditoría" en la página 358 para obtener información sobre cómo ajustar el límite de tamaño.

Tipo de base de datos SQL Server

Tabla B–4 se enumeran los valores de esquema de datos para el tipo de base de datos SQL Server.

TABLA B–4 Valores de esquema de datos para el tipo de base de datos SQL Server

Columna de base de datos	Valor
id	NVARCHAR(50) NOT NULL
name	NVARCHAR(128) NOT NULL
repomod	DATETIME NOT NULL CURRENT_TIMESTAMP
resourceName	NVARCHAR(128)
accountName	NVARCHAR(255)
objectType	NCHAR(2)
objectName	NVARCHAR(128)
action	NCHAR(2)
actionDateTime	NCHAR(21)
actionStatus	NCHAR(1)
interface	NVARCHAR(50)
server	NVARCHAR(128)
subject	NVARCHAR(128)
reason	NCHAR(2)
message	NVARCHAR(255) o CLOB (Consulte la nota [1] al final de la tabla.)
acctAttrChanges	NTEXT
acctAttr01label	NVARCHAR(50)
acctAttr01value	NVARCHAR(128)
acctAttr02label	NVARCHAR(50)
acctAttr02value	NVARCHAR(128)
acctAttr03label	NVARCHAR(50)
acctAttr03value	NVARCHAR(128)
acctAttr04label	NVARCHAR(50)

TABLA B–4 Valores de esquema de datos para el tipo de base de datos SQL Server *(Continuación)*

Columna de base de datos	Valor
acctAttr04value	NVARCHAR(128)
acctAttr05label	NVARCHAR(50)
acctAttr05value	NVARCHAR(128)
parm01label	NVARCHAR(50)
parm01value	NVARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm02label	NVARCHAR(50)
parm02value	NVARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm03label	NVARCHAR(50)
parm03value	NVARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm04label	NVARCHAR(50)
parm04value	NVARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
parm05label	NVARCHAR(50)
parm05value	NVARCHAR(128) o CLOB (Consulte la nota [1] al final de la tabla.)
sequence	NTEXT
xmlSize	NUMERIC(19,0)
xml	NTEXT

Nota – El límite de longitud de estas columnas es configurable. El tipo de datos predeterminado es VARCHAR, mientras que el límite de tamaño predeterminado se indica entre paréntesis. Consulte "Configuración del registro de auditoría" en la página 358 para obtener información sobre cómo ajustar el límite de tamaño.

Asignaciones de base de datos de registros de auditoría

La Tabla B–5 contiene las asignaciones entre las claves de base de datos de registros de auditoría almacenadas y la cadena de visualización a la que se asignan en la salida del registro de auditoría. Identity Manager almacena los elementos que se utilizan como constantes en forma de claves breves de base de datos para ahorrar espacio en el depósito. Estas asignaciones no son visibles en la interfaz del producto. Sólo se ven al examinar la salida de un volcado de los resultados del informe de auditoría.

La Tabla B–6 contiene las claves de base de datos de acciones auditables, la Tabla B–7 contiene las claves de estado de acción y la Tabla B–8 contiene los códigos de razón que se almacenan en forma de claves en la base de datos.

TABLA B–5 Claves de base de datos de tipo de clave de objeto

Nombre de tipo	Texto en castellano	DbKey
Revisión de acceso	Revisión de acceso	AV
AccessReviewWorkflow*	Flujo de trabajo de revisión de acceso	AW
AccessScan	Exploración de acceso	AS
Account	Cuenta	AN
AdminGroup	Capacidad	AG
Administrator	Administrador	AD
AdminRole	Rol de administrador (Admin)	AR
Application	Grupo de recursos	AP
AttributeDefinition	Definición de atributos	AF
AttrParse	Análisis de atributos	AT
AuditConfig	AuditConfig	AC
AuditPolicy	Directiva de auditoría	CP
BeanPod	Pod de bean	BP
ComplianceViolation	Infracción del cumplimiento	CV
Configuration	Configuración	CN
DataExporter	Exportador de datos	DE
Discovery	Discovery	DS
Email*	Correo electrónico	EM

TABLA B–5 Claves de base de datos de tipo de clave de objeto *(Continuación)*

Nombre de tipo	Texto en castellano	DbKey
EmailTemplate	Plantilla de correo electrónico	ET
EncryptionKey	Clave de cifrado	KY
Event	Evento	EV
Extract	Extract	ER
ExtractTask	ExtractTask	EX
IDMXUser*	Usuario del directorio	UX
LighthouseAccount*	Cuenta de Identity System	LA
LoadConfig	LoadConfig	LD
LoadTask	LoadTask	LT
Log	Registro	LG
LoginApp	LoginApp	LP
LoginConfig	Configuración de inicio de sesión	LC
LoginModGroup	LoginModGroup	LF
MetaView	Vista Meta	MV
ObjectGroup	Organización	OG
Policy	Directiva	PO
ProvisioningTask	Tarea de abastecimiento	PT
RemediationWorkflow*	Flujo de trabajo de remediación	RW
RemedyConfig	RemedyConfig	RC
Resource	Recurso	RS
ResourceAccount*	Cuenta de recursos	RA
ResourceAction	Acción de recurso	RN
ResourceForm	Formulario de recurso	RF
ResourceObject	ResourceObject	RE
RiskReportTask	RiskReportTask	RR
Role	Rol	RL
Rule	Regla	RU
SnapShot	SnapShot	SS

TABLA B–5 Claves de base de datos de tipo de clave de objeto *(Continuación)*

Nombre de tipo	Texto en castellano	DbKey
ServerObject	ServerObject	SV
SysLog	SysLog	SL
System	Sistema	SY
TaskDefinition	Definición de tareas	TD
TaskInstance	Instancia de tarea	TI
TaskResult	Resultado de tareas	TR
TaskResultPage	ResultPage	TP
TaskSchedule	Programación de tareas	TS
Plantilla de tareas	Plantilla de tareas	TT
TestNotification*	Notificación de prueba	TN
User	Usuario	US
UserEntitlement	Derecho de usuario	UE
UserForm	Formulario de usuario	UF
WorkflowCase*	Caso de flujo de trabajo	WC
WorkItem	Elemento de trabajo	WI
XmlData	Datos XML	XD

[1]

TABLA B–6 Claves de acción base de datos

Nombre de acción	Texto en castellano	DbKey
Allowed*	Permitido	AL
Approve	Aprobar	AP
Assign Audit Policies	Asignar directivas de auditoría	AA
Assign Capabilities	Capacidades de asignación	AC
AttestorApproved*	Autenticador aprobado	TA
AttestorRejected*	Autenticador rechazado	AR

[1] * Tipos extendidos

TABLA B–6 Claves de acción base de datos *(Continuación)*

Nombre de acción	Texto en castellano	DbKey
AttestorRemediate*	Remediación solicitada	AF
AttestorRescan*	Nuevo análisis solicitado	AN
Bulk Change Password	Cambiar contraseña en masa	BW
Bulk Create	Creación en masa	BC
Bulk Delete	Eliminación en masa	BD
Bulk Deprovision	Desabastecimiento masivo	BP
Bulk Disable	Inhabilitación en masa	BF
Bulk Enable	Habilitación en masa	BE
Bulk Modify	Modificación en masa	BM
Bulk Reset Password	Reinicializar contraseña en masa	BR
Bulk Unassign	Anulación de asignación masiva	BU
Bulk Unlink	Desvinculación masiva	BL
Bypass Verify	Eludir verificación	BV
CancelReconcile*	Cancelar reconciliación	CR
challengeResponse*	Respuesta de desafío	CD
Change Password	Cambiar contraseña	CP
Connect	Conectar	CN
Control Active Sync	Controlar sincronización activa	CA
Create	Crear	CT
CredentialsExpired*	Las credenciales caducaron	CE
Debug	Depurar	DB
Delegate	Delegar	DG
Delete	Eliminar	DL
Deprovision	Desabastecer	DP
Disable	Inhabilitar	DS
Disconnect	Desconectar	DC
Enable	Habilitar	EN
End Activity	Finalizar actividad	EA

