Sun Java™ System

Identity Installation Pack 2005Q4M3 SP4
Notas de la versión

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
EE.UU.

Referencia: 820-4368-10

Contenido

Anexos a la documentación y correcciones

Notas sobre Identity Installation Pack 2005Q4M3 SP4

Antes de instalar o actualizar el software Sun Java™ System Identity Installation Pack, consulte la sección “Notas sobre la instalación y la actualización” en la página 65.

Instalación

Utilice Identity Installation Pack 2005Q4M3 para instalar Sun Java™ System Identity Manager, Sun Java™ System Identity Auditor y Sun Java™ System Identity Manager Service Provider Edition (SPE) en un entorno nuevo o como una actualización.

Puede actualizar Identity Manager, Identity Auditor e Identity Manager SPE a partir de la versión 5.0 de Identity Manager o cualquier de sus paquete de servicios hasta 5.0 SP6. Si tiene instalada una versión anterior de Identity Manager, primero debe actualizarla a la versión 5.0 de Identity Manager.

Consulte las instrucciones detalladas de instalación del producto en *Identity Manager Upgrade* e *Identity Install Pack Installation*.

Nota La versión mínima de Java admitida es la 1.4.2.

Software y entornos admitidos

En esta sección se enumeran los programas y entornos compatibles con el software del producto Identity:

- Sistemas operativos
- Servidores de aplicación
- Exploradores
- Servidores de base de datos
- Entorno de tiempo de ejecución Java
- Puerta de enlace de Sun Identity Manager
- Recursos admitidos
- Servidores Web

Nota Como los desarrolladores de software a menudo realizan nuevas versiones, actualizaciones y correcciones al software, la información aquí incluida cambia con frecuencia. Consulte las actualizaciones en las notas de la versión antes de continuar con la instalación.

Sistemas operativos

- AIX 4.3.3, 5.2, 5L v5.3
- HP-UX 11i v1, 11i v2
- Microsoft Windows 2000 SP3 o versión posterior
- Microsoft Windows 2003
- Solaris 8, 9, 10 Sparc y x86d
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Novell SuSE Linux Enterprise Server 9 SP1

Servidores de aplicación

Con Identity Manager se debe utilizar un servidor de aplicación Servlet 2.2 compatible e instalado con la plataforma Java incluida (excepto en los casos siguientes):

- Apache Tomcat
  - Versión 4,1.x (con JDK 1.4.2)
  - Versión 5.0.x (con JDK 1.4.2)
- BEA WebLogic® Express 8.1 (con JDK 1.4.2)
- BEA WebLogic® Express 8.1 (con JDK 1.4.2)
- IBM WebSphere® 6.0
- IBM WebSphere® Application Server - Express 5.1.1 (con JDK 1.4.2)
- Sun™ ONE Application Server 7
- Sun Java™ System Application Server Platform Edition 8
- Sun Java™ System Application Server Platform Edition and Enterprise Edition 8.1

Nota Si el servidor de aplicaciones actual no admite JDK 1.4.2, póngase en contacto con el distribuidor para analizar las consecuencias de actualizar a uno que sí lo admita antes de instalar Identity Installation Pack 2005Q4M3 SP4.

Exploradores

- Microsoft Internet Explorer 5.x y posterior
- Safari v2.0 y posterior para Mac OS X 10.4.2 y posterior
- Mozilla 1.78 (con JRE 1.5)
- Firefox 1.04, 1.05, 1.06 (con JRE 1.5)

Servidores de repositorio de bases de datos

- IBM® DB2® Universal Database para Linux, UNIX® y Windows® (Versión 7.x, 8.1, 8.2)
- Microsoft SQL Server™ 2000
- MySQL™ 4.1
- Oracle 9i® y Oracle Database 10g, 10gR1 y 10gR2®

Puerta de enlace de Sun Identity Manager

Si tiene intención de configurar Windows Active Directory, Novell NetWare, Novell GroupWise, Exchange 5.5, Remedy, Lotus Domino o RSA ACE/Server, debe instalar la Puerta de enlace de Sun Identity Manager.

Recursos admitidos

El software del producto Identity admite estos recursos.

Gestión de las relaciones con los clientes (CRM)

- Siebel 6.2, 7.0.4, 7.7, 7.8

Bases de datos

- IBM® DB2® Universal Database para Linux, UNIX® y Windows® (7.x, 8.1, 8.2)
- Microsoft® Identity Integration Server (MIIS) 2003
- Microsoft SQL Server 2000
- MySQL™ 4.1.x, 5.x
- Oracle® 8i, 9i, 10g Release 1, 10g Release 2
- Sybase Adaptive Server® 12.x

Directorios

- LDAP v3
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory on Novell NetWare 5.1, 6.0
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java™ System Directory Server 5 2004Q2, 2005Q1

Notas

- Aunque Identity Manager se ha probado en Sun™ ONE Directory Server y Open LDAP, puede funcionar con servidores LDAP compatibles con la versión 3 sin modificar el adaptador de recursos.
- Sun Java™ System Directory Server 5 2005Q1 requiere instalar un parche de Directory Server retro changelog cuando se utiliza Active Sync. Este parche sólo se necesita para las repeticiones “normales” (no para repeticiones MMR).

ERP (Planificación de recursos empresariales)

- Oracle Financials on Oracle Applications 11.5.9, 11.5.10, 12
- Peoplesoft® PeopleTools 8.1 a 8.4.2 con HRMS 8.0 a 8.8
- SAP® R/3 v4.5, v4.6
- SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
- SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
- SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)
- mySAP ERP ECC 5.0 (SAP 5.0)

Servicio de asistencia

- Remedy® Help Desk 4.5, 5.0

Plataformas de mensajes

- Blackberry RIM Enterprise Server 4+ (usa adaptador de secuencia de comandos de Windows genérico)
- Sun Java System Messaging and Calender Service
- Lotus Notes® 5.0, 6.5, 6.5.4 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 5.x, 6.0

Nota Microsoft Exchange 2000 y 2003 se administran a través de los recursos de Microsoft Windows Active Directory 2000 y 2003.

Cola de mensajes

- JMS Message Queue Listener

Sistemas operativos

- HP OpenVMS 7.2
- HP-UX 11.0, 11i v1, 11i v2
- IBM AIX® 4.3.3, 5.2, 5L v5.3
- IBM OS/400® V4r3, V4r5, V5r1, V5r2, V5r3, V5r4
- Microsoft Windows® NT® 4.0
- Microsoft Windows® 2000, 2003
- Adaptador de secuencia de comandos de Windows genérico (usa puerta de enlace)
- Red Hat Linux 8.0, 9.0
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Sun Solaris™ 8, 9, 10
- SuSE Enterprise 9

Gestores de seguridad

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Host de secuencia de comandos
- INISafe Nexess 1.1.5
- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® 5.1, 6.0 para UNIX
- eTrust CA-Top Secret® Security 5.3

Control de acceso Web

- IBM Tivoli® Access Manager 4.x, 5.1
- Netegrity® Siteminder® 5.5
- RSA® ClearTrust® 5.0.1
- Sun™ ONE Identity Server 6.0, 6.1, 6.2
- Sun™ Java System Identity Server 2004Q2
- Sun™ Java System Access Manager 6 2005Q1, 7 2005Q4

Servidores web

Nota Identity Manager no requiere la integración entre un servidor de aplicación y un servidor web. Si desea lograr un mejor equilibrio de la carga y aumentar la seguridad (a través del protocolo https), puede elegir un servidor Web.

- Apache 1.3.19
- iPlanet 4.1
- Microsoft Internet Information Server (IIS) 4.0, 5.0
- Sun™ ONE Web Server 6

Software suspendido

Identity Manager dejará de ser compatible con los siguientes paquetes de software que se utilizan como servidores de aplicación, repositorios de base de datos y recursos administrados. No obstante, se admitirán hasta que aparezca la siguiente versión principal de Identity Manager. Si tiene preguntas relacionadas con la implementación de versiones más recientes de estos paquetes de software, póngase en contacto con el representante del servicio al cliente o con el servicio de asistencia al cliente.

Servidores de base de datos

- Oracle 8*i*
- IBM DB2 Universal Database para Linux, UNIX y Windows 7.0

Sistemas operativos

- Solaris 7

Recursos

- Microsoft Exchange 5.5
- IBM DB2 7.0

Compatibilidad oficial del adaptador de recursos de NT4

Dado el esfuerzo continuado por ofrecer funciones nuevas y mejoradas en las versiones más recientes, debe aceptar esto como un aviso de obsolescencia de las versiones anteriores. La obsolescencia del producto se debe al cese de la compatibilidad de Microsoft con el sistema operativo NT4. Aunque Sun no admita el sistema operativo NT, esto no afectará al resto de funcionalidades de adaptador de NT. Sun se compromete a garantizar la compatibilidad del sistema operativo NT hasta finales de 2006.

Compatibilidad API

La Interfaz de programación de aplicaciones (API) de Identity Manager v6.0 incluye las clases públicas (y cualquier método público o protegido, o campo de una clase pública) que aparecen en la tabla siguiente.

Tipo de API	Nombres de clase
SesiÃ³n	com.waveset.msgcat.* com.waveset.util.* com.waveset.object.* com.waveset.exception.* com.waveset.expression.* com.waveset.config.* com.waveset.session.SessionUtil com.waveset.session.ScriptSession com.waveset.session.SessionFactory com.waveset.session.Session com.waveset.session.UserViewConstants
Adaptador	com.waveset.adapter.* com.waveset.util.Trace
Directiva	com.waveset.policy.PolicyImplementation com.waveset.policy.StringQualityPolicy
Tarea	com.waveset.task.Executor com.waveset.task.TaskContext
IU	com.waveset.ui.FormUtil com.waveset.ui.util.RequestState com.waveset.ui.util.html.*
autenticación	com.waveset.provision.WorkflowServices com.waveset.session.WorkflowServices com.waveset.workflow.WorkflowApplication com.waveset.workflow.WorkflowContext

Identity Manager SPE también incluye las clases públicas que se indican en la tabla siguiente.

Tipo de API	Nombres de clase
SPE	com.sun.idm.idmx.api.IDMXContext com.sun.idm.idmx.api.IDMXContextFactory com.sun.idm.idmx.auditor.* com.sun.idm.idmx.txn.TransactionPersistentStore com.sun.idm.idmx.txn.TransactionQuery com.sun.idm.idmx.txn.TransactionSummary

Estas clases son las únicas que se admiten oficialmente. Si está utilizando clases que no aparecen en las tablas, póngase en contacto con el servicio al cliente para saber si se requiere la migración a una clase admitida.

API desaprobado

“En API desaprobadas, en la página 143, se enumeran todas las interfaces de programación de aplicaciones de Identity Manager que se han desaprobado en esta versión y las alternativas (si existen).

Obsolescencia

El compromiso de desarrollo de nuestros productos tiene por objeto satisfacer los requisitos de calidad que exigen nuestros clientes. Dado el esfuerzo continuado por ofrecer funciones nuevas y mejoradas en la versión más reciente de Identity Manager (v6), debe aceptar esto como un aviso de obsolescencia de las versiones anteriores. Para evitar el uso de versiones que no estén incluidas en ningún plan de mantenimiento, se recomienda empezar a planificar la migración lo antes posible.

Fin del periodo de servicio (EOSL) de asistencia del software

Durante el periodo EOSL, se ofrece asistencia en dos fases: fase de asistencia completa y fase de asistencia limitada. La duración de la fase de asistencia completa varía según el producto. Consulte la Tabla 1 que aparece a continuación para ver la lista de fases de asistencia completa y limitada según el producto.

Fase de asistencia completa

Durante la fase de asistencia completa, Sun proporciona a los clientes todos los servicios de asistencia contenidos en el contrato de servicios de Sun suscrito por el cliente (incluidos los descritos en la lista de servicios aplicable) según lo establecido en: `http://www.sun.com/service/servicelist/`. No obstante, al recibirse el anuncio de obsolescencia de un producto de software, los clientes no tendrán acceso a actualizaciones de software para ese producto.

Fase de asistencia limitada

Durante la fase de asistencia limitada, Sun proporciona a los clientes todos los servicios de asistencia contenidos en el contrato de servicios de Sun suscrito por el cliente (incluidos los descritos en la lista de servicios aplicable) según lo establecido en: `http://www.sun.com/service/servicelist/`. No obstante, los clientes no podrán enviar informes de errores del software ni recibir parches de Sun. Como ocurre durante la fase de asistencia completa, al recibirse el anuncio de obsolescencia de un producto de software, los clientes no tendrán acceso a actualizaciones de software para ese producto.

Notas sobre el fin del periodo de servicio para productos Identity Manager

A continuación se ofrecen fechas concretas. Póngase en contacto con el representante del servicio al cliente o con el servicio de asistencia al cliente si desea solicitar ayuda para planificar la actualización a Identity Manager 6.0 (2005Q4M3).

- Identity Manager 2005Q4M3 dispondrá de asistencia completa hasta el 25 de mayo de 2008, con asistencia limitada hasta el 25 de mayo de 2012.
- Identity Manager 2005Q3M1, que incluye Identity Manager 5.5 e Identity Auditor 1.5, (incluidos todos los paquete de servicios) contará con asistencia completa hasta el 11 de agosto de 2007 y con asistencia limitada hasta el 11 de agosto de 2011.
- Identity Manager 5.0 (incluidos todos los paquete de servicios) contará con asistencia completa hasta el 11 de agosto de 2007 y con asistencia limitada hasta el 11 de agosto de 2011.
- Identity Manager 2005Q3M3 se admitirá hasta octubre de 2006, sin paquete de servicios adicionales.
- Identity Manager 2005Q1M3 se admitirá hasta marzo de 2006, sin paquete de servicios adicionales.
- Lighthouse 4.1 (incluidos todos los paquete de servicios) será compatible hasta marzo de 2006, sin paquete de servicios adicionales.

- Lighthouse 4.0, incluido SP1, quedará obsoleto en septiembre de 2004.
- Lighthouse 3.1 (incluidos todos los paquete de servicios) dejará de ser compatible en septiembre de 2005.
- Lighthouse 2.0 (incluidos todos los paquete de servicios) dejará de ser compatible en mayo de 2004.
- Lighthouse 1.x (incluido 1.6) quedará obsoleto en mayo de 2004.

Identity Installation Pack 2005Q4M3 Funciones de SP4

Antes de instalar o actualizar el software Sun Java™ System Identity Installation Pack, consulte la sección “Notas de instalación y actualización” en las notas de la versión y cualquier documentación suministrada con el paquete de servicios más reciente de Identity Manager 2005Q4M3.

Funciones nuevas y defectos corregidos en esta versión

En esta sección se proporciona un resumen y detalles de las nuevas funciones de Identity Installation Pack 2005Q4M3 SP4. Consulte los detalles en las secciones correspondientes de este capítulo.

Interfaz de administrador

- Al visualizar las **Tareas del servidor**, la columna **Hora de inicio** de la ficha **Todas las tareas** se ordenará ahora cronológicamente de forma correcta. Anteriormente, la columna **Hora de inicio** no se ordenaba correctamente. (ID-16783)
- Al realizar una búsqueda de usuario en la ficha **Listar cuentas** (Cuentas > Listar cuentas), la función de búsqueda enumerará ahora los usuarios solamente una vez por organización. Anteriormente, el mismo usuario aparecía varias veces por organización en los resultados de búsqueda. (ID-16795)

  También: consulte la sección *Problemas detectados* de la página 22 con respecto a un determinado problema con la tabla de árbol de cuentas de la ficha Listar cuentas.
- Al realizar una búsqueda por usuario en la tabla de árbol de cuentas, el atributo de administrador del usuario devuelto muestra ahora el nombre completo del administrador. Anteriormente, sólo se mostraba el ID del administrador. (ID-14645)
- La columna **Estado** de la página **Modificar resultados de contraseña de usuario** se ha eliminado. Además, la columna **Estado** se ha eliminado de estas páginas: **Resultados de Cambiar las respuestas**, **Change All Results** (Cambiar todos los resultados) y **Resultados del cambio de contraseña**. La columna **Estado** no mostraba ninguna información y no tenía ninguna finalidad. (ID-16889)
- Es posible borrar el valor del tipo de campo **DatePicker** en los formularios. (ID-17022)

- Ahora la tabla **Pendiente de aprobación** se puede ordenar. Anteriormente, los usuarios con aprobaciones pendientes no podían ordenar esta tabla. En su lugar, aparecía el mensaje “No se puede obtener la página de resultados, ninguna ID de tarea o resultado”. (ID-17304)
- El componente de presentación de texto ahora indica `autocomplete="off"` en los campos de entrada donde la propiedad de presentación `autocomplete` se ha configurado en `off`. (Si se configura `autocomplete` en `off`, se impide que los navegadores inviten a almacenar las credenciales del usuario en el equipo.)

  Esta personalización se puede efectuar en XPRESS agregando la propiedad de presentación. Con un valor distinto a `off` se impide que se suministre el atributo autocomplete (lo que equivale a no definir la propiedad). (ID-17045)
- Se ha detectado y corregido una vulnerabilidad de secuencia de comandos entre sitios en las páginas siguientes (ID-17241):
  - task/taskLaunch.jsp
  - user/processLaunch.jsp
  - user/requestLaunch.jsp

Auditoría

- Los registros de auditoría para la creación de roles ahora ofrecen más información sobre el rol (por ejemplo, recursos asignados, subroles, súper roles y atributos de roles) en la sección de cambios del informe de auditoría. (ID-16327)

Sincronización de contraseña

- Debido a un cambio de comportamiento introducido en Microsoft Windows Server 2003 SP2, ha sido necesario realizar un cambio en el DLL PasswordSync de Identity Manager (`lhpwic.dll`). En SP2, las notificaciones de cambio de contraseña enviadas de Windows a PasswordSync pueden incluir datos de cuentas de equipo con un formato incorrecto. Esto puede provocar que PasswordSync devuelva una excepción. Finalmente, también puede provocar que el componente Local Security Authority Subsystem (LSASS) de Microsoft se bloquee, por lo que será necesario reiniciar el controlador de dominio.

  Puesto que PasswordSync no procesa datos de cuentas de equipo (sólo se procesan cuentas de usuario), el DLL PasswordSync se ha actualizado para descartar todas las notificaciones de cambio de cuentas de equipo en cuanto se reciben.

  Las cuentas de equipo Windows finalizan con el símbolo del dólar “$”. Por tanto, tenga en cuenta que PasswordSync no procesará ninguna cuenta que finalice con el símbolo $, incluidas las cuentas de usuario que puedan finalizar con el símbolo $. (ID-17245)

- Se ha actualizado el registro de seguimiento de PasswordSync. Cuando PasswordSync/JMS envía una notificación de cambio de contraseña de Windows Active Directory a Identity Manager y el usuario no existe en Identity Manager, el registro de seguimiento registrará ahora el mensaje correspondiente. Anteriormente, en estas circunstancias PasswordSync devolvía una excepción de puntero nulo sin ninguna explicación. (ID-16920)
- Al iniciarse un controlador de dominio Active Directory en el modo “Directory Service Restore”, ya no se producirá un ciclo de reinicio continuo si PasswordSync (`lhpwic.dll`) se bloquea. (ID-16695)
- PasswordSync se ha actualizado para impedir que se produzcan errores de falta de identificador en controladores de dominio Active Directory que ejecuten PasswordSync (`lhpwic.dll`). Cuando se actualizan cuentas de equipo en un dominio, el controlador de dominio envía incorrectamente una notificación de actualización de contraseña al DLL PasswordSync de Identity Manager. En consecuencia, el DLL no cerraba correctamente los identificadores de búsqueda. (ID-16495)

  También: se ha solucionado un problema de PasswordSync que provocaba pérdidas de identificador. (ID-16827)
- Una nueva entrada de registro de Windows generará un archivo de volcado si el DLL PasswordSync devuelve una excepción.

  Nombre clave: `dumpFilebase`

  Tipo: `REG_SZ`

  Esta clave se debe añadir a los controladores de dominio Windows que ejecuten PasswordSync. La clave de registro se debe definir en la ruta de directorio completamente calificada en la que se debe escribir el volcado de memoria, por ejemplo: `c:\temp`

  Si se define el valor de registro, el volcado de memoria se escribirá cada vez que se produzca una excepción durante el procesamiento de la contraseña.

  Nota: En Windows 2000 server (cualquier paquete de servicios), también debe instalar en el directorio configurado `DbgHelp.dll`, que proporciona Microsoft. La versión mínima de este archivo debe ser 5.1. Descargue este archivo aquí:

  `http://www.microsoft.com/whdc/DevTools/Debugging/default.mspx`

  Si no se instala el archivo DbgHelp.dll, no se generarán volcados en Windows 2000.

  Los nombres de los archivos de volcado tendrán el siguiente formato:

  `lhpwic-AAAAMMDD-HHmm-xxxxx.dmp`

  Con este nombre, `AAAAMMDD` corresponderá a la fecha del volcado, `HHmm` será la hora del volcado (formato de 24 horas) y `xxxxx` será el número de subprocesos de la aplicación.

  Tenga en cuenta que es necesario eliminar manualmente los archivos de volcado. El tamaño de estos archivos puede variar entre 20 MB y más de 100 MB, en función del tamaño del proceso de Local Security Authority Subsystem (LSASS) de Windows. Con el paso del tiempo, los sistemas con espacio de disco limitado podrían llenarse si no se eliminan estos archivos de volcado. (ID-17552)

Reconciliación

- Durante la reconciliación, se podría producir una excepción de puntero nulo al realizar búsquedas por ID de cuenta. Este problema se ha solucionado. (ID-17186)

Informes

- Los siguientes eventos se incluirán ahora en los informes de registro de auditoría, tal como el “Informe de actividad de hoy”:
  - Intentar crear un usuario con un ID de usuario o contraseña inexistente
  - Intentar crear un usuario con un rol inexistente (así como intentar asignar un rol inexistente a un usuario existente)
  - Intentar crear un usuario que infrinja la directiva de ID de cuenta
  - Intentar crear un usuario asignado con un recurso inaccesible (así como intentar asignar un recurso inaccesible a un usuario existente)
  - Intentar eliminar usuarios inexistentes

  Estos eventos se escribirán también en el registro del sistema.

  Anteriormente, los intentos fallidos de crear y eliminar usuarios sólo se escribían en el registro del sistema. (ID-13284)

- Identity Manager ahora admite el tipo de datos CLOB para acctAttrChanges cuando se utiliza una base de datos Oracle como repositorio de Identity Manager.

  La ventaja de utilizar CLOB (en lugar del tipo de datos predeterminado VARCHAR(4000)) es que permite registrar muchos más cambios; sin embargo, también dificulta la consulta de esta columna debido a la naturaleza propietaria de las rutinas de acceso de CLOB.

  Para habilitar conjuntos de cambios más amplios, debe cambiar el tipo de columna log.acctAttrChanges a CLOB (desde VARCHAR(4000)) y ajustar como corresponde el atributo maxLogAcctAttrChangesLength del objeto de configuración RepositoryConfiguration. (ID-15326)

Recursos

- Debido al adaptador de recursos Solaris, los usuarios deben cambiar ahora sus contraseñas en el siguiente inicio de sesión. Para habilitar esta función, añada `expirePassword` a la columna de atributos de usuario de Identity System del mapa de esquema y `force_change` a la columna de atributos de usuario de recurso. Este tipo de atributo se debe definir como cadena. (ID-17032, ID -17146)
- El adaptador de recursos de Oracle se ha actualizado para proporcionar un mensaje de error más detallado cuando el adaptador no pueda añadir, modificar o eliminar una responsabilidad de usuario. El adaptador incluye ahora la responsabilidad que no podía actualizar. (ID-16656)
- El adaptador de recursos de Sun Access Manager puede conectarse ahora a Access Manager en el modo SSL. Anteriormente, al comprobar la configuración del adaptador de recursos, los administradores recibían un error de imposibilidad de crear AuthContext (“AuthContext cannot be created”). (ID-16454)
- La puerta de enlace ADSI de Microsoft se ha actualizado. Si se utiliza un recurso de Active Directory para autenticar un usuario que inicie sesión en Identity Manager, la UI de Identity Manager solicitará ahora al usuario cambiar su contraseña si la contraseña de Windows del usuario ha caducado. Antes, el usuario sencillamente recibía un mensaje de error indicando que su contraseña había caducado. (ID-16681)
- Ha cambiado el tipo de acceso a los servidores de Remedy. La puerta de enlace ya no depende de la versión 4.5 de las bibliotecas de API de Remedy. Los clientes deberán situar ahora las bibliotecas de Remedy en el directorio de la puerta de enlace. Estas bibliotecas se hallan en el servidor de Remedy. (ID-17361, ID-16551)
- Con este paquete de servicios, Identity Manager es compatible con las versiones 6.3 y 7.0 de Remedy. Sin embargo, entre estas versiones existen abundantes diferencias fundamentales en cuanto a datos de ejemplo, valores predeterminados y configuración inmediata. Por ejemplo, el esquema “ticket” se denomina HPD:HelpDesk en la versión 6.3, mientras que en la 7.0 se ha cambiado a HPD:Help Desk. (ID-17361, ID-14611)
- Al configurar un recurso de Active Directory, ahora es posible especificar un dominio en la sección de propiedades de autenticación de recursos. Los administradores deben especificar un dominio en entornos multidominio o de bosques para que los inicios de sesión sólo se autentiquen según el dominio de Active Directory correcto. Si no se especifica un dominio, el usuario puede bloquearse tras sólo un intento fallido de inicio de sesión. Esto se debe a que el usuario puede recibir un fallo de contraseña por cada dominio que comparta una relación de confianza con el dominio principal. (ID-16603)
- Se ha solucionado un problema que existía con el adaptador de recursos de SecurId Unix. Antes de solucionarlo, un cambio en el nombre o el apellido del usuario provocaba que los grupos del usuario se eliminaran del recurso de SecurId. (ID-16914)

Programador

- El Programador se ha actualizado para suprimir la salida de la entrada de SystemLog (syslog) `'EVNT00', LockedByAnother`. En entornos en clúster, este mensaje de error se enviaba al registro demasiadas veces. (ID-15714)
- El Programador se ha actualizado para reducir la posibilidad de que dos instancias de Identity Manager ejecuten a la vez el mismo flujo de trabajo. Antes de esta actualización, los entornos en clúster con varios Programadores que utilizaban todos ellos el mismo repositorio eran vulnerables a este problema. (ID-16500)

Otros problemas corregidos

16382

Problemas detectados

- La tabla de árbol de cuentas de la ficha **Listar cuentas** (Cuentas > Listar cuentas) no muestra la columna **Manager**. (Sólo aparecen las columnas **Nombre**, **Apellido** y **Nombre**.)

  Para corregir este problema, utilice el editor de procesos de negocio para editar el objeto de configuración UserUIConfig.

  Localice el elemento `<AppletColumns>` e introduzca el siguiente couplet XML al final de la lista:

  ```
  <Object name='idmManager'>
    <Attribute name='label' value='UI_ATTR_MANAGER'/>
  </Object>
  ```

  Guarde los cambios y reinicie el servidor de aplicaciones. (ID-17710)
- En la interfaz de administrador, la única forma de cancelar una delegación enviada (**Aprobaciones** > **Delegar mis aprobaciones**) es definiendo la misma Fecha final y Fecha de inicio (o una fecha pasada). (ID-16790, ID-16799)
- El visualizador TaskScheduleViewer no formatea la fecha de inicio con el mismo formato necesario para la entrada. En consecuencia, debe corregir la fecha de inicio al editar un programa de tareas. (ID-5675)

- De forma predeterminada, cuando un usuario introduce una respuesta a una pregunta de autenticación, los caracteres se enmascaran con asteriscos (*). No obstante, esta práctica inhabilita la capacidad de ciertos editores de métodos de entrada (IME) para crear caracteres complejos, tales como los utilizados en japonés kanji.

  Para que los usuarios puedan utilizar un IME a fin de responder a preguntas de autenticación, utilice la página de depuración para cambiar el valor de la propiedad `secret` a `false` en el formulario de usuario de inicio de sesión con preguntas.

  ```
  <Property name='secret' value='false'/>
  ```

  Nota: La definición de este valor como “false” supone un riesgo de seguridad, ya que las respuestas a las preguntas de autenticación se podrán leer en la pantalla. Aún así, las respuestas se guardan cifradas. (ID-7424)
- Algunas de las opciones de configuración que aparecen en la interfaz del administrador de Identity Manager no se utilizan con Identity Manager SPE. (ID-10843). Entre ellas se encuentran:
  - Opciones de configuración del asistente de recursos: excluir regla de cuentas, aprobadores y organizaciones
  - Atributos de función
- FireFox 1.5 no muestra correctamente algunos formularios de Identity Manager. Por ejemplo, en el formulario de usuario con fichas, el explorador no ajusta las etiquetas, por lo que todos los elementos se desplazan a la derecha. (ID-13109)
- La casilla de verificación “Report only users whose user name” aparece enumerada dos veces en los informes de usuario y de preguntas de usuario. Una casilla de verificación dispone de I-help, mientras que la otra no. Cualquiera de las casillas de verificación devolverá los datos correctos al utilizarse individualmente. (ID-13155)
- Si se produce un error HTTP Status 500 al conectarse a las páginas de usuario final SPE, ello podría indicar que hay múltiples claves de cifrado en la configuración de SPE. Esto podría estar provocado por generarse una nueva en Identity Manager durante el proceso de actualización.