TABLA B–6 Claves de acción base de datos *(Continuación)*

Nombre de acción	Texto en castellano	DbKey
End Process	Finalizar proceso	PE
End Workflow	Finalizar flujo de trabajo	EW
Execute	Ejecutar	LN
Expired*	Caducado	EX
Export	Exportar	EP
Fixed*	Solucionado	FX
Import	Importar	IM
List	Lista	LI
Lock	Bloquear	LK
Login	Inicio de sesión	LG
Logout*	Cierre de sesión	LO
Mitigated*	Mitigada	VM
Modify	Modificar	MO
Modify Active Sync	Modificar sincronización activa	MA
NativeChange*	Cambiar atributos nativos	NC
Notify*	Notificar	NO
PostOperation*	Llamada posterior a la operación	PT
PreOperation*	Llamada previa a la operación	PP
Prioritize*	Priorizar	PR
Provision	Abastecer	PV
Recurring*	Periódico	RC
Reject	Rechazar	RJ
Remediated*	Remediado	VR
Rename	Cambiar nombre	RE
RequestReconcile*	Solicitar reconciliación	RR
ResetPassword	Reinicializar contraseña	RP
Run Debugger	Ejecutar depurador	RD
ScanBegin*	Inicio del análisis	SB

TABLA B–6 Claves de acción base de datos *(Continuación)*

Nombre de acción	Texto en castellano	DbKey
ScanEnd*	Finalización del análisis	SE
StartActivity*	Iniciar actividad	SA
StartProcess*	Iniciar proceso	SP
StartWorkflow*	Iniciar flujo de trabajo	SW
Terminate*	Terminar	TR
Unassign	Anular asignación	UA
Unlink	Desvincular	UN
Unlock	Desbloquear	UL
updateAuthenticationAnswers*	Actualizar respuestas de autenticación	AQ
usernameRecovery*	Recuperación del nombre de usuario	UR
View	Ver	VW
View Only	Sólo visualización	VO

2

TABLA B–7 Claves de base de datos de estado de acción

Resultado	DbKey
Satisfactorio	S
No satisfactorio	F

TABLA B–8 Razones almacenadas como claves

Nombre de razón	Texto en castellano	DbKey
PolicyViolation	Infracción de directiva {0}:{1}	PV
InvalidCredentials	Credenciales no válidas	CR
InsufficientPrivileges	Privilegios insuficientes	IP
DatabaseAccessFailed	Falló acceso a la base de datos	DA
AccountDisabled	Cuenta inhabilitada	DI

2 * Acciones extendidas

◆ ◆ ◆ APÉNDICE C

Referencia rápida de la interfaz de usuario

La Tabla C–1 ofrece una referencia rápida para las tareas habituales de Identity Manager. La tabla muestra la ubicación principal de la interfaz de Identity Manager donde debe situarse para comenzar cada tarea, junto con ubicaciones alternativas o métodos (en su caso) que puede usar para realizar la misma tarea.

Referencia de tareas de la interfaz de Identity Manager

TABLA C–1 Referencia de tareas

Para realizar esta tarea	Vaya a	O bien a
Administrar usuarios de Identity Manager:		
Crear y editar usuarios	Ficha Cuentas, seleccione Listar cuentas	Ficha Cuentas, seleccione Buscar usuarios (página Resultados de la búsqueda de cuentas de usuario)
Aprobar creación de cuenta de usuario	Ficha Elementos de trabajo, ficha Aprobaciones	
Configurar autenticación de usuario (directivas)	Ficha Seguridad, seleccione Directivas	
Cambiar contraseñas de usuario	Ficha Modificar contraseña de usuario, seleccione Modificar contraseña de usuario	Ficha Cuentas, seleccione Listar cuentas Ficha Cuentas, seleccione Buscar usuarios (página Resultados de la búsqueda de cuentas de usuario) Interfaz de usuario de Identity Manager

TABLA C–1 Referencia de tareas *(Continuación)*

Para realizar esta tarea	Vaya a	O bien a
Reinicializar contraseñas de usuario	Ficha Contraseñas, seleccione Reinicializar contraseña de usuario	Ficha Cuentas, seleccione Listar cuentas Ficha Cuentas, seleccione Buscar usuarios (página Resultados de la búsqueda de cuentas de usuario)
Buscar usuarios	Ficha Cuentas, seleccione Buscar usuarios	Ficha Modificar contraseña de usuario, seleccione Modificar contraseña de usuario
Habilitar o inhabilitar usuarios	Ficha Cuentas, seleccione Listar cuentas	Ficha Cuentas, seleccione Buscar usuarios (página Resultados de la búsqueda de cuentas de usuario)
Desbloquear usuarios	Ficha Cuentas, seleccione Listar cuentas	Ficha Cuentas, seleccione Buscar usuarios (página Resultados de la búsqueda de cuentas de usuario)
Administrar administradores de Identity Manager:		
Configurar la administración delegada (mediante organizaciones)	Ficha Cuentas, seleccione Listar cuentas, página Crear usuario	
Asignar capacidades	Ficha Cuentas, seleccione Listar cuentas, página Crear o Editar usuario, ficha Seguridad	
Asignar capacidades (mediante roles de administrador)	Ficha Cuentas, seleccione Listar cuentas, página Crear o Editar usuario, ficha Seguridad	
Configurar aprobadores (para validar la creación de cuentas)	Ficha Cuentas, seleccione Listar cuentas, página Organización Ficha Roles, página Crear roles	
Configurar Identity Manager:		
Crear y administrar recursos (asistente de recursos)	Ficha Recursos	
Administrar grupos de recursos	Ficha Recursos, seleccione Listar Grupos de recursos	
Crear y administrar roles	Ficha Roles	

TABLA C–1 Referencia de tareas *(Continuación)*

Para realizar esta tarea	Vaya a	O bien a
Buscar roles	Ficha Roles, seleccione Buscar roles	
Editar capacidades	Ficha Seguridad, seleccione Capacidades	
Crear y editar roles de administrador	Ficha Seguridad, seleccione Roles de administrador (Admin), página Crear/Editar rol de administrador (Admin)	
Configurar plantillas de correo electrónico	Ficha Configurar, seleccione Plantillas de correo electrónico	
Configurar directivas de contraseñas, de cuentas y de asignación de nombres; asignar directivas a organizaciones	Ficha Seguridad, seleccione Directivas	
Cargar y sincronizar cuentas y datos:		
Importar archivos de datos (como formularios en formato XML)	Ficha Configurar, seleccione Importar archivo de intercambio	
Cargar cuentas de recurso	Ficha Cuentas, seleccione Cargar desde recurso	
Cargar cuentas desde archivo	Ficha Cuentas, seleccione Cargar desde archivo	
Comparar usuarios de Identity Manager con cuentas de recursos	Ficha Recursos, seleccione Reconciliar con recursos	
Auditar y administrar el cumplimiento:		
Inhabilitar o habilitar auditoría	Ficha Configurar, seleccione Auditoría	
Configurar eventos de auditoría para capturar	Ficha Configurar, seleccione Auditoría	
Definir directivas de auditoría (crear, editar, eliminar)	Ficha Cumplimiento, seleccione Administrar directivas	
Asignar directivas de auditoría	Ficha Cuentas, seleccione Cumplimiento	

TABLA C–1 Referencia de tareas *(Continuación)*

Para realizar esta tarea	Vaya a	O bien a
Definir remediadores y asignar flujos de trabajo de remediación para una directiva de auditoría	Ficha Cumplimiento, ficha Administrar directivas	
Responder a solicitudes de remediación de infracciones de directiva	Ficha Mis elementos de trabajo, seleccione Remediaciones	
Mitigar infracciones de directivas	Ficha Elementos de trabajo, ficha Remediaciones	
Revisar infracciones de directivas remediadas	Ficha Elementos de trabajo, ficha Remediaciones	
Generar informes de directivas de auditoría	Ficha Informes, ficha Ejecutar informe	
Realizar un análisis de auditoría en uno o más usuarios u organizaciones	Ficha Cuentas, seleccione Analizar en la lista Acciones de usuario u Acciones de organización	
Configurar revisiones de acceso periódicas	Ficha Cumplimiento, seleccione Administrar exploraciones de acceso	
Supervisar revisiones de acceso periódicas	Ficha Cumplimiento, seleccione Revisiones de acceso	
Ver informes de auditoría	Ficha Informes, seleccione el tipo de informe Auditor	
Editar capacidades de auditoría de administrador	Ficha Seguridad, ficha Capacidades	
Configurar plantillas de correo electrónico para notificación de auditoría	Ficha Configurar, ficha Plantillas de correo electrónico	
Importar reglas/archivos de datos (como formularios en formato XML)	Ficha Configurar, ficha Importar archivo de intercambio	
Definir Realiza una exploración de revisión de acceso	Ficha Cumplimiento, ficha Administrar exploraciones	
Ejecutar una revisión de acceso	Ficha Cumplimiento, ficha Revisiones de acceso	