  La solución es eliminar las claves de cifrado (EncryptionKeys) del directorio de configuración de SPE y volver a exportarlas desde Identity Manager. (ID-13162)
- Una vez definido un valor para un atributo de correo electrónico de un usuario, no se podrá eliminar. El valor se puede cambiar, pero no se puede volver a definir como nulo. (ID-13164)

- Si modifica un formulario de roles para cambiar el valor de la variable showSuperAndSubRoles de 0 a 1 y luego importa un archivo de definición de súper roles que contenga los subroles existentes mediante la ficha Configurar, los subroles no se modificarán para incluir la sección <SuperRoles>. Sin embargo, si utiliza la interfaz gráfica de usuario de Identity Manager para crear un súper rol, los subroles asociados al súper rol se actualizarán. (ID-15053)

  Este problema puede producirse con roles creados fuera de Identity Manager que hacen referencia a roles (subroles o súper roles) existentes en el sistema.

  Cuando se importan estos roles, los existentes no se actualizan para reflejar la nueva relación; por ejemplo, no se mantiene la integridad referencial. Utilice RoleUpdater para comprobar y corregir la integridad referencial cuando importe roles de esta manera.

  Solución: Consulte ID-15482, descrito en “Roles”.

- Las características de bloqueo de Microsoft SQL Server 2000 pueden dar lugar a errores de bloqueo en Identity Manager cuando se dan determinadas condiciones de sobrecarga. (ID-16068)

  Solución: Actualice Microsoft SQL Server 2000 a Microsoft SQL Server 2005 utilizando un modo nativo.

  Se ha probado el funcionamiento de Microsoft SQL Server 2005 (que incluye una función nueva denominada *Snapshot Isolation*) con Identity Manager en condiciones de sobrecarga y no presenta los mismos problemas de bloqueo que SQL Server 2000.

  Algunos usuarios han descubierto que es conveniente modificar la base de datos para utilizar la opción `READ_COMMITTED_SNAPSHOT` de la siguiente forma:

  ```
  ALTER DATABASE dbname SET READ_COMMITTED_SNAPSHOT ON
  </quote>
  ```

- Por problemas de interoperabilidad entre los orígenes de datos de WebSphere y los controladores Oracle JDBC, los clientes de Oracle que deseen utilizar un origen de datos de WebSphere con Identity Manager deben usar Oracle 10g R2 y el correspondiente controlador JDBC. (El controlador Oracle 9 JDBC no funciona con un origen de datos de WebSphere e Identity Manager.) Si tiene una versión de Oracle anterior a 10g R2 y no puede actualizar a 10g R2, configure el repositorio de Identity Manager de manera que se conecte a la base de datos de Oracle mediante un controlador administrador JDBC de Oracle (no un origen de datos de WebSphere). (ID-16167)

  Para obtener más información, consulte la URL siguiente:

  `http://www-1.ibm.com/support/docview.wss?uid=swg21225859`

- Algunas palabras de la ficha de la pantalla “Editar usuario” pueden ajustarse en el modo de varios idiomas. (ID-16054)

  Solución: Para asegurarse de que las palabras mostradas en las fichas no se ajusten, agregue lo siguiente a `$WSHOME/styles/customStyle.css`:

```
table.Tab2TblNew td {
background-image:url(../images/tabs/level2_deselect.jpg);
background-repeat:repeat-x;background-position:left top;
background-color:#C4CBD1;
border:solid 1px #8f989f;
white-space:nowrap;
}

table.Tab2TblNew td.Tab2TblSelTd {
border-bottom:none;
background-image:url(../images/tabs/level3_selected.jpg);
background-repeat:repeat-x;background-position:left bottom;
background-color:#F2F4F3;
border-left:solid 1px #8f989f;
border-right:solid 1px #8f989f;
border-top:solid 1px #8f989f;
white-space:nowrap;
}
```

Funciones anteriores y correcciones de errores

Funciones anteriores

En esta sección se describen las funciones añadidas en paquete de servicios anteriores para Identity Installation Pack 2005Q4M3.

Instalación y actualización

- Si utiliza SQL Server 2000 SP4 como repositorio y el controlador JDBC de Microsoft, deberá emplear el controlador de SQL Server 2000 para el controlador JDBC SP3. (ID-9917)
- Se ha añadido el atributo de sistema `waveset.serverId`. Utilice este atributo para definir nombres de servidor exclusivos cuando en la implantación se incluyan múltiples instancias de Identity Manager que señalen a un repositorio en un solo servidor físico. (ID-11578)
- Identity Manager admite ahora Oracle Database 10g Release2® como repositorio. (ID-12908)
- El instalador permite ahora actualizar instalaciones en las que se haya borrado, inhabilitado o cambiado el nombre de la cuenta predeterminada de Configurator. El instalador solicita ahora el nombre de usuario adecuado y la contraseña que pueden importar el archivo update.xml durante el proceso posterior de actualización. Si se introduce el usuario o contraseña incorrectos, el sistema solicitará al usuario hasta tres veces que introduzca la contraseña correcta. El error debe mostrarse en el cuadro de texto situado detrás. (ID-13006)

  Para la instalación manual, debe proporcionar los indicadores `-U` *`<nombreusuario>`* `-P` *`<contraseña>`* para transferir las credenciales al procedimiento UpgradePostProcess.
- Identity Manager se instala correctamente en máquinas sin tarjeta gráfica. (ID-14258)

Interfaces de administrador y usuario

- Los paneles **Configurar > Servidores > Editar ajustes del servidor/Editar ajustes del servidor predeterminados** incluyen ahora la ficha Plantillas de correo electrónico. Esta ficha incluye la variable de host SMTP predeterminado/por servidor que utilizarán como valor predeterminado todas las plantillas de correo electrónico con la variable `$(smtpHost)`. Esta ficha utilizará también la variable de configuración de servidor si el campo de host SMTP está en blanco. (ID-3574)

- Al hacer clic en Reinicializar consulta en la pantalla Buscar usuarios, el despliegue de nombres y el límite de resultados se reinicializan ahora al estado inicial.(ID-8961)
- Las páginas Cambiar contraseña de usuario y Reinicializar contraseña de usuario de la interfaz de administrador de Identity Manager incluyen ahora opciones de menú para el tipo de búsqueda. Estas opciones desplegables incluyen **comienza con**, **contiene** y **es** como operandos para buscar usuarios cuya contraseña sea necesario cambiar o reinicializar. (ID-8965)
- La página Depurar proporciona ahora las opciones de **exportar valor predeterminado** y **exportar todo**. Estas opciones funcionan de manera similar a las opciones de la consola, exceptuando que las opciones de la página Depurar no ofrecen ninguna opción para el nombre del archivo exportado. En su lugar, Identity Manager crea un archivo con el nombre `export<`***`fecha`***`>.xml` que se puede guardar desde la página Depurar. (ID-9270)
- Ahora es posible importar una plantilla de correo electrónico que contenga una dirección con “cc”. (ID-9768)
- La página de atributos de identidad muestra ahora una sección de contraseñas, en la que se describe el estado de la generación de contraseñas con respecto a los atributos de identidad. Puede configurar Identity Manager para asignar contraseñas a nuevos usuarios en función de un valor predeterminado, una regla o mediante la asignación de una directiva de cuentas del sistema Identity que genera contraseñas. (ID-10274, 12560)
- Mensajes de error revisados asociados a la edición de directivas. (ID-12187)
- Identity Manager incluye ahora un atributo Manager predeterminado, que proporciona compatibilidad para relaciones administrador-empleado creadas. Esta información se almacena en el objeto de usuario de Identity Manager. Para obtener más información, consulte la sección *Adiciones y correcciones de la documentación* de estas notas de la versión. (ID-12416)
- Ahora es posible configurar atributos de identidad en función de cambios recientes realizados en recursos (ya sean operaciones de edición o de creación). (ID-12678) Si los recursos se han modificado desde la última vez que se guardaron los atributos de identidad en la interfaz de administrador de Identity Manager, la página de atributos de identidad mostrará este mensaje: “Se ha modificado uno o varios recursos desde que se guardaron Atributos de identidad por última vez. Si estos cambios afectan a los Atributos de identidad, se deberán adaptar mediante la página Configure Identity Attributes from Resource Changes (Configurar Atributos de identidad a partir de cambios de recursos)”. Identity Manager proporciona un vínculo a la página Configure Identity Attributes from Resource Changes que permite seleccionar los atributos desde los mapas de esquema de recursos modificados que se deben utilizar como orígenes o destinos para los atributos de identidad.

Después de guardar un recurso desde la página de atributos de cuenta o el asistente de recursos, Identity Manager muestra una página en la que se pregunta si desea configurar atributos de identidad en función de los cambios realizados en recursos recientemente. Seleccione **Sí** para acceder a la página Configure Identity Attributes from Resource Changes. Seleccione **No** para volver a la lista de recursos.

Para inhabilitar esta página, seleccione **No preguntar de nuevo**. De esta forma, la página se inhabilita definiendo como false la propiedad `idm_showMetaViewFromResourceChangesPage` del usuario que ha iniciado sesión.

- Los objetos de selección múltiple (MultiSelect) ahora ordenan los valores disponibles cuando se configuran las propiedades `noApplet=true` y `sorted=true`. (ID-12823)
- En la tabla de árbol de cuentas no se detectaban los cambios realizados en un objeto de configuración que incluyese una lista estática. Por ejemplo, las organizaciones controladas de un administrador estaban determinadas por una regla que recuperaba una lista estática de un objeto de configuración. Antes, el servidor se debía reiniciar para detectar cambios realizados en el objeto de configuración. Ahora, la tabla de árbol cambia a objetos de configuración cuando los usuarios cierran la sesión actual y vuelven a iniciar otra. (ID-14442)
- DatePicker puede tener ahora un rango de fechas definido para que sólo se puedan seleccionar determinadas fechas del calendario. (ID-10100)
- Las plantillas de configuración de servidores y de modificación de correo electrónico se han modificado para que el administrador pueda determinar si se debe realizar SSL o autenticación en el servidor de SMTP. (ID-12465)
- La página continueLogin.jsp muestra ahora el mensaje correctamente. (ID-13193)
- Se han realizado los siguientes cambios en Identity Manager 7.1 Identity Manager Integrated Development Environment (IDE) a fin de proporcionar compatibilidad para Identity Manager versión 2005Q4M3 SP3: (ID-14089, 15211)
  - El depurador de Identity Manager está ahora habilitado de forma predeterminada.

    Si está implementando en producción, se recomienda que defina la propiedad de configuración del sistema como `serverSettings.default.debugger.enabled=`**`false`**.
  - El depurador de Identity Manager permite ahora definir puntos de interrupción en bibliotecas de reglas.
  - La sincronización de contraseña en modo directo requiere que `SimpleRpcHandler` se configure en `web.xml`. `SimpleRpcHandler` interfiere con determinadas llamadas de `RemoteSession`. Si no está utilizando la sincronización de contraseña en modo directo y tiene problemas

con llamadas de `RemoteSession`, puede eliminar la configuración de `SimpleRpcHandler` del servlet `rpcrouter2` para solucionar los problemas de `RemoteSession`.

Cambie estas entradas en `web.xml`:

```
<init-param>
<param-name>handlers</param-name>
<param-
value>com.waveset.rpc.SimpleRpcHandler,com.waveset.rpc.Passwor
dSyncHandler</param-value>
</init-param>
```

a lo siguiente:

```
<init-param>
<param-name>handlers</param-name>
<param-value>com.waveset.rpc.PasswordSyncHandler</param-value>
</init-param>
```

Si desea utilizar `RemoteSession` y la sincronización de contraseña en modo directo, configure un servlet independiente para administrar las llamadas de `RemoteSession`.

- Se ha solucionado un problema en que un objeto de organización no se desbloqueaba cuando un usuario con derechos insuficientes intentaba eliminarlo. (ID-14942)

Formularios

- En los formularios, el uso de `<set>` dentro de `<Expansion>` ahora funciona correctamente. (ID-9617)
- Los mensajes de reglas de verificación ahora aparecen en el entorno regional del cliente y no en el servidor. (ID-12780)

Puerta de enlace

- La puerta de enlace se ejecuta ahora en imágenes vmware de Windows 2000 SP4 y Windows 2003 SP1. (ID-12826)

Componentes de visualización HTML

- La clase de presentación DatePicker dispone de la nueva propiedad `strict`. Si se define, esta propiedad hace que se validen las fechas introducidas manualmente. (ID-11037)
- Ahora es posible inhabilitar la regeneración forzada del menú de usuario final añadiendo la propiedad `doNotRegenerateEndUserMenu` del formulario de menú de usuario final. (ID-11327)

- El componente SortingTable respeta ahora las propiedades `align`, `valign` y `width` de los componentes secundarios de los que consta la tabla al representarse en HTML. También hay un componente InlineAlert que muestra mensajes de error, advertencia, confirmación y de información en formularios. (ID-12560)
- El componente de tabla de árbol admite ahora columnas ajustables. Ahora puede establecer el ancho de las columnas de las tablas de listas de usuarios y recursos mediante CSS en un valor porcentual o en un valor fijo expresado en píxeles. También puede cambiar el tamaño de las columnas con el ratón haciendo clic sobre el borde derecho del encabezado de la columna y arrastrándolo. (ID-11474)

Nota En Firefox/Mozilla y otros navegadores basados en Gecko, se puede seleccionar el texto del navegador al cambiar el tamaño de una columna. Esto no ocurre con Internet Explorer o Safari, ya que el comportamiento de DHTML onselectstart se puede suprimir.