TABLA C–1 Referencia de tareas *(Continuación)*

Para realizar esta tarea	Vaya a	O bien a
Terminar una revisión de acceso	Ficha Cumplimiento, ficha Revisiones de acceso	
Programar una revisión de acceso	Ficha Tareas del servidor, ficha Administrar programación	
Configurar revisiones de acceso periódicas	Ficha Cumplimiento, ficha Administrar exploraciones de acceso	
Supervisar estado de revisión de acceso	Ficha Cumplimiento, ficha Revisiones de acceso	
Configurar autenticadores	Ficha Cumplimiento, ficha Administrar exploraciones de acceso	
Ejercer tareas de autenticador (revisar y certificar derechos de usuario)	Ficha Elementos de trabajo, ficha Mis elementos de trabajo, ficha Autenticación	
Análisis de riesgo e informes:		
Ejecutar y administrar informes	Ficha Informes, seleccione Ejecutar informes para crear, ejecutar y descargar informes; Ver informes para ver resultados de informes.	
Definir y ejecutar informes de análisis de riesgo	Ficha Informes, seleccione Análisis de riesgo	
Ver informes gráficos	Ficha Informes, seleccione Ver paneles	
Revisar informe de separación de tareas	Ficha Informes, ficha Ejecutar informe	
Administrar tareas de Identity Manager:		
Ejecutar una tarea o proceso definido	Ficha Tareas del servidor, seleccione Ejecutar tareas	
Programar una tarea	Ficha Tareas del servidor, seleccione Administrar programación	
Ver resultados de tareas	Ficha Tareas del servidor, seleccione Buscar tareas o Todas las tareas	

TABLA C–1 Referencia de tareas *(Continuación)*

Para realizar esta tarea	Vaya a	O bien a
Suspender o terminar una tarea	Ficha Tareas del servidor, seleccione Todas las tareas	
Administrar los usuarios de Service Provider:		
Administrar los usuarios de Service Provider	Ficha Cuentas, Administrar los usuarios de Service Provider	
Administrar transacciones de proveedor de servicios	Ficha Tareas del servidor, seleccione Transacciones de proveedor de servicios	
Configurar transacciones de proveedor de servicios	Ficha Service Provider, seleccione Editar configuración principal	
Configurar valores predeterminados de transacción	Ficha Service Provider, seleccione Editar configuración de transacciones	
Crear o editar directivas de Service Provider	Ficha Seguridad, seleccione Directivas	

◆ ◆ ◆ APÉNDICE D

Definiciones de capacidades

En este apéndice se definen las distintas capacidades de Identity Manager.

La información se ha dividido en las secciones siguientes:

Encontrará información general acerca de las capacidades en "Conceptos y administración de capacidades" en la página 216.

Nota – Todas las capacidades conceden al usuario o al administrador acceso a las fichas Contraseñas → Cambiar mi contraseña y Modificar mis respuestas.

Definiciones de capacidades basadas en tareas

En esta sección se describen las capacidades basadas en tareas que pueden asignarse a los usuarios. También se indican las fichas principales y secundarias a las que se accede con cada capacidad. Las capacidades se enumeran por orden alfabético.

Nota – Esta tabla no contiene información sobre las fichas principales y secundarias predeterminadas que están disponibles para todos los usuarios, como Cambiar mi contraseña ficha.

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador del informe de detalle de revisión de acceso	Crear, editar, eliminar y ejecutar informes de detalle de revisión de acceso, informes de cobertura de revisión de acceso e informes de cobertura de ámbito de usuario de exploración de acceso.	Informes → fichas Ejecutar informes y Ver informes
Administrador del informe de resumen de revisión de acceso	Crear, editar, eliminar y ejecutar informes de resumen de revisión de acceso.	Informes → fichas Ejecutar informes y Ver informes
Administrador de cuentas	Realizar todas las operaciones con los usuarios, incluida asignación de capacidades. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas, Buscar usuarios, Extraer a archivo, Cargar desde archivo y Cargar desde recurso Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de informes administrativos	Crear, editar, eliminar y ejecutar informes administrativos e informes de roles de administrador.	Informes → fichas Ejecutar informes y Ver informes (sólo informes administrativos e informes de roles de administrador)
Administrador de roles de Admin	Crear, editar y eliminar roles de administrador.	Seguridad → ficha Roles de administrador (Admin)
Administrador de aplicaciones	Crear, editar y eliminar roles de aplicación.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas (sincronizar roles) Roles → fichas Listar roles y Buscar roles
Administrador de activos	Crear, editar y eliminar roles de activos.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas (sincronizar roles) Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador para asignar directivas de auditoría	Asignar directivas de auditoría a cuentas de usuario y organizaciones. Editar directivas de auditoría de usuario en la lista Acciones de usuario y directivas de auditoría de organización en la lista Acciones de organización.	Cuentas → fichas Listar cuentas y Buscar usuarios
Administrador para asignar directivas de auditoría de organización	Asignar directivas de auditoría a organizaciones solamente. Editar directivas de auditoría de organización en la lista Acciones de organización.	Cuentas → ficha Listar cuentas
Administrador para asignar directivas de auditoría de usuario	Asignar directivas de auditoría a usuarios solamente. Editar directivas de auditoría de de usuario en la lista Acciones de usuario.	Cuentas → fichas Listar cuentas y Buscar usuarios
Asignar capacidades de usuario	Cambiar las asignaciones de capacidades del usuario (asignar y anular la asignación). Debe asignarse con otra capacidad de administrador de usuarios (por ejemplo, Crear usuario o Habilitar usuario).	Cuentas → fichas Listar cuentas (sólo Editar) y Buscar usuarios
Administrador de directivas de auditoría	Crear, modificar y eliminar directivas de auditoría.	Cumplimiento → ficha Administrar directivas
Administrador de informe de análisis de directivas de auditoría	Ejecutar o programar tareas de análisis de directivas de auditoría.	Tareas del servidor → fichas Buscar tareas, Todas las tareas, Ejecutar tareas y Administrar programa
Administrador de informes de auditoría	Crear, editar, eliminar y ejecutar informes de auditoría. Acceso a informes de registro de auditoría, de cambios históricos de usuario, de registros de auditoría de usuarios individuales y de uso.	Informes → fichas Ejecutar informes y Ver informes
Administrador de informe de AuditLog	Crear, modificar, eliminar y ejecutar informes de registro de auditoría.	Informes → ficha Ejecutar informes
Administrador de informe de atributos auditados	Crear, modificar, eliminar y ejecutar informes de atributos auditados.	Informes → fichas Ejecutar informes y Ver informes

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de exploraciones de acceso de Auditor	Crear, editar y eliminar exploraciones de revisiones de acceso periódicas.	Cumplimiento → ficha Administrar exploraciones de acceso
Administrador del Auditor	Configurar, administrar y supervisar directivas de auditoría, análisis de auditoría y cumplimiento de usuario.	Cuentas → fichas Listar cuentas y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas, Ejecutar tareas y Administrar programa Informes → fichas Ejecutar informes y Ver informes Cumplimiento → fichas Administrar directivas, Administrar exploraciones de acceso y Revisiones de acceso
Autenticador de Auditor	Es necesario para autenticar las autenticaciones de otros usuarios mientras está habilitada la seguridad de la organización.	Sólo fichas predeterminadas de Contraseñas y Elementos de trabajo
Administrador de revisiones de acceso periódicas de Auditor	Administrar revisiones de acceso periódicas (PAR), exploraciones de acceso, autenticaciones e informes de revisiones de acceso periódicas.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Cumplimiento → fichas Administrar exploraciones de acceso y Revisión de acceso
Remediador del Auditor	Remediar, mitigar y remitir infracciones de directivas de auditoría.	Sólo fichas predeterminadas de Contraseñas y Elementos de trabajo
Administrador de informe de Auditor	Crear, modificar, eliminar y ejecutar cualquiera de los informes de Auditor.	Tareas del servidor → fichas Buscar tareas, Todas las tareas, Ejecutar tareas y Administrar programa Informes → todas las acciones con informes de auditoría
Usuarios de la vista de auditor	Ver la información de cumplimiento asociada al usuario.	Cuentas → fichas Listar cuentas y Buscar usuarios
Administrador del historial de infracciones de directivas de auditoría	Crear, modificar, eliminar y ejecutar el informe del Historial de infracciones de directivas de auditoría.	Informes → ficha Ejecutar informes

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de cuentas en masa	Realizar todas las operaciones normales y en masa con los usuarios, incluida asignación de capacidades.	Cuentas → fichas Listar cuentas, Buscar usuarios, Iniciar acciones masivas, Extraer a archivo, Cargar desde archivo y Cargar desde recurso Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de cambios de cuentas en masa	Realizar operaciones normales y en masa con los usuarios existentes, incluyendo asignación de capacidades y exceptuando la eliminación de usuarios. No puede crear ni eliminar usuarios.	Cuentas → fichas Listar cuentas, Buscar usuarios e Iniciar acciones masivas Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de cambio de contraseñas de recursos en masa	Cambiar la contraseña para la cuenta de conexión especificada en los recursos.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → fichas Listar recursos e Iniciar acciones masivas
Administrador de cambios de cuentas de usuario en masa	Realizar operaciones normales y en masa, excepto la eliminación de usuarios existentes. No puede crear, eliminar ni asignar capacidades a los usuarios.	Cuentas → fichas Listar cuentas, Buscar usuarios e Iniciar acciones masivas Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Creación de usuarios en masa	Asignar recursos e iniciar solicitudes de creación de usuario (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo Crear), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Eliminación de usuarios en masa	Borrar cuentas de usuario de Identity Manager; desabastecer, anular asignaciones y anular vínculos de cuentas de recursos (con usuarios individuales o mediante operaciones en masa).	Cuentas → fichas Listar cuentas, Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Eliminar masivamente usuarios de IDM	Borrar cuentas de usuario de Identity Manager (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo Eliminar), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Desabastecimiento masivo de usuarios	Borrar y desvincular cuentas de recursos existentes (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo Desabastecer), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Inhabilitación de usuarios en masa	Inhabilitar usuarios y cuentas de recursos existentes (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo Inhabilitar), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Habilitar usuarios en masa	Habilitar usuarios y cuentas de recursos existentes (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo Habilitar), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de reinicialización de contraseñas de recursos en masa	Reinicializar la contraseña para la cuenta de conexión especificada en los recursos.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → fichas Listar recursos e Iniciar acciones masivas
Desasignación masiva de usuarios	Desasignar y desvincular cuentas de recursos existentes (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo Anular asignación), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Desvinculación masiva de usuarios	Desvincular cuentas de recursos existentes (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo Desvincular), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Actualización de usuarios en masa	Editar, mover y actualizar usuarios y cuentas de recursos existentes (con usuarios individuales y mediante operaciones en masa).	Cuentas → fichas Listar cuentas (sólo editar, mover y actualizar), Buscar usuarios e Iniciar acciones masivas Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de cuentas de usuario en masa	Realizar operaciones normales y en masa con los usuarios.	Cuentas → fichas Listar cuentas, Buscar usuarios, Iniciar acciones masivas, Extraer a archivo, Cargar desde archivo y Cargar desde recurso Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de roles de negocio	Crear, editar y eliminar roles de negocio.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas (sincronizar roles) Roles → fichas Listar roles y Buscar roles
Administrador de capacidades	Crear, modificar y eliminar capacidades.	Seguridad → ficha Capacidades
Administrador de cambios de cuentas	Realizar todas las operaciones con los usuarios existentes, incluyendo asignación de capacidades y exceptuando la eliminación de usuarios. No incluye las operaciones en masa. Crear informes de administrador y de usuario, ejecutar y editar informes de administrador, ejecutar informes de AuditLog dentro del ámbito. No puede ejecutar informes de administrador o de usuario en organizaciones fuera del ámbito. No puede eliminar usuarios.	Cuentas → fichas Listar cuentas y Buscar usuarios Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de cambios de sincronización activa de recursos	Cambiar los parámetros de recursos de Active Sync.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → ficha Listar recursos

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de cambio de contraseñas	Cambiar contraseñas de cuenta de usuario y recursos. Acceso sólo a la tarea de análisis de exportación de contraseña (en la ficha Ejecutar tareas).	Cuentas → fichas Listar cuentas y Buscar usuarios Contraseñas → Modificar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de cambio de contraseñas (requiere verificación)	Cambiar contraseñas de cuentas de usuario y de recursos después de una validación con éxito de las respuestas a las preguntas de autenticación del usuario. Acceso sólo a la tarea de análisis de exportación de contraseña (en la ficha Ejecutar tareas).	Cuentas → fichas Listar cuentas y Buscar usuarios Contraseñas → ficha Modificar contraseña de usuario (requiere verificación antes de la acción) Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de cambio de contraseñas de recursos	Cambiar contraseñas de cuenta de administrador de recursos. Cambiar contraseñas de recursos solamente (con Administrar conexión → Cambiar contraseña en el menú de acciones)	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → ficha Listar recursos
Administrador de cambios de cuentas de usuario	Realizar todas las operaciones con usuarios existentes, excepto eliminación y operaciones en masa. Tampoco puede crear, eliminar ni asignar capacidades a los usuarios.	Cuentas → fichas Listar cuentas y Buscar usuarios Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Configurar auditorías	Configurar los eventos y grupos de configuración que se auditan en el sistema.	Configurar → ficha Auditoría
Configurar certificados	Configurar certificados y CRLs en los que se confía.	Seguridad → ficha Certificados

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de control de recursos de Active Sync	Controlar el estado de los recursos de Active Sync (como, por ejemplo, el inicio, la detención y la actualización)	Recursos → ficha Listar recursos Para recursos de Active Sync: menú de acciones de Active Sync
Crear usuario	Asignar recursos e iniciar solicitudes de creación de usuarios. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Crear) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de almacén de datos	Configurar el Exportador de datos y ejecutar la tarea Iniciador del exportador de almacén de datos.	Informes → fichas Gráficos del panel y Ver paneles Recursos → ficha Listar recursos Configurar → ficha Almacén
Consulta de almacén de datos	Configurar y ejecutar consutas forenses.	Informes → fichas Gráficos del panel y Ver paneles Recursos → ficha Listar recursos Cumplimiento → Consulta forense
Eliminar usuario	Borrar cuentas de usuario de Identity Manager; desabastecer, anular asignaciones y anular vínculos de cuentas de recursos. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Eliminar) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Eliminar usuario de IDM	Eliminar cuentas de usuario de Identity Manager. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Eliminar) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Desabastecer usuario	Borrar y desvincular cuentas de recursos existentes. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Desabastecer) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Inhabilitar usuario	Inhabilitar usuarios y cuentas de recursos existentes. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Inhabilitar) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Habilitar usuario	Habilitar usuarios y cuentas de recursos existentes. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Habilitar) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de usuario final	Ver y modificar los derechos sobre los tipos de objetos especificados en la capacidad de usuario final y mediante la regla de organizaciones controladas por el usuario final.	Todas las fichas predeterminadas
Administrador de recursos externos	Ver y configurar sólo recursos externos. No puede crear nuevos recursos.	Configurar → ficha Recursos externos
Configurar esquema de Identity Manager	Ver y configurar el esquema efectivo para los usuarios o roles mediante el objeto de configuración `IDM Schema Configuration` de Identity Manager.	Todas las fichas predeterminadas
Importar usuario	Importar usuarios desde los recursos definidos.	Cuentas → fichas Listar cuentas, Buscar usuarios, Extraer a archivo, Cargar desde archivo y Cargar desde recurso Roles → fichas Listar roles y Buscar roles
Administradores de importación/exportación	Importar y exportar todos los tipos de objetos.	Configurar → ficha Importar archivo de intercambio
Administrador de roles de TI	Crear, editar y eliminar roles de TI.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas (sincronizar roles) Roles → fichas Listar roles y Buscar roles
Administrador de inicio de sesión	Editar el conjunto de módulos de inicio de sesión para una determinada interfaz.	Seguridad → ficha Inicio de sesión