Identity Auditor

- Ahora puede crearse una directiva de auditoría para examinar sólo un conjunto restringido de recursos. (ID-9127)
- El servidor de información de identidad de Microsoft y de tablas de bases de datos utiliza ahora los formularios personalizados, especificados para estos dos recursos. (ID-10302)
- El título del informe de acceso de usuario se muestra correctamente. (ID-11538)
- La tarea de exploración de acceso funciona ahora en organizaciones dinámicas. (ID-12437)
- La opción de vista de usuario CallViewValidators (UserViewConstants.OP_CALL_VIEW_VALIDATORS) se puede definir en la cadena “true” o “false” para habilitar o inhabilitar (respectivamente) la comprobación de directivas de auditoría durante el aprovisionamiento. (ID-12757)
- El proceso de actualización ya no sobrescribe la plantilla de correo electrónico de aviso de revisión de accesos. (ID-13216)

Identity Manager SPE

Identity Manager SPE 2005Q4M3 SP1 introdujo las siguientes funciones nuevas. Para obtener información detallada sobre estas funciones, consulte *Identity Manager Service Provider Edition Administration Addendum* e *Identity Manager SPE Deployment*.

Páginas de usuario final mejoradas

Las páginas de usuario final se han mejorado. En las páginas de ejemplo se incluyen las siguientes funciones:

- Inicio de sesión (y salida) que incluye autenticación mediante preguntas de desafío
- Registro
- Cambio de contraseña y nombre de usuario
- Edición de las preguntas de desafío y de la dirección de notificación
- Gestión de nombre de usuario y contraseña olvidados
- Notificación por correo electrónico
- Auditoría

Las páginas se pueden personalizar según la implementación. Se puede personalizar lo siguiente:

- Marcas
- Opciones de configuración (por ejemplo, el número de intentos de inicio de sesión fallidos)
- Adición y eliminación de páginas

Directiva de ID de cuenta y contraseña

Existen ahora directivas de ID de cuenta y contraseña para Identity Manager SPE y cuentas de recurso. Estas directivas se implementan con la misma infraestructura de directiva que Identity Manager. (ID-12556)

Coexistencia de Active Sync e Identity Manager SPE Sync

Ahora es posible ejecutar la sincronización de SPE y Active Sync en el mismo servidor de Identity Manager. No ejecute los dos en el mismo recurso. (ID-12178)

Directorios independientes de configuración y de usuario de LDAP

La información de usuario y de configuración se puede almacenar ahora en instancias de LDAP independientes. Estas instancias se seleccionan durante la configuración inicial. (ID-12548)

Integración de Access Manager

Ahora puede utilizar Sun Java System Access Manager 7 2005Q4 para autenticación en páginas de usuario final de Identity Manager SPE. Access Manager asegura que sólo los usuarios autenticados puedan acceder a las páginas de usuario final.

Otras correcciones

- Ahora, Identity Manager SPE reanuda el procesamiento de las transacciones cuando el servicio se detiene de forma irregular (por ejemplo, el servidor de aplicaciones se cierra con un error de falta de memoria). (ID-14579)
- Ahora, las transacciones de Identity Manager SPE pueden utilizar niveles de coherencia de actualización de usuarios configurables. Las bases de datos de almacenamiento de transacciones existentes deberán modificarse para agregar una columna más, `userId VARCHAR(N)`, donde `N` es lo suficientemente grande como para contener la longitud máxima previsible para los ND de usuario de Identity Manager SPE y otros 8 caracteres más. Este cambio de la base de datos no se realiza automáticamente cuando se ejecutan los archivos de comandos de actualización. (ID-13830)

Localización

- Las claves de mensajes utilizadas como preguntas de autenticación ahora se muestran correctamente en la página de resultados. (ID-13076)

Inicio de sesión

- Los eventos de Active Sync se registran ahora en el registro del sistema. (ID-12446)
- Los cambios en las preguntas de autenticación del usuario se registran ahora en los registros de auditoría. (ID-13082)
- Ahora es posible realizar el seguimiento de subllamadas de método directas e indirectas. (ID-13436) Esto puede ser útil a la hora de depurar problemas que se sabe que se producen en algún nivel inferior a un método de entrada específico. Para habilitar esta función, defina el nivel de seguimiento para un ámbito con el modificador `subcalls`, como se indica en el siguiente ejemplo:

  ```
  trace 4,subcalls=2
  com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
  ```

  De esta forma se realizará el seguimiento del método `reconcileAccount()` en el nivel 4 y de todas las subllamadas en el nivel 2.
- Los errores que se producen en el Programador de actividades se registran ahora en el registro del sistema, en lugar de conservarse en el objeto TaskSchedule. (ID-14261)

Reconciliación

- La definición de la tarea de notificación de finalización de reconciliaciones se completa correctamente cuando se especifica como flujo de trabajo posterior a la reconciliación (ID-9259)
- Cuando existe un gran número de objetos de cuenta (éstos se crean como resultado de reconciliaciones y provisiones), el rendimiento de reconciliación y aprovisionamiento puede disminuir drásticamente.

  Para tratar esta cuestión, se debe crear un índice en la columna “name” de la tabla “account” del repositorio. En el directorio de ejemplo se proporcionan varias secuencias de comandos que facilitan esta tarea. `account_index.sqlserver` es para Microsoft SQL Server; `account_index.sql` es para las demás bases de datos. (ID-14478)

Informes

- Identity Manager crea ahora eventos de auditoría cuando se crean y se modifican capacidades. (ID-9734).
- Identity Manager proporciona ahora una nueva opción de roles incluida en el campo **Seleccione los atributos de Identity Manager que desea mostrar para cada usuario**. Al seleccionar esta opción para informes nuevos y existentes, aparece una lista de roles separada por comas en el informe. (ID-9777)
- Ahora puede especificar una lista de atributos para mostrarla en su propia columna en informes en formato CSV y PDF. Si no especifica la lista, todos los atributos se mostrarán en una sola columna denominada Atributos susceptibles de auditoría. (ID-10468)
- De forma predeterminada, los siguientes informes se ajustan ahora automáticamente al ámbito del conjunto de organizaciones controlado por el administrador conectado, a menos que se anule explícitamente al seleccionar una o varias organizaciones según las cuales se deba ejecutar el informe. (ID-12116)
  - Informe de resumen de roles de administración
  - Informe resumido del administrador
  - Informe resumido de roles
  - Utilizar informe de preguntas del usuario
  - Informe resumido de usuario

  Para admitir esta función, el componente de ámbito de organización se ha cambiado de un componente `Select` único a otro `MultiSelect`.

- Dos nuevos informes permiten introducir compatibilidad incorporada para relaciones administrador-empleado: My Direct Reports Summary (Resumen de mis informes directos), My Direct Employee Summary (Resumen de mis empleados directos), My Direct and Indirect Employee Summary (Resumen de mis empleados directos e indirectos) y My Direct Reports Individual (Mis informes directos individuales). (ID-12416, ID-12689)
- El informe de usuario de recursos genera ahora archivos CSV y PDF correctamente. (ID12509, 13701)
- Se admite el registro de auditoría para la creación, modificación y eliminación de roles de administración. (ID-12514)
- El informe de usuario incluye ahora un atributo de búsqueda para facilitar la ejecución de un informe basado en un administrador de usuario. (ID-12689)
- Los informes de usuario muestran ahora el ID de todas las cuentas del recurso en una lista separada por puntos y comas.(ID-12820) También se enumeran las cuentas y los recursos asignados indirectamente mediante un rol o un grupo de recursos. Si sólo hay una cuenta de recursos, el ID de cuenta sólo se mostrará si no es el mismo que el ID de cuenta de Identity Manager.
- Los nombres de columna se muestran ahora correctamente en informes en PDF. (ID-12794)
- Ya se ha corregido el error por el que se generaban nombres de `TaskTemplate` demasiado largos (superiores al valor de MAX_NAME_LENGTH). (ID-13790)

Repositorio

- Identity Manager admite ahora Oracle Database 10g Release2® como repositorio. (ID-12908)
- SQL Server 2005 se admite ahora como repositorio. (ID-14755) Realice los siguientes pasos para utilizar esta versión de SQL Server.
  1. Descargue el controlador JDBC para SQLServer 2005 (versión 1.2) desde el sitio web de Microsoft.
  2. Guarde la versión anterior del controlador, ubicado en el directorio `$WSHOME/WEB-INF/lib`. A continuación, sustituya la versión anterior por el controlador `sqljdbc.jar` en el mismo directorio.
  3. Revise la secuencia de comandos de creación de la base de datos. Al crear la base de datos, es posible que desee quitar los comentarios de las líneas:

```
ALTER DATABASE waveset SET READ_COMMITTED_SNAPSHOT ON
GO
```

     Consulte la documentación de SQLServer 2005 para obtener información sobre esta configuración.

4. Al configurar el repositorio con el comando lh setup o lh setRepo, utilice los siguientes valores:

```
type = SQLServer
jdbc driver = com.microsoft.sqlserver.jdbc.SQLServerDriver
url =
jdbc:sqlserver://Nombredemáquina:Puerto;DatabaseName=waveset
```

Deberá sustituir el nombre de máquina y el puerto en la URL por valores válidos.

- El repositorio de IDM se inicializa ahora con mayor rapidez. (ID-14937)

Recursos

Recursos nuevos

Se ha añadido compatibilidad para los siguientes recursos a partir de Identity Manager 2005Q4M3: Consulte el documento *Identity Manager Resources Reference Addendum* para obtener más información.

- HP OpenVMS (ID-8556)
- BridgeStream SmartRoles (ID-12262)
- OS/400 v4r5, v5r2, v5r3 y v5r4 (5.2, 5.3 y 5.4).
- Shell Script (ID-11906, ID-9866)
- Scripted JDBC (ID-7540)
- Siebel 7.8
- Compatibilidad con Realm en Sun Java System Access Manager (ID-12414)

General

- Identity Manager permite ahora almacenar atributos de cuentas binarias. Los siguientes adaptadores permiten esta función: (ID-8851, 12665)
  - Active Directory
  - LDAP
  - Flat File Active Sync
  - Tabla de base de datos
  - JDBC con secuencia de comandos
  - Servicios de comunicación del sistema Sun Java

  Active Directory admite ahora los atributos binarios `thumbnailPhoto` (Windows 2000 Server y superior) y `jpegPhoto` (Windows 2003). Los demás adaptadores admiten ahora atributos tales como `jpegPhoto`, `audio` y `userCertificate`.

Identity Manager devolverá una excepción si intenta enviar atributos binarios o complejos a un recurso que no admita atributos binarios.

Los atributos binarios deben ser lo más pequeño posible. Si carga un atributo binario que sea demasiado grande (por ejemplo, 200 KB), es posible que aparezca un mensaje de error indicando que ha superado el tamaño de paquete máximo permitido. Póngase en contacto con el servicio al cliente para obtener instrucciones si necesita administrar atributos de mayor tamaño.

- Los adaptadores de recurso de agente proporcionan ahora un atributo de recurso opcional que permite retener las conexiones en operaciones de bloqueo: RA_HANGTIMEOUT. Este atributo especifica el valor de tiempo de espera, en segundos, antes de que finalice el tiempo de espera de una solicitud a la puerta de enlace y se considere bloqueada. Su valor predeterminado es 0, que indica no comprobar si la conexión se ha bloqueado. (ID- 12455)
- Las modificaciones realizadas en objetos AttrParse pueden surtir efecto ahora sin reiniciar Identity Manager. (ID-12516)
- Se han introducido mejoras en `AttrParse`. El análisis ya no envía ni capta una excepción por cada carácter del búfer analizado. (ID-13384)
- Identity Manager admite ahora conexiones a recursos de mainframe utilizando Reflection de Attachmate para la biblioteca de clases de emulador web (Web Emulator Class Library). Consulte la sección *Anexos a la documentación y correcciones* de estas notas de la versión para obtener información sobre la configuración de esta función. (ID-14815)

ActiveSync

- El Asistente de Active Sync se ha internacionalizado más. (ID-10504)
- El sistema permite ahora realizar reintentos de Active Sync en un recurso. Para habilitar esta función, actualice el XML de recurso para incluir dos atributos de recurso adicionales del formulario:

  ```
  <ResourceAttribute name='syncRetryCountLimit' type='string'
  multi='false' facets='activesync' value='180'/>
  <ResourceAttribute name='syncRetryInterval' type='string'
  multi='false' facets='activesync' value='10000'/>
  ```

  `syncRetryCountLimit` es el número de veces que se reintenta la actualización, y `syncRetryInterval` es el número de milisegundos que se espera entre reintentos. Estos valores aparecerán a continuación como valores de recurso personalizados al configurar Active Sync. Es conveniente especificar un displayName, utilizando una clave de catálogo personalizada si se desea localización. (ID-11255)
- El número máximo de registros de Active Sync configurados en un recurso de Active Sync ahora se corresponde correctamente. (ID-11848)

Domino

- Ahora es posible crear un usuario de Domino sin archivo de ID o dirección de correo electrónico, sino con sólo una entrada en el directorio de Domino. (ID-11201)
- En recursos de Domino 6.x, ahora puede inhabilitar cuentas sin proporcionar una lista de Denegar grupos. Si no se especifica ninguna lista de Denegar grupos, Identity Manager utilizará el atributo CheckPassword para habilitar e inhabilitar en el recurso de Domino. Un valor de 2 inhabilita la cuenta. (ID-12088)
- En el adaptador de Domino, las actualizaciones concurrentes de HTTPPassword con varios usuarios mediante la llamada a la API `NSFNoteComputeWithForm()` ya no da como resultado el error de puerta de enlace “-551”. (ID-12466)

Directorio

- Identity Manager proporciona ahora un mecanismo más escalable para editar atributos de objeto de recursos con valor de lista grande. En `sample/forms/LDAPgroupScalable.xml` se proporcionan formularios de ejemplo para utilizar este método a fin de administrar grupos de LDAP. (ID-9882)
- El adaptador de recursos de LDAP utiliza ahora directamente el proveedor JSSE. (ID-9958) La versión mínima compatible con Java en Identity Manager es ahora 1.3, que permite utilizar proveedores de seguridad de terceros para la comunicación SSL en el caso de los adaptadores de recursos de Domino, LDAP y NDS SecretStore. Puede registrar bibliotecas de proveedores de seguridad de terceros utilizando el archivo java.security estándar.

  Para obtener más información, consulte http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html#ProviderInstalling
- Ahora puede editar grupos de LDAP cuyos nombres incluyan barras diagonales. (ID-9872)

  El atributo de configuración `ldapJndiConnectionFactory.alwaysUseNames` se ha añadido al archivo `Waveset.properties`.

  De forma predeterminada, esta propiedad está habilitada. Al habilitarse, todos los nombres de cadena se analizan en un nombre utilizando el NameParser del contexto. Esto permite evitar problemas de salida de JNDI. Esta opción tendrá sentido solamente si la opción `ldapJndiConnectionFactory.wrapUnpooledConnections` se define como true.

  Al basarse en el valor predeterminado (true) o si este valor se define explícitamente como true, se requerirá un JVM de versión 1.4 o posterior. Debido a un problema con JNDI, en JVM anteriores, algunas operaciones de cambio de nombre pueden fallar cuando esta opción se habilita.

- El adaptador de LDAP ya no crea nombres distinguidos (ND) incorrectos para las cuentas nuevas. (ID-10951)

  El método escape de `com.sun.idm.util.ldap.DnUtil` ahora puede utilizarse en los formularios para que se introduzcan valores de escape en las plantillas de identidades de los adaptadores de recursos con el formato de ND de LDAP. Como alternativa, puede utilizarse una directiva de ID de cuenta con la opción “Required LDAP DN format” (Formato de ND de LDAP necesario) seleccionada para validar la entrada de nombres distinguidos de LDAP en Identity Manager a través de datos introducidos por los usuarios, ActiveSync y procesos de reconciliación.
- El valor predeterminado del atributo **Objectclasses to synchronize** de Active Sync en los recursos de LDAP ahora es inetorgperson. (ID-11644)
- Se ha optimizado el filtro de búsqueda `LDAPActiveSync` que detecta cambios en el registro de cambios. La parte de filtro (`objectClass=changelogEntry`) se ha eliminado del filtro de búsqueda predeterminado. (ID-11722)

  El comportamiento anterior se puede recuperar añadiendo el atributo **Remove objectClass from Search Params Filter** directamente a la definición del recurso con un valor false, como se indica:

  ```
  <ResourceAttribute name='Remove objectClass from Search Params
  Filter' displayName='Remove objectClass from Search Params
  Filter' facets='activesync' value='false'>
  </ResourceAttribute>
  ```

  Nota: Esta configuración no se puede cambiar desde la interfaz gráfica de usuario.
- El cambio de la afiliación a grupos de LDAP ahora permite añadir o suprimir miembros de uno en uno sin necesidad de volver a escribir el grupo completo (es decir, sustituir el atributo uniqueMember completo). (ID-13035)
- El adaptador de LDAP se puede configurar para que se realice una clasificación VLV según un valor distinto a `uid`. (ID-13321) Para cambiar este valor, añada lo siguiente a la definición del recurso:

  ```
  <ResourceAttribute name='vlvSortAttribute' displayName='VLV Sort
  Attribute' description='VLV Sort Attribute'
  value='myValue'></ResourceAttribute>
  ```
- El atributo `PasswordNeverExpires` de Active Directory ahora puede configurarse durante las actualizaciones. (ID-13710)
- El adaptador de NDS Active Sync ya no interroga sobre cambios basados en la marca de tiempo lastModifiedTimeStamp del objeto de usuario. Este atributo se actualizaba cuando un usuario iniciaba una sesión o la finalizaba. Para solucionar este problema, el último valor modificado se calcula ahora en función de la marca de tiempo lastModifiedTimestamp de los atributos de un usuario definidos en el mapa de esquema. Si la marca de tiempo

lastModifiedTimestamp de un atributo es superior a la marca alta de agua que presenta el adaptador, la puerta de enlace enviará a este usuario al servidor como modificado. (ID-13896)

- Se ha corregido un problema que provocaba que los usuarios de NDS recién creados no pudieran acceder a sus directorios iniciales. (ID-14208)
- Los tiempos de espera de recuperación de datos de Active Directory ya no provocan que las reconciliaciones finalicen prematuramente. (ID-14564)
- Se ha corregido un problema por el que el adaptador de Active Sync de Active Directory se bloqueaba al no cerrarse las conexiones con la puerta de enlace. (ID-14597)
- El adaptador de LDAP permite que el método abreviado de activación `nsaccountlock` utilice una lógica basada en la existencia o ausencia de valor al determinar si un usuario de LDAP está inhabilitado. (ID-14925) Consulte la sección *Adiciones y correcciones de la documentación* de estas notas de la versión para obtener más información.

Oracle ERP

- Se han añadido múltiples atributos al adaptador de Oracle ERP para que admita funciones de auditoría. (ID-11725) Consulte la sección *Adiciones y correcciones de la documentación* de estas notas de la versión para obtener más información.
- El adaptador de Oracle ERP ya no falla a la hora de cerrar cursores de base de datos de Oracle. Anteriormente, el fallo provocaba el siguiente error: (ID-12222)
- En formularios para adaptadores de Oracle ERP, el método `listResourceObjects` de la clase `com.waveset.ui.FormUtil` puede devolver ahora responsabilidades específicas de un usuario y se puede filtrar para devolver todas las responsabilidades, o bien responsabilidades activas solamente. (ID-12629)

  Las opciones incluidas son las siguientes:

  - `key id`: (Cadena) identifica la identidad de recurso cuyas responsabilidades se devuelven.
  - `activeRespsOnly`: (Cadena) true o false. Este valor es false de forma predeterminada si no se envía.
- El adaptador de Oracle ERP proporciona ahora una palabra clave `sysdate` o `SYSDATE`. Esta palabra clave se utiliza con `to_date` para especificar una fecha de caducidad de una responsabilidad con la hora local de un servidor Oracle E-Business Suite (EBS). (ID-12709)

- El adaptador de Oracle ERP de Identity Manager proporciona ahora un nuevo atributo de cuenta `employee_number`. Este atributo representa un número de empleado (`employee_number`) de la tabla `per_people_f`. Consulte la sección *Adiciones y correcciones de la documentación* de estas notas de la versión para obtener más información. (ID-12710).
- La actualización de una responsabilidad de una cuenta de Oracle ERP utilizando el adaptador de Oracle ERP ya no provoca que se actualicen otras responsabilidades asociadas a la cuenta. (ID-13889) Como resultado, sólo se actualiza la marca de tiempo de auditoría de Oracle ERP correspondiente a la responsabilidad modificada. Las marcas de tiempo de auditoría de Oracle ERP de las demás responsabilidades de cuenta no se modifican.
- Se ha añadido el atributo de cuenta person_fullname al mapa de esquema para el adaptador de Oracle ERP. En el formulario de usuario de Oracle ERP, este atributo se utiliza para mostrar el campo Person Name. Este campo es de sólo lectura y mostrará el nombre completo del usuario si una cuenta de Oracle ERP está vinculada al sistema Oracle HR mediante el número de empleado. (ID-14675)
- El adaptador de Oracle ERP evita ahora la desvinculación de cuentas de recursos si no se puede acceder al recurso de Oracle ERP durante una reconciliación completa. (ID-14960) (El recurso puede ser inaccesible por varios motivos, por ejemplo, por ser incorrecta la configuración de conexión con los recursos.)
- El adaptador de Oracle ERP admite ahora Oracle E-Business Suite 12. Consulte la sección *Anexos a la documentación y correcciones* de estas notas de la versión para obtener más información. (ID-15062, 16705)
- Se ha añadido el atributo de cuenta `npw_number` al adaptador de Oracle ERP para admitir cuentas de trabajadores eventuales. (ID-16507)

SAP y SAP HR

- Ahora puede configurar el adaptador de SAP HR para procesar IDOC de cualquier tipo de mensaje. Anteriormente, sólo se podían procesar IDOC del tipo HRMD_A. (ID-12120)

  ```
  ORA-01000: superado el número máximo de cursores abiertos
  ```

- Los adaptadores de SAP y SAP HR ahora admiten tres nuevos atributos de recursos que proporcionan los parámetros necesarios para reintentar operaciones de SAP cuando se produce un fallo en la red. (ID-12579) Estos atributos son:
  - Recuento de reintentos BAPI de SAP: número de veces de reintento de la operación.
  - Recuento de reintentos de conexión con SAP: número de veces que debe intentarse la conexión con el servidor de SAP.
  - Tiempo de espera de reintento de conexión con SAP: cantidad de milisegundos que es preciso esperar antes de volver a intentar la conexión con el servidor de SAP.

- Las contraseñas se pueden configurar ahora como no caducadas al utilizar el modo CUA en un recurso de SAP. (ID-13355)
- El adaptador de SAP ya no devolverá una excepción JCO_ERROR_FUNCTION_NOT_FOUND cuando el sistema SAP no contenga el módulo de función PASSWORD_FORMAL_CHECK. (ID-14663)
- El adaptador de SAP informa ahora correctamente del estado de las cuentas inhabilitadas. (ID-14834)
- Los grupos de actividades (roles) y los perfiles del entorno CUA se pueden actualizar con la fecha de inicio y final. (ID-15613)

  Para los roles, asigne el atributo `activityGroups` del adaptador a:

  `CUA->directLocalActivityGroupObjects`

  Para los perfiles, asigne `profiles` a:

  `CUA->directLocalProfileObjects`
- El adaptador de SAP permite actualizar el campo ALIAS en SAP. La asignación de atributo en la configuración de esquema es ALIAS->USERALIAS. (ID-16320)

UNIX

- Los adaptadores basados en UNIX incluyen ahora un atributo de recurso de directorio base. Cuando está presente, este atributo sustituye el valor del directorio base del recurso nativo correspondiente a la cuenta que se esté creando. El valor es el definido en este atributo anexado con el `accountID`. Si define el directorio base del usuario en los atributos de cuenta, ese valor tendrá preferencia sobre el directorio base. (ID-8587)
- Es posible definir valores predeterminados de tiempo de espera mediante la directiva de tipo de recurso. Además, puede utilizar también la propiedad `maxWaitMilliseconds` para controlar la frecuencia de interrogación que utiliza el adaptador con secuencia de comandos de Identity Manager al esperar a que el recurso finalice una tarea. (ID-11906)
- Los adaptadores de Solaris y Linux ahora devuelven un año en la última información de inicio de sesión. (ID-12182)
- Al visualizar información de cuentas de un recurso Solaris configurado con NIS, se muestra información de afiliación a grupos con el nombre de grupo, en lugar del ID de grupo numérico. (ID-12667)
- Se han añadido dos atributos de recurso, Default Primary Group y Login Shell, a los adaptadores de recursos de Solaris, AIX, HP-UX, Red Had Linux y SuSE Linux. (ID-15034)

Otros adaptadores

- El adaptador de recursos de RACF ahora permite controlar directamente las reglas de conjunto de datos, en lugar de que las administre Identity Manager. Esto permite crear reglas de conjunto de datos distintas de las nativas de Identity Manager. (ID-10446)

  En el ejemplo siguiente, se crea una regla de conjunto de datos de `<user id>.test1.**`, en lugar de la predeterminada de Identity Manager, `<user id>.**`.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE ResourceAction PUBLIC 'waveset.dtd' 'waveset.dtd'>
<ResourceAction name='create after action'>
  <ResTypeAction restype='RACF'>
    <act>
      var TSO_PROMPT = "READY";
      var TSO_MORE = "***";
      var cmd1 = "addsd '"+identity+".test1.**'
owner('"+identity+"')[enter]";
      var result1 = hostAccess.doCmd(cmd1, TSO_PROMPT, TSO_MORE);
    </act>
  </ResTypeAction>
</ResourceAction>
```

- El adaptador de RACF ahora admite filtros de búsqueda para `listAllObjects`. (ID-10895)
- Ahora puede crear y actualizar objetos en Siebel que requieren navegación por el componente comercial principal/secundario. Consulte la sección *Anexos a la documentación y correcciones* de estas notas de la versión para obtener más información. (ID-11427)
- El método `isPickListAttribute` del adaptador de Siebel ya no se identifica erróneamente como `isMVGAttribute` en el sistema de seguimiento. (ID-11471)
- Para recursos SecurId, el atributo de clientes se trata ahora como atributo opcional. (ID-11509)
- El adaptador de Flat File Active Sync ahora proporciona un mensaje de advertencia en el archivo de registro de Active Sync (si está habilitado) cada vez que se produce un error que impide la acción `diff` para efectuar la sincronización. (ID-12484)
- Si configura Identity Manager para acceder a un recurso de RSA Clear Trust 5.5.2, no se requerirán bibliotecas adicionales para la comunicación SSL como era el caso con versiones de Clear Trust anteriores. (ID-12499)
- El asistente de tablas de bases de datos ya no permite configurar tablas a las que no se puede acceder. (ID-12643)

- El adaptador de Siteminder LDAP ahora realiza las siguientes operaciones de forma correcta aunque el usuario de Siteminder esté bloqueado tras haber fracasado en sucesivos intentos de iniciar la sesión:
  (ID-12824)
  - habilitar
  - inhabilitar
  - caducar contraseña (con habilitar/inhabilitar)
  - no caducar contraseña (con habilitar/inhabilitar)
- El adaptador de RACF ya no examina una cadena de caracteres larga una vez por cada usuario recuperado en `listAllObjects`, lo que normalmente da lugar a un mejor rendimiento de esta función cuando maneja grandes cantidades de usuarios. (ID-12829)
- Los espacios de tablas temporales no mantienen valores de cuota y, si se intenta desde Oracle 10gR2, se producirá una excepción SQL. (ID-12843)

  Hasta ahora, el adaptador de recursos definía una cuota en un espacio de tablas temporal, aunque el atributo de cuenta oracleTempTSQuota no estuviese asignado. Este comportamiento se ha cambiado. Si asigna el atributo oracleTempTSQuota, el comportamiento anterior se mantiene (sin cambios), pero si elimina la asignación, no se definirá ninguna cuota en el espacio de tablas temporal.

  En recursos Oracle 10gR2, elimine el atributo oracleTempTSQuota del adaptador de recursos.
- Identity Manager ahora borra los privilegios de administrador, si existen, antes de tratar de eliminar un usuario de Secure ID. (ID-13053)
- Se ha corregido un problema que se producía al realizar una reconciliación en VMS. (ID-13425)
- El adaptador de SecurID para UNIX ahora codifica y decodifica el juego de caracteres UTF-8 cuando interopera con RSA. (ID-13451)
- El adaptador de Shell Script puede detectar ahora errores generados a partir de una acción de recurso durante las funciones de creación y actualización de usuarios. (ID-13465)
- Al crear una cuenta en un recurso de Windows NT a través del adaptador de recursos de Windows NT, ya no aparece el mensaje de error siguiente en la página de resultados de Crear usuario: “Error requiring password: put_PasswordRequired(): 0X80004005:E_FAIL”. (ID-13618)
- Se ha añadido un nuevo parámetro de configuración de recursos (enableEmptyString) al adaptador de tabla de base de datos que permite escribir una cadena vacía, en lugar de un valor NULL, en columnas basadas en caracteres definidas como no nulas en el esquema de tablas. Esta opción no afecta a la manera en que se escriben las cadenas para tablas basadas en Oracle. (ID-13737)

- El adaptador de Shell Script admite ahora las funciones de cambio de nombre, de inhabilitación y de habilitación. (ID-14472)
- El adaptador de Scripted JDBC actualiza ahora correctamente un atributo en el que el valor original era nulo pero se definía como valor no nulo. (ID-14655)

Roles

- Los roles y grupos de recursos ofrecen ahora la capacidad, tanto individualmente como en combinación, de asignar varias cuentas a los usuarios en un recurso. Consulte la sección *Adiciones y correcciones de la documentación* de estas notas de la versión para obtener más información. (ID-6684)
- Cuando se importan roles que contienen vínculos recíprocos con súper roles existentes, Identity Manager actualiza ahora los roles existentes con los importados. (ID-15482)

  Identity Manager detecta y crea vínculos entre los súper roles existentes y los subroles asociados. Durante la actualización, Identity Manager ejecuta la clase RoleUpdater que permite reparar roles.

  Puede actualizar roles fuera del proceso de actualización importando un nuevo archivo RoleUpdater.xml existente en sample/forms/RoleUpdater.xml. De forma predeterminada, Identity Manager añade los vínculos de subrol durante la actualización o al importar el archivo RoleUpdater.xml.

  Para deshabilitar esta nueva función, configure el atributo `nofixsubrolelinks` de la clase RoleUpdater como true. Por ejemplo:

  ```
  <MapEntry key='nofixsubrolelinks' value='true' />
  ```

  Consulte la información relacionada con la actualización automática de roles durante la importación en ID-15053 que se describe en “Problemas detectados”.

Seguridad

- Los usuarios con capacidades de aprobador pueden delegar ahora sus solicitudes de aprobación futuras a uno o varios usuarios, que no sean aprobadores de Identity Manager, durante un determinado periodo de tiempo. Los usuarios pueden delegar mediante tres interfaces: (ID-8485)
  - Menú principal de usuario final – vínculo “Delegar aprobaciones”
  - Ficha Admin Approvals (Aprobaciones de administrador) – subficha “Delegar mis aprobaciones”
  - Admin Create/Edit/View User (Crear/Editar/Ver usuario de administrador) – sección Seguridad
- La generación de contraseñas funciona ahora correctamente, y falla de la manera prevista cuando las contraseñas no se generan correctamente. (ID-12275)

- Identity Manager proporciona ahora el tipo de autorización (authType) EndUserLibrary de usuario final. La capacidad EndUser (AdminGroup) ofrece ahora acceso de lista y vista a bibliotecas cuyo authType es EndUserLibrary. (ID-12469)

  Para conceder acceso a usuarios finales al contenido de una biblioteca, defina `authType='EndUserLibrary'` y compruebe que el valor MemberObjectGroup de la biblioteca es Todos.

- Un usuario de Identity Manager puede tener sesiones concurrentes iniciadas. Sin embargo, puede limitar sesiones concurrentes a una por aplicación de inicio de sesión cambiando el valor del atributo de configuración security.authn.singleLoginSessionPerApp en el objeto de configuración del sistema. Este atributo es un objeto que contiene un atributo por cada nombre de aplicación de inicio de sesión (por ejemplo, la interfaz de administrador, la interfaz de usuario o BPE). Al cambiar el valor de este atributo a true, se asegura que haya una sola sesión por cada usuario. (ID-12778)

  Si se aplica, un usuario se podrá conectar a más de una sesión. No obstante, sólo la última sesión iniciada estará activa y será válida. Si el usuario realiza una acción en una sesión no válida, el sistema le expulsará automáticamente de la sesión y ésta terminará.

- Los cambios de contraseña de usuario final iniciados por administradores, a través de SPML u otros medios, no se añadirán al historial de contraseñas. Existen ahora dos métodos para configurar la aplicación a fin de guardar una contraseña en el historial de los usuarios. Sólo un método es necesario. (ID-13029)

  - Opción de vista (tendrá prioridad si está presente o tiene el valor true) Defina el atributo 'savePasswordHistory' en el formulario de destino. Por ejemplo:

```
<Field name='savePasswordHistory'>
  <Default>
    <Boolean>true</Boolean>
  </Default>
</Field>
```

  - Utilice los siguientes valores de configuración del sistema y cambie el comportamiento de la interfaz deseada. Esto se deberá añadir al objeto de configuración del sistema si aún no está presente.

```
<Attribute name='security'>
  <Object>
    <Attribute name='admin'>
      <Object>
        <Attribute name='changePassword'>
          <Object>
            <Attribute name='Administrator Interface'>
              <Object>
                <Attribute name='savePasswordHistory'>
```

```
                    <Boolean>true</Boolean>
                  </Attribute>
                </Object>
              </Attribute>
              <Attribute name='Command Line Interface'>
                <Object>
                  <Attribute name='savePasswordHistory'>
                    <Boolean>true</Boolean>
                  </Attribute>
                </Object>
              </Attribute>
              <Attribute name='IVR Interface'>
                <Object>
                  <Attribute name='savePasswordHistory'>
                    <Boolean>false</Boolean>
                  </Attribute>
                </Object>
              </Attribute>
              <Attribute name='SOAP Interface'>
                <Object>
                  <Attribute name='savePasswordHistory'>
                    <Boolean>true</Boolean>
                  </Attribute>
                </Object>
              </Attribute>
              <Attribute name='User Interface'>
                <Object>
                  <Attribute name='savePasswordHistory'>
                    <Boolean>false</Boolean>
                  </Attribute>
                </Object>
              </Attribute>
            </Object>
          </Attribute>
        </Object>
      </Attribute>
....
```

Servidor

- Los subobjetos TaskInstance, como aprobaciones, ahora se borran adecuadamente cuando finaliza la tarea. (ID-3258)
- Identity Manager ahora requiere acceder al directorio `tmp`. (ID-7804) Para lograrlo, si el servidor de aplicación utiliza una directiva de seguridad, necesita añadir el permiso siguiente:

```
permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",
"read,write,delete";
```

- La página Buscar usuarios gestiona ahora jerarquías profundamente anidadas de muchas organizaciones. (ID-10352)
- En entornos en clúster, un inicio de sesión fallido en las páginas de usuario final ya no genera ninguna excepción relacionada con la serialización. (ID-10556)
- El servidor ya no activa en sí mismo el mecanismo de reconexión de emergencia y finaliza sus propias tareas cuando tarda demasiado tiempo en procesar información de tareas. (ID-10920)
- Los atributos ampliados de usuario se eliminan ahora correctamente de objetos de usuario. (ID-11721)
- ResourceConnectionManager ahora recibe notificación de cierres pendientes. En consecuencia, el servidor ya no tiene que esperar a que finalice el tiempo de espera de las conexiones SSH para poder salir. (ID-12214)
- Se ha corregido la condición que provocaba un error por inexistencia de antememoria ("no cache error") en la página Todas las tareas para usuarios de suborganizaciones que no disponen de acceso de administrador a organizaciones principales. (ID-12288)
- El procesamiento de delimitadores ahora se suprime entre corchetes. Por tanto, todos los caracteres que se encuentren entre corchetes se tratarán como un índice o un filtro. Nota: en estos momentos no hay ningún mecanismo de escape para el corchete de cierre "]". (ID-12384)
- Las acciones de finalización de instancias de tareas ahora se auditan como acciones Finalizar en lugar de acciones Modificar. (ID-12791)
- Las acciones de usuario se pueden realizar en usuarios después de eliminar un recurso directamente asignado a ellos. (ID-14806)

SOAP

- La compatibilidad con SPML se ha ampliado para cubrir roles y grupos de recursos además de personas. (ID-8850)
- La nueva capacidad SPMLAccess permite a los administradores de cuentas acceder a la interfaz de SPML. (ID-10854)
- El servidor de SPML devuelve ahora errores para solicitudes que contienen filtros que utilizan operadores no implementados aún. (ID-11343)
- La interfaz de SPML de Identity Manager proporciona un `login` ExtendedRequest que permite a los llamadores iniciar una sesión como administrador. A partir de esta versión, la interfaz de SPML proporciona también un `loginUser` ExtendedRequest que permite al llamador obtener una sesión para autoprovisión de usuario. Este `loginUser` ExtendedRequest permite iniciar una sesión con una contraseña o con respuestas a preguntas de seguridad. (ID-12103)

Vistas

- La vista de usuario proporciona ahora el siguiente atributo de control: (ID-4383)

  `accounts[`***resname***`].waveset.forceUpdate`

  donde ***resname*** representa el nombre del recurso. El valor de este atributo es una lista de atributos de cuenta de recursos que siempre se enviará al recurso para actualizarse cuando se modifica un usuario.
- Las vistas de cuenta de recursos (DeprovisionViewer, DisableViewer, EnableViewer, PasswordViewer, RenameUserViewer, ReprovisionViewer y UnlockViewer) admiten ahora dos nuevas opciones para buscar atributos de cuenta de recursos del usuario: (ID-10176)
  - `fetchAccounts` (booleano): permite que la vista incluya atributos de cuenta para los recursos asignados al usuario.
  - `fetchAccountResources`: enumera nombres de recursos para elegirlos. Si esto no se especifica, Identity Manager utilizará todos los recursos asignados.

Flujo de trabajo

- Ya no se devuelven advertencias de comprobaciones de referencias (checkReference) no válidas al ejecutar flujos de trabajo. (ID-10802)
- Si se utiliza `notification.redirect` para redirigir los mensajes a un archivo, ese archivo ahora se escribe utilizando `emailNotifier.contentCharset`, igual que ocurriría si el mensaje se enviase por correo electrónico. Gracias a esto, el archivo puede contener caracteres no pertenecientes al juego ISO-8859-1. (ID-10331, 14984)
- Ahora se añade más información al mensaje de flujo de trabajo cuando un aprobador trata de aprobar o rechazar un elemento de trabajo que ya ha sido aprobado o rechazado. (ID-11045)
- Identity Manager proporciona ahora el servicio de flujo de trabajo `auditPolicyScan`. Puede utilizar esta llamada de servicio de flujo de trabajo para explorar un usuario a fin de detectar infracciones de directivas de auditoría en función de las directivas asignadas al usuario. Si no se ha asignado ninguna directiva al usuario, se utilizará una directiva asignada a la organización, si existe alguna. Consulte la sección *Adiciones y correcciones de la documentación* de estas notas de la versión para obtener más información. (ID-12589)
- Se ha asignado el tipo de autorización (authType) RoleAdminTask a Manage Role TaskDefinition y se ha asignado el tipo de autorización ResourceAdminTask a Manage Resource TaskDefinition. (ID-12768)

Problemas corregidos en versiones anteriores

En esta sección se detallan problemas corregidos desde Identity Installation Pack 2005Q4M3.

Instalación y actualización

- El proceso de actualización ya no sobrescribe la plantilla de correo electrónico de revisión de acceso. (ID-13216)

Interfaz de administrador

- Al configurar una nueva acción de usuario para el menú de applet de usuario, las teclas de texto aparecen ahora correctamente. (ID-8400)
- Identity Manager gestiona ahora correctamente las presentaciones de ayuda que causaban errores cuando contenían caracteres especiales. (ID-8747)
- Cuando el atributo singleLoginSessionPerApp de una aplicación de inicio de sesión se define como true, Identity Manager se comporta como se indica a continuación: un usuario puede iniciar una sesión en la misma aplicación más de una vez. No obstante, la última sesión que inicie el usuario será la única activa y válida. Si el usuario intenta realizar una tarea mientras tiene otra sesión iniciada como el mismo usuario de Identity Manager, el sistema le expulsará automáticamente y la sesión terminará. (ID-9543)
- Cuando un usuario se asigna directamente a una organización, y una regla UserMemberRule asigna también ese usuario a la misma organización, el usuario ya no aparecerá duplicado en la lista. (ID-10410)
- La página de inicio de sesión de tiempo de espera de la sesión se puede localizar ahora y aparecerá en el idioma especificado por la configuración regional del usuario. (ID-10571)
- El formulario LDAP Password Sync de muestra (sample/forms/LDAPPasswordActiveSyncForm.xml) define ahora el campo `waveset.password` en lugar de `password.password` y `password.confirmpassword`. (ID-11660)
- La interfaz de administrador de Identity Manager ya no genera errores cuando los resultados de búsqueda incluyen un nombre de usuario que contiene una comilla simple, y ese nombre se utiliza en un vínculo para un comando posterior. (ID-11123)
- Los componentes MultiSelect muestran ahora correctamente cadenas sencillas. (ID-11979)

- Identity Manager mostrará el mensaje correcto de error si intenta editar un tipo de objeto de recurso que no admita actualizaciones. (ID-12242)
- Al utilizar la tabla de árbol para enumerar recursos, los nodos con nombres que contienen caracteres de subrayado se expanden ahora correctamente. (ID-12478)
- La ayuda en línea muestra ahora las páginas correctas de ayuda cuando se seleccionan opciones sin asistente en el submenú de configuración de ActiveSync. (ID-12597)
- Ahora puede eliminar correctamente usuarios cuando utilice la configuración regional de idioma francés. (ID-12642)
- La tabla de árbol, la página de cuentas y la página Find Results muestran ahora un atributo Manager no resuelto como nombre del administrador de Identity Manager entre paréntesis. Cada vez que se actualiza el usuario, Identity Manager intenta resolver el atributo Manager no resuelto. Si resuelve el atributo, Identity Manager quitará el paréntesis y realizará la comprobación de restricciones en el nuevo valor. (ID-12726)
- El vínculo de la bandeja de entrada para inicio de sesión de usuario anónimo está dirigido ahora a la nueva tabla de lista de elementos de trabajo de usuario final. (ID-12816)
- Ahora puede incluir botones del componente TabPanel. (ID-12797)
- Identity Manager convierte ahora las plantillas de correo electrónico que tienen el valor mail.example.com predeterminado a la nueva función de variable de configuración del servidor. (ID-12720)
- Los campos de contraseña aparecen ahora de forma condicional cuando la interfaz de usuario de Identity Manager no incluye el módulo de inicio de sesión LH, y al usuario se le asigna un rol de administrador. (ID-12692)
- Identity Manager muestra ahora listas de grupos de recursos a las que se accede desde la ficha de recursos en el orden en que se guardó la lista. (Anteriormente, los recursos estaban ordenados.) (ID-14117)
- Ahora puede encontrar roles con muchas organizaciones mediante la página Buscar Roles sin que aparezca un error de ObjectGroup. (ID-15303)
- Cuando se desasignan cuentas de recurso a un usuario mediante la funcionalidad de edición de usuario, la SITUACIÓN de las cuentas en el índice de cuenta ya se actualiza correctamente en todos los casos. (ID-15310)
- La ficha Roles > Buscar Roles > menú Aprobadores ya pueden mostrar usuarios con la capacidad “Aprobador de rol”. (ID-15373)
- Se ha corregido un problema donde Internet Explorer falla cuando una URL tiene más de 2.000 caracteres. (ID-15801)
- Si se utiliza Internet Explorer 6 o 7 con actualización de seguridad 912812, ya no es necesario que los usuarios hagan doble clic en un cuadro de selección múltiple para resaltarlo ni en un elemento para moverlo. (ID-15824)

- Al especificar `true` para `IAPI.cancel` (que cancela las actualizaciones pendientes detectadas para el usuario que se esté procesando) en el formulario de entrada de ActiveSync, la vista del usuario ya no permanece bloqueada después de procesarse. (ID-15912)
- Ahora se devuelven resultados válidos al realizar una búsqueda de usuario en la que se seleccione la opción “Users organization” (Organización de usuarios), así como otras opciones de búsqueda. (ID-16076)
- En la página Buscar rol, la lista de aprobadores aparece ahora ordenada. (ID-16392)
- El componente DatePicker funciona correctamente en todas las zonas horarias. (ID-16618)

Editor de proceso de negocio

- Puede mostrar y editar valores negativos (en segundos) para tiempos de espera de acción manual. (ID-9715)
- La selección del atributo **Store en el repositorio de Identity Manager** al editar un atributo MetaView funciona ahora de la manera planificada. (ID-12396)

Formularios

- Identity Manager proporciona nuevos formularios LDAP Create y Update Group de muestra que admiten nombres de miembro no exclusivos. (ID-8831)
- Los componentes MultiSelect gestionan ahora correctamente elementos con etiquetas idénticas (nombres de presentación). (ID-10964)
- La longitud máxima predeterminada del componente Text es ahora ilimitada (se ha cambiado a partir de 256 caracteres) (ID-11995).
- Los campos de grupos NTForm y NDSUserForm ahora implementan correctamente la regla ListObjects. (ID-12301)
- Los asistentes de recursos del adaptador de host administran mejor los campos affinityAdmin, impidiendo duplicados y entradas nulas. (ID-12024)
- El formulario LDAP Update Group ya no omite ediciones cuando la afiliación de red sigue siendo la misma. (ID-12162)
- El método `listResourceObjects` de `com.waveset.ui.FormUtil` ejecuta ahora correctamente los filtros definidos. Consulte los documentos JavaDocs para obtener información adicional sobre este método. (ID-14422)

Identity Auditor

- Al comprobar directivas durante la creación de usuarios, ya no se crean instancias de tareas adicionales. (ID-10489)

Identity Manager SPE

- Al crear una cuenta de recurso, si ese recurso está inactivo, Identity Manager SPE recordará los valores del atributo de recurso. La próxima vez que ese usuario se edite en Identity Manager SPE, la cuenta se creará en el recurso si se encuentra disponible. (ID-11168)
- Ahora puede inhabilitar eventos objeto de seguimiento en SPE cancelando la selección de “Enable tracked event collection” (Habilitar colección de eventos objeto de seguimiento) en la página **Service Provider > Editar configuración principal**. También puede inhabilitar de forma selectiva en la misma página la recopilación de datos de eventos objeto de seguimiento para cada escala de tiempo. Al igual que con todos los valores de esta página, los objetos de configuración modificados se deben exportar al directorio principal de SPE para que surtan efecto. (ID-12033)
- El método deleteObjects IDMXContext de SPE ahora elimina correctamente objetos del almacén de directorio. (ID-11251)
- El subsistema de auditoría de Service Provider Edition ya no devuelve una excepción de puntero nulo al cerrarse el contenedor. (ID-12845)
- El visualizador IDMXUserViewer devolvía una excepción de puntero nulo si el formulario asociado a las propiedades especificadas de vista era distinto a incluir o destinos, y la asignación de opciones transferida a los métodos del controlador de la vista (crear/proteger/desproteger/actualizar) era nula. (ID-12861)
- Los atributos eliminados de LDAP ahora se propagan una vez que un recurso inactivo vuelve a encontrarse disponible. (ID-15471)

Iniciar sesión

- El inicio de sesión ya no se ralentiza excesivamente al iniciarse una tarea personalizada durante el inicio de sesión. (ID-12377)
- Identity Manager ahora registra correctamente los intentos fallidos de inicio de sesión de administrador para usuarios que no poseen capacidades, organizaciones o capacidades/organizaciones. (ID-12497)

Sincronización de contraseña

- La aplicación de configuración de la sincronización de contraseña (Configure.exe) no trunca las propiedades JMS con el signo de igualdad (=) cuando se leen del repositorio. (ID-12658)
- El `passwordsync.dll` devuelve ahora los mensajes correctos de error correspondientes a fallos de conexión. Así también se solucionan posibles pérdidas de identificadores con los fallos de conexión. (ID-15451)
- Las contraseñas interceptadas con caracteres que estén fuera del rango ASCII de 7 bits se codifican ahora correctamente como UTF-8 antes del cifrado. (ID-15829)

Reconciliación

- Las reconciliaciones no se detienen cuando los usuarios de los recursos están duplicados. (ID-14949)
- Algunas coincidencias de cuentas ambiguas durante la reconciliación se consideran una coincidencia perfecta para evitar errores de reconciliación innecesarios. (ID-14965)
- Las reconciliaciones no se detienen cuando las normalizaciones realizadas por el usuario eliminan toda la información de los recursos de un usuario. (ID-15028)

Informes

- La exploración de cuentas inactivas de Windows 2000 Active Directory (tarea que reside en la barra de menús superior de análisis de riesgos) se realiza ahora correctamente. (ID-11148)
- Ahora puede utilizar el informe de usuario de recursos con más de un usuario. (ID-11420)
- Cuando un administrador delegado ejecuta un informe de usuario, se incluyen ahora los usuarios que son miembros de una organización por una regla UserMembersRule. (ID-11871)
- Cuando se selecciona un nombre de recurso para el eje y de un informe de uso, el valor se utiliza ahora en la consulta. (ID-12035)
- De forma predeterminada, los siguientes informes se ajustarán automáticamente al ámbito del conjunto de organizaciones controlado por el administrador conectado, a menos que se anule explícitamente al seleccionar una o varias organizaciones según las cuales se deba ejecutar el informe. Para admitir esta función, el componente de ámbito de organización se ha cambiado de un componente Select único a otro MultiSelect. (ID-12116)
- Identity Manager ahora audita correctamente modificaciones de afiliación a grupos de LDAP. (Incluye valores antiguos y nuevos.) (ID-12163)

- Ahora es posible personalizar un informe CSV codificado con el juego de caracteres UTF-8 y texto multibyte para poder mostrarlo en aplicaciones que no admiten codificación UTF-8, tal como Microsoft Excel. (ID-13574, 15407)
- Los informes en formato PDF que se envían por correo electrónico mantienen el tipo de fuente y la incorporación de fuente configurados en todos los niveles. (ID-15328)
- Las etiquetas HTML ahora se suprimen en los siguientes informes PDF: (ID-15408)
  - Todos los roles de administrador
  - Todos los administradores
  - Todos los roles
- Los formularios de informes de uso deben especificar ahora un valor de atributo de eje X. (ID-15777)

Repositorio

- El repositorio de Identity Manager realiza ahora la gestión propietaria de Oracle para columnas BLOB. Las secuencias de comandos de ejemplo para Oracle definen ahora la columna xml como tipo de datos BLOB (en lugar de LONG VARCHAR). En instalaciones nuevas, todas las tablas se crearán con columnas xml BLOB. Al realizar una actualización, sólo las tablas nuevas tendrán una columna xml BLOB, pero las tablas restantes se pueden convertir a BLOB realizando los cambios indicados en la secuencia de comandos de actualización (en implementaciones grandes, este proceso de actualización puede tardar varias horas en realizarse). Debe instalar el controlador JDBC de Oracle más reciente para obtener el mejor rendimiento posible con BLOB. (ID-11999)
- El repositorio de Identity Manager se ha cambiado para evitar un bloqueo específico de Microsoft SQL Server 2000. El repositorio utiliza ahora el ID (en lugar del nombre) del LAST_MOD_ITEM cuando selecciona el último valor modificado para un tipo. (ID-12297)
- Los sistemas lentos de bases de datos de Oracle ya no pueden causar tareas suspendidas para ejecutarse en más de un Programador simultáneamente. (ID-15372)
- La eliminación de un rol de un usuario en un grupo similar de usuarios no afecta a las entradas del repositorio pertenecientes a los demás usuarios, y tampoco impide encontrar a dichos usuarios mediante búsquedas por rol. (ID-15584)

Recursos

Puerta de enlace

- La puerta de enlace ya no se bloquea cuando se utilizan API de Identity Manager directamente sin pasar por la interfaz de Identity Manager. (ID-12481)

General

- Puede utilizar de forma segura comillas sencillas en contraseñas. (ID-10043)
- Los asistentes de recursos del adaptador de host administran mejor los campos affinityAdmin, impidiendo duplicados y entradas nulas. (ID-12024)
- Los procesos de Active Sync que se ejecutan en un clúster Websphere utilizando un inicio “Automático con reconexión de emergencia” ya no se bloquean. (ID-12540)
- En algunos adaptadores de recursos, las reglas de exclusión se aplican antes de que se busquen usuarios durante la reconciliación. Esto permite excluir usuarios específicos, impide que el recurso genere errores y puede mejorar el rendimiento de un gran número de usuarios. (ID-14436)
- Identity Manager admite la combinación de funciones deny, ignore para un recurso. La acción no se realiza cuando se selecciona **`ignore`**, pero en algunos casos puede aparecer un mensaje en la GUI. (ID-14948)
- En los casos en los que se utiliza la configuración del sistema para el inicio de sesión de los recursos comunes y falla el inicio de sesión de uno de estos recursos, el fallo deja de producirse si hay otro recurso en la pila de módulos de inicio de sesión que no es un recurso común y que requiere propiedades de autenticación distintas de los recursos anteriores. (ID-15047)
- Active Sync no continúa ejecutándose cuando Crear cuentas sin asignar se configura en verdadero y se supera el número máximo de errores permitidos. (ID-15662)

Directorios

- El adaptador de recursos de Active Directory devolverá ahora una excepción si se especifica un tipo de cifrado no válido. Los valores válidos son nada (vacío), “none”, “kerberos” y “ssl”. (ID-9011)
- Identity Manager ahora agrupa las conexiones de LDAP. (ID-10219)
- La administración de atributos Out of Office de un usuario de Active Directory (Exchange) con habilitación de correo ya no fallará si `msExchHideFromAddressLists` se define como true. Además, el

formulario de usuario de ejemplo de Active Directory se ha actualizado para evitar que Identity Manager muestre atributos Out of Office cuando `msExchHideFromAddressLists` está habilitado. (ID-12231)

- El procesamiento de Active Sync Changelog LDAP gestiona ahora el tipo de cambio MODIFICAR que no tiene ningún valor. (ID-12298)
- El adaptador de recursos de ADSI cierra las conexiones cuando se consultan objetos de recurso. (ID-15098)
- Identity Manager ya no lee atributos de cuenta de sólo escritura del directorio de LDAP ni de Active Directory. (ID-15838)

Mainframe

- En el adaptador de RACF, un cambio realizado en DFLTGRP da como resultado la adición (si es necesario) de DFLTGRP a los grupos (GROUPS) para asegurar que DFLTGRP se pueda definir como el nuevo grupo predeterminado. (ID-9987)
- Las conexiones del adaptador de recursos de mainframe se agrupan correctamente y ya no provocan que las operaciones de mainframe se bloqueen. (ID-12388)
- La emulación de terminal utilizada ahora para crear una cuenta NaturalResourceAdapter admite nombres de usuario de 8 caracteres que no utilizan una ficha para seleccionar el atributo Copy Links. (ID-12503)
- El mecanismo AttrParse de lista de usuarios de RACF predeterminado se ha ampliado para administrar muchas autorizaciones de clase (CLASS AUTHORIZATIONS) y usuarios de plantillas con entradas de grupo como “GROUP SYS1 USER CONNECTION NOT INDICATED”. (ID-15021)
- Si una cuenta de afinidad de recursos de RACF carece de suficientes privilegios para mostrar un usuario, Identity Manager generará un mensaje de error adecuado. (ID-15331)
- Al eliminar cuentas de RACF, el sistema consultará, mediante una máscara de búsqueda, los perfiles de conjuntos de datos que tiene el usuario, enumerará dichos perfiles y eliminará los conjuntos de datos individuales (en contraposición a intentar eliminarlos todos mediante un DELDSD .**). (ID-15413)
- Al borrar un atributo RACF en un formulario, Identity Manager no borraba el atributo en el usuario al enviar el formulario; se trataba de un “noop”. Identity Manager ahora borra el atributo. (ID-15971)
- El adaptador de recursos de Top Secret gestiona ahora correctamente `ASUSPEND`, `PSUSPEND`, `VSUSPEND` y `XSUSPEND` al habilitar e inhabilitar usuarios. (ID-16295)
- Se ha corregido un problema en el adaptador de Top Secret por el que los atributos de usuario incompletos se cargaban. (ID-16334)

Oracle y Oracle ERP

- Durante una sesión con el adaptador de OracleResource, todos los cursores de Oracle se cierran, incluso cuando se producen excepciones. (ID-10357)
- Para los adaptadores de recursos de Oracle y Oracle ERP que se conectan a entornos de Oracle RAC utilizando un controlador fino, utilice el siguiente formato: (ID-10875)

  jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=host01)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host02)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host03)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=PROD)))
- Oracle ERP puede limitar opcionalmente cuentas devueltas por el iterador de cuentas e interfaces listObjects definiendo el atributo de recursos `activeAccountsOnly` como TRUE. El valor predeterminado es FALSE. Cuando se define como FALSE, todas las cuentas del recurso se devuelven. Si se define como TRUE, sólo se devolverán las cuentas con START_DATE y END_DATE que abarquen el valor de SYSDATE (ahora). (ID-12303)
- Los adaptadores de Oracle ERP se han actualizado para cerrar PreparedStatements con mayor coherencia, reduciendo el número de cursores abiertos. (ID-12564)

SAP

- El adaptador de SAP gestiona ahora casos en los que grupos de actividades duplicados se devuelven desde listAllObjects(). (ID-7776)
- El adaptador de SAP proporciona la capacidad de devolver la contraseña temporal generada en el objeto WavesetResult si el adaptador no puede definir una contraseña como no caducada. Esto sólo se produce en las siguientes condiciones:
  - se solicita un cambio de contraseña de administrador y expirePassword = false
  - la contraseña deseada no cumple la directiva de contraseñas de SAP

  El fallo se produce con mayor probabilidad cuando la contraseña deseada ya se encuentra en el historial de contraseñas de SAP.

  El atributo de recursos `Return SAP Temporary Passwords on Failure` se ha creado para habilitar esta capacidad, pero el atributo no funciona todavía. (ID-12185)
- El adaptador de SAP comprueba ahora con mayor eficacia la contraseña de un usuario con respecto a su contraseña actual cuando la solicitud es un cambio de contraseña de administrador y el indicador `expirePassword` es false. Esto evita que se produzca una condición de error cuando la contraseña deseada y la actual del usuario son las mismas. (ID-12447)

- La introducción de perfiles y grupos de actividades de SAP en el entorno de administración de usuario central (CUA) no hace que una nueva fila de la tabla se divida en dos filas cuando la información se separa mediante dos puntos. (ID-14371)

UNIX

- Los adaptadores de UNIX proporcionan la función de reinicialización e inicialización `sudo` básica. No obstante, si se define una acción de recurso y contiene un comando en la secuencia de comandos que requiere autorización `sudo`, deberá especificar el comando `sudo` junto con el comando UNIX. (Por ejemplo, deberá especificar `sudo useradd` en lugar de sólo `useradd`.) Los comandos que requieren `sudo` se deben registrar en el recurso nativo. Utilice `visudo` para registrar estos comandos. (ID-10206)
- Los adaptadores de Red Hat Linux y SuSE Linux rellenan ahora los campos de grupo principal, grupo secundario y último inicio de sesión en procesos de lista globales tales como cargar desde recurso y exportar a archivo. (ID-11627)

  Si el mapa de esquema indica que se debe realizar el seguimiento del campo de último inicio de sesión, el proceso de lista global puede ralentizarse considerablemente, ya que el adaptador debe solicitar individualmente la información de último inicio de sesión de cada usuario.
- Ahora puede asignar el atributo `time_last_login resource` en adaptadores de Solaris, HP-UX y Linux a un nombre de atributo distinto del predeterminado (hora del último inicio de sesión). (ID-11692)
- Si utiliza Create Resource Object para un recurso de servidor Solaris NIS, selecciona varias cuentas en Users y guarda la información, todas las cuentas se añaden al archivo de grupo del directorio fuente de contraseña de NIS del servidor NIS gestionado. Antes sólo se realizaba esta operación si se seleccionaba una cuenta. (ID-15085)
- Identity Manager ya no añade el destino `netid` cuando se utiliza Solaris con configuración NIS, ya que no era necesario y generaba mensajes de error durante el seguimiento. (ID-15503)
- Identity Manager tampoco impide el uso del comando `sudo` con la configuración NIS de Solaris si el directorio que contiene los archivos de plantilla `passwd`, `shadow` y `group` de NIS están protegidos y el administrador no los puede leer. (ID-15505)
- Cuando se utiliza Solaris con configuración NIS tampoco se crea parcialmente una cuenta si falta el grupo principal predeterminado o es un nombre no incluido en el archivo de grupo. (ID-15509)
- Se ha corregido un problema por el que fallaba la generación de ID de grupo o usuario con la configuración NIS de Solaris al comenzar por un entorno sin usuarios o grupos, estando los archivos de plantilla `passwd` y `group` en un directorio distinto a `/etc`. (ID-15510)

- En Solaris con NIS, cuando se crean dos cuentas de una vez y se especifica un intérprete de comandos para la primera pero no para la segunda (no está definida en el archivo `defadduser` o el archivo `defadduser` no existe), la segunda cuenta deja de crearse con el intérprete de comandos de la primera. (ID-15511)
- En la configuración NIS de Solaris, el archivo `/usr/sadm/defadduser` se utiliza como origen opcional de los valores predeterminados de las cuentas recién creadas. En versiones anteriores de Identity Manager, el sistema utilizaba un elemento incorrecto de este archivo para definir el grupo principal predeterminado de un nuevo usuario de Identity Manager. Ahora es el elemento `defgname` el que define correctamente el grupo principal predeterminado. Este valor de grupo principal predeterminado es anulado por el atributo de recursos **Default Primary Group**, que a su vez es anulado por el atributo de cuenta de nombre similar. (ID-15512)
- Identity Manager ya no almacena las contraseñas cifradas de Solaris NIS y HP-UX NIS en los archivos de plantilla `passwd` y `shadow` de NIS cuando se actualiza una cuenta. El marcador de posición “x” se almacena en el archivo `passwd`. (ID-15593)
- Se ha corregido un problema que permitía crear un grupo en un recurso de configuración NIS de Solaris con un nombre o ID de un grupo existente. (ID-15755)
- Al eliminar un usuario de un recurso Solaris, Identity Manager ya no da un resultado positivo falso si el usuario está actualmente conectado al recurso y la eliminación falla. (ID-15761)

Otros

- El adaptador de SecurID UNIX procesa correctamente los atributos de cuenta de usuario del sistema Identity cuando los nombres predeterminados se han cambiado. (ID-10521)
- Si dispone de un recurso Active Sync de componente de PeopleSoft que utilice la interfaz de componente LH_AUDIT_RANGE_COMP_INTF, deberá realizar cambios en el recurso si desea seguir utilizando la interfaz de componente LH_AUDIT_RANGE_COMP_INTF. (ID-11226)

  Confirme que su recurso tiene un atributo de recurso `auditLegacyGetUpdateRows` definido como true.