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de organizaciones	Crear y editar organizaciones y uniones de directorios. Eliminar organizaciones solamente.	Cuentas → ficha Listar cuentas
Aprobador de organización	Aprobar solicitudes de nuevas organizaciones.	Sólo fichas predeterminadas de Contraseñas y Elementos de trabajo
Administrador del historial de infracciones de la organización	Crear, editar, eliminar y ejecutar informes del Historial de infracciones de la organización solamente.	Informes → ficha Ejecutar informes
Administrador de contraseñas	Enumerar, cambiar y reinicializar contraseñas de cuenta de usuario y de recursos.	Cuentas → fichas Listar cuentas y Buscar usuarios Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de contraseñas (requiere verificación)	Enumerar, cambiar y reinicializar contraseñas de cuenta de usuario y de recursos solamente. Las respuestas a las preguntas de autenticación de usuario deben validarse satisfactoriamente para que la acción tenga éxito.	Cuentas → fichas Listar cuentas y Buscar usuarios Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Realizar depuración	Acceder y ejecutar operaciones desde las páginas de depuración de Identity Manager. **Nota –** No es posible acceder a las páginas de depuración de Identity Manager desde el menú. Para acceder a las páginas de depuración, escriba la URL siguiente en el navegador: `http://<`*AppServerHost*`>:<`*Port*`>/idm/debug`	Todas las fichas predeterminadas
Administrador de directivas	Crear, editar y eliminar directivas.	Seguridad → ficha Directivas

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador del informe resumido de directivas	Crear, editar, eliminar y ejecutar informes resumidos de directivas.	Informes → fichas Ejecutar informes y Ver informes
Registrar componente del producto Identity Manager	Registrar una instalación de Identity Manager con Sun Microsystems o crear una etiqueta de servicio local.	Configurar → ficha Registro del producto
Administrador de reconciliaciones	Editar directivas de reconciliación y controlar tareas de reconciliación.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas (ver tarea de reconciliación) Recursos → fichas Listar recursos y Examinar índice de cuenta
Administrador de informes de reconciliación	Crear, editar, eliminar y ejecutar informes de reconciliación.	Informes → fichas Ejecutar informes (sólo Informe de índice de cuenta) y Ver informes
Administrador de peticiones de reconciliación	Administrar solicitudes de reconciliación.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → fichas Listar recursos (sólo funciones de listar y reconciliar) y Ver informes
Administrador de integración de Remedy	Editar la configuración de integración de Remedy (ver tareas, ejecutar sincronización de roles).	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Configurar → ficha Integración de Remedy
Cambiar nombre de usuario	Cambiar nombres de cuentas de usuario y de recursos existentes (listar todas las cuentas del ámbito, cambiar nombres de usuario).	Cuentas → fichas Listar cuentas y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de informes	Configurar parámetros de auditoría y ejecutar todos los tipos de informe (ver tareas, ejecutar sincronización de roles).	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Informes → fichas Ejecutar informes, Ver informes, Ejecutar análisis de riesgo y Ver análisis de riesgo Roles → fichas Listar roles y Buscar roles Configurar → ficha Auditoría
Administrador de reinicialización de contraseñas	Reinicializar contraseñas de cuenta de usuario y recursos.	Cuentas → fichas Listar cuentas y Buscar usuarios (sólo Reinicializar contraseña) Contraseñas → Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas (no hay tareas disponibles para los usuarios que tienen esta capacidad) Roles → fichas Listar roles y Buscar roles
Administrador de reinicialización de contraseñas (requiere verificación)	Reinicializar contraseñas de cuenta de usuario y recursos. Las respuestas a las preguntas de autenticación de usuario deben validarse satisfactoriamente para que la acción tenga éxito.	Cuentas → fichas Listar cuentas y Buscar usuarios Contraseñas → Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas (no hay tareas disponibles para los usuarios que tienen esta capacidad) Roles → fichas Listar roles y Buscar roles
Administrador de contraseñas de reinicialización de recursos	Reinicializar contraseñas de cuentas de administrador de recursos (con Administrar conexión → Reinicializar contraseña en el menú de acciones).	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → ficha Listar recursos

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de recursos	Crear, editar y eliminar recursos. Informe de usuario de recurso e Informe de grupo de recursos devuelven un error con los recursos fuera del ámbito. Editar directivas, parámetros y grupos de recursos globales. No puede administrar conexiones ni objetos de recurso.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → fichas Listar recursos, Listar grupos de recursos y Examinar índice de cuenta Configurar → Servidores de conectores
Aprobador de recursos	Aprobar asignaciones de recursos.	Todas las fichas predeterminadas de Contraseñas y Elementos de trabajo
Administrador de grupo de recursos	Crear, editar y eliminar grupos de recursos.	Recursos → ficha Listar grupos de recursos
Administrador de objetos de recursos	Ver, crear, modificar y eliminar objetos de recurso.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → ficha Listar recursos
Administrador de contraseñas de recursos	Cambiar y reinicializar contraseñas de cuentas proxy de recurso.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Recursos → ficha Listar recursos (Cambiar contraseña de recursos solamente con Administrar conexión → Cambiar contraseña en el menú de acciones)
Administrador de informes de recursos	Crear, editar, eliminar y ejecutar informes de recursos.	Informes → fichas Ejecutar informes y Ver informes
Administrador del historial de infracciones del recurso	Crear, editar, eliminar y ejecutar informes del historial de infracciones de recursos.	Informes → Ejecutar informes
Administrador de análisis de riesgo	Crear, editar, eliminar y ejecutar análisis de riesgo.	Informes → fichas Análisis de riesgo y Ver análisis de riesgo
Administrador de roles	Crear, editar, sincronizar y eliminar roles.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Aprobador de roles	Aprobar asignaciones de roles.	Todas las fichas predeterminadas de Contraseñas y Elementos de trabajo

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de informes de rol	Crear, editar, eliminar y ejecutar informes de recursos.	Informes → fichas Ejecutar informes y Ver informes Roles → ficha Listar roles
Ejecutar informe de detalle de revisión de acceso	Ejecutar el informe de detalle de revisión de acceso.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe de resumen de revisión de acceso	Ejecutar el informe de resumen de revisión de acceso.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe administrativo	Ejecutar informes de administrador.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe de análisis de directivas de auditoría	Ejecutar el informe de análisis de directivas de auditoría.	Tareas del servidor → sólo fichas Buscar tareas, Todas las tareas y Ejecutar tareas
Ejecutar informe de auditoría	Ejecutar informes de auditoría, de registro de auditoría, de cambios históricos de usuario, de registros de auditoría de usuarios individuales y de uso solamente.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe de atributos auditados	Ejecutar y ver el informe de atributos auditados.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe de Auditor	Ejecutar todos los informes del tipo Informe de AuditLog.	Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe de AuditLog	Ejecutar y ver los informes de AuditLog, Actividad de hoy y Actividad semanal.	Informes → Ejecutar informes
Ejecutar historial de infracciones de directivas de auditoría	Ejecutar y ver los informes del Historial de infracciones de la organización, Actividad de hoy y Actividad semanal.	Informes → Ejecutar informes
Ejecutar informe resumido de directivas	Ejecutar y ver el informe resumido de directivas.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar historial de infracciones de la organización	Ejecutar el informe del historial de infracciones de la organización.	Informes → ficha Ejecutar informes

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Ejecutar informes de reconciliación	Ejecutar y ver informes de índice de cuenta.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe de recursos	Ejecutar y ver informes de usuarios de recursos y de grupos de recursos.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar historial de infracciones del recurso	Ejecutar informes del historial de infracciones del recurso.	Informes → ficha Ejecutar informes
Ejecutar análisis de riesgo	Ejecutar y ver informes de análisis de riesgo.	Informes → fichas Ejecutar análisis de riesgo y Ver análisis de riesgo
Ejecutar informes de rol	Ejecutar y ver informes de rol.	Informes → fichas Ejecutar informes y Ver informes Roles → ficha Listar roles
Ejecutar informe de separación de tareas	Ejecutar y ver informes de separación de tareas.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informes de tareas	Ejecutar y ver informes de tareas.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe de acceso de usuario	Ejecutar y ver informes detallados de usuarios y de acceso de usuarios.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informes de usuario	Ejecutar y ver informes de usuario.	Informes → fichas Ejecutar informes y Ver informes
Ejecutar informe resumido de infracciones	Ejecutar el informe resumido de infracciones.	Informes → ficha Ejecutar informes

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Administrador de seguridad	Crear usuarios con capacidades, habilitar e inhabilitar usuarios, listar y controlar objetos de recurso, administrar claves de cifrado, administrar configuraciones de inicio de sesión y de auditoría, y administrar directivas.	Cuentas → fichas Listar cuentas (algunas acciones) y Buscar usuarios (informe de auditoría) Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas, Ejecutar tareas y Configurar tareas Informes → Ejecutar informes, Ver informes, Gráficos del panel, Ver paneles y Configurar informes Recursos → Listar recursos Configurar → fichas Auditoría y Almacén Seguridad → fichas Certificados, Iniciar sesión y Directivas Service Provider → Editar la configuración de búsqueda de usuarios
Administrador del informe de separación de tareas	Crear, editar, ejecutar, ver y eliminar informes de separación de tareas.	Informes → fichas Ejecutar informes y Ver informes
Administrador de roles de administrador de Service Provider	Administrar los roles de administrador de Service Provider y las reglas asociadas.	Seguridad → ficha Roles de administrador (Admin)
Administrador de Service Provider	Crear, editar y administrar usuarios y transacciones de proveedor de servicios; configurar la base de datos de transacciones y eventos rastreados.	Cuentas → ficha Administrar los usuarios de Service Provider Tareas del servidor → ficha Transacciones de proveedor de servicios Informes → ficha Gráficos del panel Informes → ficha Ver paneles Service Provider → fichas Editar configuración principal, Editar configuración de transacciones y Editar la configuración de búsqueda de usuarios

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Crear usuario de Service Provider	Crear cuentas de usuario para usuarios de proveedor de servicios (extranet).	Cuentas → ficha Administrar los usuarios de Service Provider
Eliminar usuario de Service Provider	Eliminar una cuenta de usuario de proveedor de servicios.	Cuentas → ficha Administrar los usuarios de Service Provider
Actualizar usuario de Service Provider	Actualizar una cuenta de usuario de proveedor de servicios.	Cuentas → ficha Administrar los usuarios de Service Provider
Administrador de usuarios de Service Provider	Administrar usuarios de proveedor de servicios (extranet).	Cuentas → ficha Administrar los usuarios de Service Provider
Ver usuario de Service Provider	Ver información de cuentas de usuario de proveedor de servicios (extranet).	Cuentas → ficha Administrar los usuarios de Service Provider
Administrador de informes de tareas	Crear, editar, eliminar, ejecutar y ver informes de tareas.	Informes → fichas Ejecutar informes y Ver informes
Anular asignación de usuario	Desasignar y desvincular cuentas de recursos existentes. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Anular asignación) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Desvincular usuario	Desvincular las cuentas de recursos existentes. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Desvincular) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Desbloquear usuario	Desbloquear cuentas de recursos de los usuarios existentes que admitan la función de desbloqueo. No incluye las operaciones en masa.	Cuentas → fichas Listar cuentas (sólo Desbloquear) y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas, Ejecutar tareas Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Actualizar usuario	Editar usuarios existentes e iniciar solicitudes de actualización de usuarios. Administrar tareas de servidor existentes.	Cuentas → fichas Listar cuentas y Buscar usuarios Tareas del servidor → fichas Buscar tareas, Todas las tareas, Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de informe de acceso de usuario	Crear, editar, eliminar, ejecutar y ver informes de acceso de usuario.	Informes → fichas Ejecutar informes y Ver informes
Administrador de cuenta de usuario	Todas las operaciones con usuarios, salvo asignar capacidades de usuario.	Cuentas → fichas Listar cuentas, Buscar usuarios, Extraer a archivo, Cargar desde archivo y Cargar desde recurso Contraseñas → fichas Modificar contraseña de usuario y Reinicializar contraseña de usuario Tareas del servidor → fichas Buscar tareas, Todas las tareas y Ejecutar tareas Roles → fichas Listar roles y Buscar roles
Administrador de informes de usuario	Crear, editar, eliminar, ejecutar y ver informes de usuario.	Informes → fichas Ejecutar informes y Ver informes
Ver aplicación	Listar roles del tipo aplicación y ver información sobre roles del tipo aplicación. No puede realizar acciones de modificación.	Roles → fichas Listar roles y Buscar roles
Ver activo	Listar roles del tipo activo y ver información sobre roles del tipo activo. No puede realizar acciones de modificación.	Roles → fichas Listar roles y Buscar roles
Ver rol de negocio	Listar roles de negocio y ver información sobre roles de negocio. No puede realizar acciones de modificación.	Roles → fichas Listar roles y Buscar roles
Ver rol de TI	Listar roles de TI y ver información sobre roles de TI. No puede realizar acciones de modificación.	Roles → fichas Listar roles y Buscar roles
Ver rol	Listar todos los tipos de roles y ver información sobre todos los roles. No puede realizar acciones de modificación.	Roles → fichas Listar roles y Buscar roles

TABLA D–1 Definiciones de capacidades basadas en tareas de Identity Manager *(Continuación)*

Capacidad	Permite al administrador/usuario	Ofrece acceso a estas fichas
Ver usuario	Ver los datos de cada usuario. No puede realizar acciones de modificación.	Cuentas → fichas Listar cuentas y Buscar usuarios
Administrador del informe resumido de infracciones	Crear, editar, eliminar y ejecutar informes resumidos de infracciones.	Informes → ficha Ejecutar informes
Administrador de Identity System (Sistema de identidad)	Realizar tareas que afectan a todo el sistema, como editar objetos de configuración del sistema, sincronizar roles, editar plantillas de adaptador de origen y ejecutar informes.	Tareas del servidor → fichas Buscar tareas, Todas las tareas, Ejecutar tareas, Administrar programación y Configurar tareas Informes → fichas Ejecutar informes, Ver informes, Gráficos del panel, Ver paneles y Configurar informes Recursos → Listar recursos Configurar → fichas Auditoría, Almacén, Plantillas de correo electrónico, Asignaciones de formularios y procesos, Servidores, Interfaz de usuario y Registro del producto Cumplimiento → Revisiones de acceso Seguridad → Certificados

Definiciones de capacidades funcionales

Las capacidades funcionales son capacidades basadas en tareas y otras capacidades funcionales.

- **Administrador de cuentas**
  - Administrador aprobador
    - Aprobador de organización
    - Aprobador de recursos
    - Aprobador de roles
  - Asignar capacidades de usuario
  - Acceso a SPML
  - Administrador de cuenta de usuario
    - Crear usuario
    - Eliminar usuario
      - Eliminar usuario de IDM

        - Desabastecer usuario
        - Anular asignación de usuario
        - Desvincular usuario
      - Inhabilitar usuario
      - Habilitar usuario
      - Administrador de contraseñas
        - Administrador de cambio de contraseñas
        - Administrador de reinicialización de contraseñas
      - Cambiar nombre de usuario
      - Desbloquear usuario
      - Actualizar usuario
      - Ver usuario
      - Importar usuario
- **Administrador de roles de Admin**
- **Administrador de Auditor**
  - Asignar directivas de auditoría
    - Asignar directivas de auditoría de organización
    - Asignar directivas de auditoría de usuario
  - Administrador de directivas de auditoría

    Usuarios de la vista de auditor
  - Administrador de revisiones de acceso periódicas de Auditor

    Administrador de exploraciones de acceso de Auditor
  - Administrador de informe de Auditor
  - Administrador de contraseñas
  - Administrador de cuenta de usuario
  - Asignar capacidades de usuario
- **Administrador de informe de Auditor**
  - Administrador del informe de detalle de revisión de acceso

    Ejecutar informe de detalle de revisión de acceso
  - Administrador del informe de resumen de revisión de acceso

    Ejecutar informe de resumen de revisión de acceso
  - Administrador de informe de análisis de directivas de auditoría

    Ejecutar informe de análisis de directivas de auditoría
  - Administrador de informe de atributos auditados

Ejecutar informe de atributos auditados

- Administrador del historial de infracciones de directivas de auditoría

  Ejecutar informe de historial de infracciones de directivas de auditoría
- Administrador del historial de infracciones de la organización

  Ejecutar informe de historial de infracciones de la organización
- Administrador de informes de resúmenes de directivas
- Administrador del historial de infracciones del recurso

  Ejecutar informe de historial de infracciones del recurso
- Ejecutar informe de Auditor
- Administrador del informe de separación de tareas

  Ejecutar informe de separación de tareas
- Administrador de informe de acceso de usuario

  Ejecutar informe de acceso de usuario
- Administrador del informe resumido de infracciones

- **Usuarios de la vista de auditor**

  Ver usuario
- **Administrador de cuentas en masa**
  - Administrador aprobador
  - Asignar capacidades de usuario
  - Administrador de cuentas de usuario en masa
    - Crear usuarios en masa
    - Eliminar usuarios en masa
      - Borrar masivamente usuarios de IDM
      - Desabastecimiento masivo de usuarios
      - Desasignación masiva de usuarios
      - Desvinculación masiva de usuarios
    - Inhabilitación de usuarios en masa
    - Habilitar usuarios en masa
    - Administrador de contraseñas
    - Cambiar nombre de usuario
    - Desbloquear usuario
    - Ver usuario
    - Importar usuario
- **Administrador de cambios de cuentas en masa**

- Administrador aprobador
- Asignar capacidades de usuario
- Administrador de cambios de cuentas de usuario en masa
  - Inhabilitación de usuarios en masa
  - Habilitar usuarios en masa
  - Actualización masiva de usuarios
  - Administrador de contraseñas
  - Cambiar nombre de usuario
  - Desbloquear usuario
  - Ver usuario

- **Administrador de recursos en masa**
  - Administrador de cambios de sincronización activa de recursos
  - Administrador de control de recursos de Active Sync
  - Administrador de grupo de recursos
- **Administrador de contraseñas de recursos en masa**
  - Administrador de cambio de contraseñas de recursos en masa
  - Administrador de reinicialización de contraseñas de recursos en masa
- **Administrador de capacidades**
- **Administrador de cambios de cuentas**
  - Administrador aprobador
  - Asignar capacidades de usuario
  - Administrador de cambios de cuentas de usuario
    - Administrador de contraseñas
      - Administrador de cambio de contraseñas
      - Administrador de reinicialización de contraseñas
    - Inhabilitar usuario
    - Habilitar usuario
    - Cambiar nombre de usuario
    - Desbloquear usuario
    - Actualizar usuario
    - Ver usuario
- **Configurar certificados**
- **Administrador de almacén de datos**
- **Consulta de almacén de datos**
- **Depurar**
- **Administrador de usuario final**

- **IDM Schema Configuration**
- **Administradores de importación/exportación**
- **Administrador de licencia**
- **Administrador de inicio de sesión**
- **Administrador de vista Meta**
- **Administrador de organización**
- **Administrador de contraseña (requiere verificación)**
  - Administrador de cambio de contraseñas (requiere verificación)
  - Administrador de reinicialización de contraseñas (requiere verificación)
- **Administrador de directivas**
- **Administrador del producto**
- **Administrador de reconciliaciones**

  Administrador de peticiones de reconciliación
- **Administrador de integración de Remedy**
- **Administrador de informes**
  - Administrador de informes administrativos

    Ejecutar informe administrativo
  - Administrador de informes de auditoría

    Ejecutar informe de auditoría
  - Administrador de informe de Auditor
    - Administrador del informe de detalle de revisión de acceso

      Ejecutar informe de detalle de revisión de acceso
    - Administrador del informe de resumen de revisión de acceso

      Ejecutar informe de resumen de revisión de acceso
    - Administrador de informe de análisis de directivas de auditoría

      Ejecutar informe de análisis de directivas de auditoría
    - Administrador de informe de atributos auditados

      Ejecutar informe de atributos auditados
    - Administrador de informe de AuditLog

      Ejecutar informe de AuditLog
    - Administrador del historial de infracciones de directivas de auditoría

      Ejecutar historial de infracciones de directivas de auditoría
    - Administrador del historial de infracciones de la organización

      Ejecutar historial de infracciones de la organización

- Administrador de informes de resúmenes de directivas

  Ejecutar informe resumido de directivas
- Administrador de informes de reconciliación

  Ejecutar de informes de reconciliación
- Administrador del historial de infracciones del recurso

  Ejecutar historial de infracciones del recurso
- Ejecutar informe de Auditor
  - Ejecutar informe de detalle de revisión de acceso
  - Ejecutar informe de resumen de revisión de acceso
  - Ejecutar informe de análisis de directivas de auditoría
  - Ejecutar informe de atributos auditados
  - Ejecutar informe de AuditLog
  - Ejecutar historial de infracciones de directivas de auditoría
  - Ejecutar historial de infracciones de la organización
  - Ejecutar informe resumido de directivas
  - Ejecutar historial de infracciones del recurso
  - Ejecutar informe de separación de tareas
  - Ejecutar informe de acceso de usuario
  - Ejecutar informe resumido de infracciones
- Administrador del informe de separación de tareas

  Ejecutar informe de separación de tareas
- Administrador de informe de acceso de usuario

  Ejecutar informe de acceso de usuario
- Administrador del informe resumido de infracciones

  Ejecutar informe resumido de infracciones

- Administrador de informes de reconciliación

  Ejecutar de informes de reconciliación
- Administrador de informes de recursos

  Ejecutar informe de recursos
- Administrador de análisis de riesgo

  Ejecutar análisis de riesgo
- Administrador de informes de rol

  Ejecutar informes de rol
- Administrador de informes de tareas

  Ejecutar informes de tareas
- Administrador de informes de usuario

Ejecutar informes de usuario

- Configurar auditorías

- **Administrador de recursos**
  - Administrador de cambios de sincronización activa de recursos
  - Administrador de control de recursos de Active Sync
  - Administrador de grupo de recursos
- **Administrador de objetos de recursos**
- **Administrador de contraseñas de recursos**
  - Administrador de cambio de contraseñas de recursos
  - Administrador de contraseñas de reinicialización de recursos
- **Administrador de roles**
  - Administrador de aplicaciones
  - Administrador de activos
  - Administrador de roles de negocio
  - Administrador de roles de TI
- **Administrador de seguridad**
- **Administrador de Service Provider**
  - Administrador de usuarios de Service Provider
  - Crear usuario de Service Provider
  - Eliminar usuario de Service Provider
  - Actualizar usuario de Service Provider
  - Ver usuario de Service Provider
- **Administrador de roles de administrador de Service Provider**
- **Administrador de Waveset**

Glosario

activo (rol) Uno de los cuatro tipos de rol de Identity Manager. El rol de activo se reserva (normalmente) a los recursos no conectados o los recursos no digitales que requieren abastecimiento manual, por ejemplo, teléfonos móviles y equipos portátiles. Los roles de activo no pueden asignarse directamente a los usuarios pero pueden asignarse a roles de TI y roles de negocio.

adaptador de recursos Componente de Identity Manager que ofrece un vínculo entre el motor de Identity Manager y el recurso.

Este componente permite a Identity Manager administrar las cuentas de usuarios en un determinado recurso (incluidas las capacidades de creación, actualización, eliminación, autenticación y exploración), así como utilizar ese recurso para una autenticación PTA (pass-through authentication).

administrador Persona que configura Identity Manager o es responsable de las tareas de funcionamiento, como, por ejemplo, la creación de usuarios y la administración del acceso a los recursos.

aprobación Proceso de conceder o denegar la solicitud de acceso de un usuario a un rol, un recurso o una organización. Un administrador de Identity Manager con permiso para ver y responder a un elemento de trabajo de aprobación se denomina *aprobador*.

aprobador Usuario con capacidades administrativas, responsable de aprobar o rechazar las solicitudes de acceso.

asignación de esquema. Asignación de atributos de cuenta de recurso a los atributos de cuenta de Identity Manager para un recurso.

Los atributos de cuenta de Identity Manager crean un vínculo común a los diversos recursos y se hace referencia a ellos en los formularios.

asistente de recursos. Herramienta de Identity Manager que le guía por el proceso de creación y modificación de recursos, incluida la configuración de los parámetros del recurso, los atributos de cuenta, la plantilla de identidad y los parámetros de Identity Manager.

atributo de cuenta Los atributos de cuenta permiten a los administradores de Identity Manager crear un conjunto estándar de nombres que se asignan a atributos en recursos administrados. Por ejemplo, un atributo de Identity Manager denominado *fullname* podría asignarse al atributo *displayName* en recursos de Active Directory, y al atributo *cn* en recursos LDAP. Cualquier cambio que se realice al atributo *fullname* del usuario en Identity Manager se transferirá a los atributos *displayName* y *cn* en las cuentas de recurso remoto del usuario.

autenticación Proceso por el que se certifica que un usuario específico tiene los privilegios adecuados sobre los recursos pertinentes en un determinado momento. Un usuario de Identity Manager con permiso para ver y responder a un elemento de trabajo de autenticación se denomina *autenticador*. Las reglas de Identity Manager determinan si un registro de derecho de usuario debe autenticarse manualmente, o si se puede aprobar o rechazar de forma automática.

autenticador Usuario que acepta la responsabilidad de certificar (*autenticar*) que un derecho de usuario es adecuado. Un autenticador posee en Identity Manager privilegios extendidos que se necesitan para administrar los derechos de usuario que requieren autenticación.

autenticar Una acción realizada por un autenticador durante una revisión de acceso para confirmar que un derecho de usuario es adecuado.

capacidad Grupo de derechos de acceso para las cuentas de usuario que controla las acciones realizadas en Identity Manager el control de acceso de nivel bajo de Identity Manager.

cuenta de adaptador de recursos Credenciales utilizadas por un adaptador de recursos de Identity Manager para acceder a un recurso administrado.

cuenta de usuario Cuenta creada mediante Identity Manager.

Puede designar una cuenta de Identity Manager o una cuenta de un recurso remoto administrado por Identity Manager. Configurar una cuenta de usuario es un proceso dinámico. La información y los campos que deben completarse dependen de los recursos proporcionados directa o indirectamente al usuario mediante un asignación de rol.

delegación El proceso de asignar temporalmente elementos de trabajo futuros a uno o varios usuarios durante un determinado periodo de tiempo.

derecho Véase *derecho de usuario*

derecho de usuario En Identity Manager, un privilegio de acceso auditable concedido a un usuario sobre un recurso o un sistema que impone restricciones de acceso.

directiva Establece limitaciones para las cuentas de Identity Manager.

Las directivas de Identity Manager definen opciones de usuario, contraseña y autenticación y están vinculadas a organizaciones o usuarios. Las directivas de contraseñas de recurso y de ID de cuenta definen reglas, palabras permitidas y valores de atributo y están vinculadas a recursos individuales.

editor de procesos de negocio (BPE, del inglés Business Process Editor). Vista gráfica de formularios, reglas y flujo de trabajo de Identity Manager que se incluía con las versiones de Identity Manager anteriores a la 7.0. BPE ha sido sustituida por Identity Manager IDE en las versiones actuales de Identity Manager. Consulte Glosario

elementos de trabajo Una solicitud de acción generada por un flujo de trabajo, formulario o procedimiento de Identity Manager. Aprobaciones, aprobaciones de cambio, autenticaciones y remediaciones son cuatro tipos de elementos de trabajo.

esquema Lista de atributos de cuenta de usuario para un recurso.

flujo de trabajo. Proceso lógico repetitivo durante el cual los documentos, la información y las tareas se transfieren de un participante a otro. Los flujos de trabajo de Identity Manager se componen de varios procesos que controlan la creación, actualización, habilitación, inhabilitación y eliminación de cuentas de usuario.

formulario Objeto asociado a una página Web que contiene reglas sobre cómo el explorador Web debe mostrar los atributos de vista de usuario en esa página. Los formularios pueden incorporar lógica empresarial y se utilizan a menudo para manipular datos antes de presentárselos al usuario.

grupo de recursos Conjunto de recursos utilizado para ordenar la creación, eliminación y actualización de las cuentas de recurso de un usuario.

Identity Manager IDE Identity Manager Integrated Development Environment (Identity Manager IDE) es una aplicación que permite ver, personalizar y depurar objetos de Identity Manager en su implantación. Identity Manager IDE está disponible como un complemento NetBeans.

interfaz de administrador Interfaz de usuario que los administradores utilizan para configurar y administrar Identity Manager.

interfaz de usuario En Identity Manager, la interfaz de usuario permite a los usuarios sin capacidades administrativas realizar una serie de tareas de autoservicio, como el cambio de sus contraseñas, la definición de respuestas para las preguntas de autenticación o la administración de asignaciones delegadas. También se denomina *interfaz de usuario final*.

organización Contenedor de Identity Manager utilizado para habilitar la delegación administrativa.

Las organizaciones definen el ámbito de las entidades (como las cuentas de usuario, los recursos y las cuentas de administrador) que un administrador puede controlar o administrar. Las organizaciones ofrecen un contexto de ubicación, especialmente para los fines administrativos de Identity Manager.

organización virtual Organización definida dentro de una unión de directorios. *Véase* unión de directorios.

plantilla de identidad Define el nombre de cuenta de recurso del usuario.

reconciliación Una función de Identity Manager que compare periódicamente las cuentas de recursos de Identity Manager con las cuentas situadas en los propios recursos. La reconciliación correlaciona los datos de cuenta y resalta las diferencias.

recurso Un recurso de Identity Manager almacena información sobre cómo conectarse a un recurso remoto o un sistema en el que se crean las cuentas. Entre los recursos remotos a los que Identity Manager ofrece acceso se incluyen los administradores de seguridad de sistemas centrales (mainframe), bases de datos, servicios de directorio, aplicaciones, sistemas operativos, sistemas ERP, plataformas de mensajería y más.

regla Objeto del repositorio de Identity Manager que contiene una función escrita en los lenguajes XPRESS, XML Object o JavaScript. Las reglas ofrecen mecanismos para almacenar las variables estáticas o lógicas utilizadas frecuentemente para reutilizarlas en formularios, flujos de trabajo y roles.

remediación El proceso de corregir las infracciones de cumplimiento detectadas por la función de auditoría de Identity Manager. Identity Manager audita datos en toda la empresa para asegurar el cumplimiento de las directivas y normativas internas y externas. Un usuario con permiso para ver y responder a las infracciones de directivas se denomina *remediador*.

remediador Usuario de Identity Manager que se especifica como remediador asignado para una directiva de auditoría.

Cuando Identity Manager detecta una infracción de cumplimiento que requiere remediación, crea un elemento de trabajo de remediación y lo envía a la lista de elementos de trabajo del remediador.

revisión de acceso Proceso auditado que permite a los administradores u otros responsables revisar y certificar los privilegios de acceso de los usuarios. Los registros de derecho de usuario se pueden aprobar o rechazar de forma automática o autenticarse manualmente. Véase también *autenticación*.

revisión de acceso periódica Una revisión de acceso que se efectúa a intervalos periódicos, por ejemplo, cada trimestre.

rol Un rol es un objeto de Identity Manager que permite agrupar los derechos de acceso a los recursos y asignarlos eficazmente a los usuarios. Los roles se clasifican en cuatro tipos: roles de negocio, roles de TI, roles de aplicación y activos. Los roles de TI, de aplicación y activos organizan los derechos de recursos en grupos. Estos tres grupos se asignan a roles de negocio, que permiten a los usuarios acceder a los recursos que necesitan para realizar su trabajos.

rol de administrador Un conjunto único de capacidades para cada conjunto de organizaciones asignadas a un usuario administrativo.

Rol de aplicación Uno de los cuatro tipos de rol de Identity Manager. El rol de aplicación es una colección de recursos, o grupos de recursos, o aplicaciones específicas en recursos, que los usuarios necesitan para realizar sus trabajos. Los roles de aplicación no se pueden asignar directamente a los usuarios, pero se pueden asignar a roles de TI y de negocio.

Rol de negocio Uno de los cuatro tipos de rol de Identity Manager. Los roles de negocio sirven para organizar en grupos los derechos de acceso que necesitan las personas encargadas de tareas similares en una organización. Un rol de negocio está formado por uno o varios roles de autenticación, roles de aplicación o roles de TI. Los roles de negocio están concebidos para asignarse directamente a los usuarios.

Rol de TI Uno de los cuatro tipos de rol de Identity Manager. El rol de TI es una colección de roles (activos, aplicaciones u otros recursos de TI anidados), así como recursos o grupos de recursos. En algunas configuraciones, los roles de TI se pueden asignar directamente a los usuarios, pero normalmente se asignan a roles de negocio, que a su vez se asignan a usuarios.

tarea de autenticación Recopilación lógica de revisiones de derechos de usuario que requieren autenticación. Los derechos de usuario se agrupan en una sola tarea de autenticación si se asignan al mismo autenticador y se generan a partir de la misma instancia de revisión de acceso.

tiempo de espera de escalada Intervalo de tiempo que se especifica para una solicitud de elemento de trabajo cuyo propietario asignado debe responder antes de que el proceso de Identity Manager la envíe al destinatario asignado.

unión de directorios Conjunto de organizaciones relacionadas jerárquicamente que refleja el conjunto real de contenedores jerárquicos de recursos de directorio. Cada organización de una unión de directorios constituye una *organización virtual*.

usuario Persona que tiene una cuenta del sistema Identity Manager. Los usuarios pueden tener diversas capacidades en Identity Manager. Quienes poseen capacidades ampliadas son *administradores* de Identity Manager.

usuarios de proveedor de servicios Usuarios de extranet o clientes de un proveedor de servicios que se diferencian del personal o los usuarios de la intranet de la empresa proveedora de servicios.

Índice

B

C

D

E

F

G

J

L

M

N

O

P

R

S

T

U

V

W