```
<ResourceAttribute name='auditLegacyGetUpdateRows'
    value='true'
    displayName='Use Legacy Get Update Rows'
    type='boolean'
    multi='false'
    facets='activesync' >
</ResourceAttribute>
```

- Ahora puede eliminar objetos de organización de Sun Access Manager del applet de recursos de Identity Manager. (Identity Manager elimina posteriormente todos los objetos secundarios sin confirmación. (ID-11516)
- Al administrar usuarios de SecurId, Identity Manager admite ahora tres token por usuario. (ID-11723)
- Para el adaptador de tabla de base de datos, las conexiones con bases de datos se cierran ahora lo antes posible durante la iteración y la interrogación, por lo cual se evita retener innecesariamente las conexiones que no se utilicen. (ID-11986)
- El adaptador de JMS Listener ya no falla en Websphere 6.0. Se ha cambiado el procesamiento de mensajes de asíncrono a síncrono, por lo que JMS Listener funciona en servidores J2EE que prohíben el procesamiento asíncrono de mensajes JMS en una aplicación web. La frecuencia de interrogación ahora se debe definir para recursos de JMS Listener. (ID-12654)
- Los adaptadores de SecurID aplican el requisito de RSA por el cual el atributo de inicio de sesión predeterminado únicamente puede contener caracteres ingleses de un solo byte. (!D-13805)
- La puerta de enlace configura correctamente las contraseñas con caracteres fuera del rango ASCII de 7 bits (creación y actualización) cuando Identity Manager se implementa con Tivoli Access Manager y Active Directory. (ID-15006)
- El adaptador de Shell Script ahora detecta e informa del resultado de secuencias de comandos de eliminación que abiertamente se devuelven con un error. (ID-15340)
- El adaptador de tabla de base de datos permite especificar el parámetro de recurso **Volver a enviar todas las SQLExceptions**. Si esta opción no está marcada, se procesarán y eliminarán las excepciones de las sentencias SQL que envíen SQLExceptions con 0 como código de error. (ID-15390)
- Se ha solucionado un problema por el que se producían bloqueos al utilizar Active Sync y el recurso de PeopleSoft. (ID-16109)

Reconciliación

- Al definir una regla ControlledOrganizationRule en el rol de administrador de usuario, ya no se impide que se inicie el daemon de reconciliación. (ID-12695)

Repositorio

- Los mensajes de error del formulario, `com.waveset.util.InternalError: La longitud de la cadena de resumen (2185) supera el valor máximo (2048)` ya no se producen al guardar usuarios u otros objetos. (ID-12492)

Roles

- Los nombres de roles que contienen apóstrofes ya no se truncan al editar roles. (ID-8806)
- Identity Manager gestiona ahora correctamente la adición y eliminación de grupos asignados mediante atributos de roles. (ID-10832)
- Los roles creados en Identity Manager 5.0 y que eran subroles de otros roles incluyen ahora vínculos a sus súper roles. (ID-11477)
- Si se cambia el nombre de un recurso, los atributos de roles seguirán haciendo referencia de forma correcta al recurso correspondiente. (ID-11689)
- Las acciones globales pueden eliminar el rol de waveset.roles cuando contiene un rol solamente. (ID-14568)
- El sistema ahora actualiza correctamente los subroles y súper roles durante una acción SaveAs. (ID-16010)

Seguridad

- Puede suprimir la información detallada de depuración oculta en comentarios HTML definiendo la propiedad `ui.web.disableStackTraceComments` del archivo `Waveset.properties` como true. Si actualiza a partir de una versión anterior de Identity Manager, deberá añadir esta propiedad a config/Waveset.properties. La propiedad se omitirá (lo que equivale a definirla como false) si no está presente en el archivo de propiedades. (ID-10499)
- Los usuarios anónimos pueden acceder ahora a varios tipos de objetos, tales como reglas, sin definir el atributo `endUserAccess` desaprobado del objeto de configuración del sistema. (ID-11248)
- Para configurar esta versión a fin de acceder a un recurso de Clear Trust 5.5.2, deberá instalar el archivo `ct_admin_api.jar` desde el CD de instalación de Clear Trust 5.5.2. No se necesitan bibliotecas adicionales para la comunicación SSL. (ID-12449)
- Durante la creación de un rol de administrador, Identity Manager ahora gestiona correctamente la inclusión y exclusión de todos los tipos de objetos. (ID-12491)
- Los administradores que disponen de las siguientes capacidades pueden acceder ahora a la página de lista de recursos: (ID-12647)
  - Administrador de contraseñas de recursos
  - Cambiar administrador de contraseña de recurso
  - Administrador de reinicialización de contraseñas de recurso
  - Cambiar el administrador de recursos de Active Sync
  - Controlar el administrador de recursos de Active Sync

  - Administrador de reconciliaciones
  - Administrador de peticiones de reconciliación
- Cuando se crea un usuario, se pueden añadir contraseñas al historial de contraseñas del mismo. (ID-15179)
- Un aprobador que no controle la organización superior puede ver ahora las aprobaciones anteriormente aprobadas o rechazadas. (ID-15271)
- Cuando se elimina un usuario que es propietario de los elementos de trabajo pendientes, Identity Manager evita que los elementos de trabajo se pierdan: (ID-15868)
  - Si el elemento de trabajo pendiente ha sido delegado y quien lo ha delegado no se ha eliminado, el elemento se devuelve al delgado, quien vuelve a ser el propietario del mismo.
  - Cuando el elemento de trabajo pendiente se delega y quien lo ha delegado se elimina, o cuando el elemento no se delega, el intento de eliminación no produce efecto hasta que el elemento se resuelve o se remite a otro usuario.

Servidor

- El servidor de aplicación ya no se bloquea al utilizar controladores OCI de Oracle con SSL. (ID-7109)
- Ya no recibirá una excepción de puntero nulo cuando intente iniciar una sesión en el menú de usuario final si el usuario de Identity Manager tiene un rol en un recurso en el que no exista. (ID-12379)
- Ahora la sesión se define correctamente durante las expansiones y derivaciones mientras se procesa la creación de cuentas de recurso en una acción global. (ID-16181)
- En determinadas condiciones, varios servidores podían procesar una tarea programada en una determinada hora de inicio también programada. Ahora esto se ha evitado. (ID-16318)

SOAP

Ahora puede controlar llamadas de SPML 1.0 mediante la función `debug/callTimer.jsp`. La llamada exterior (método `doRequest()` de com.waveset.rpc.SpmlHandler) es más útil para determinar el rendimiento de SOAP/SPML. Los métodos SPML individuales (por ejemplo, `addRequest`) están también sincronizados para facilitar el control. (ID-8463)

Flujo de trabajo

- En determinadas condiciones, un elemento de trabajo caducado se podía editar sin devolverse ningún error. Ahora se devolverá un error indicando que el elemento de trabajo no es válido. (ID-15439)
- La variable de flujo de trabajo WF_ACTION_ERROR se define ahora correctamente cuando se produce un error en el adaptador de recursos de Remedy. (ID-16360)
- Ahora es posible utilizar una plantilla de correo electrónico (emailTemplate) personalizada para las aprobaciones reenviadas. La plantilla de correo electrónico que se utilice se debe especificar en los subprocesos de aprobación por ID. (ID-16468)

Otros problemas corregidos

6496, 8586, 8739, 8958, 8960, 9936, 10235, 10475, 10483, 10832, 11232, 11642, 11767, 11979,12135, 12203, 12234, 12274, 12368, 12377, 12464,12483, 12510, 12585, 12611, 12614, 12673, 12967, 13054, 13338, 13434, 13965, 14044, 14178, 14334, 14792, 14874, 14893, 14899, 15036, 15073, 15219, 15474, 16107, 16282, 16389, 16395, 16610, 17346

Notas sobre la instalación y la actualización

Notas de instalación

- Debe instalar Identity Install Pack de forma manual en HP-UX.
- Para ejecutar Identity Manager con Tomcat 4.1.x, descargue los archivos jar de JSSE a través del sitio web de Sun, `http://java.sun.com/products/jsse/index-103.html`, y guárdelos en el directorio `idm\WEB-INF\lib`.
- Para ejecutar la Puerta de enlace de Sun Identity Manager en Windows NT es preciso instalar la extensión de cliente de Microsoft Active Directory Puede obtener el DSClient en la dirección `http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358`.
- A causa de problemas de licencia, se han eliminado los siguientes archivos jar. (ID-9338) Estos archivos son imprescindibles con los adaptadores de recursos que se indican abajo. A continuación se identifica cada uno de ellos y se ofrece información para obtener el archivo jar del proveedor.

  Adaptador: OS400ResourceAdapter

  URL: `http://jt400.sourceforge.net`

  Proyecto: JTOpen

  JAR: jt400.jar

  Versión: 2.03

  Adaptador: ONTDirectorySmartAdapter

  URL: `http://my.opennetwork.com`

  Proyecto: Directory Smart

  JAR: dsclass.jar, DSUtils.jar

  Versión: n/d

Notas de actualización

Al actualizar Identity Manager, revise la sección de instalación de su servidor de aplicaciones para obtener instrucciones específicas de él. En esta sección se incluye un resumen de tareas para realizar la actualización de la versión 6.0 a 6.0 SP4 de Identity Manager. Para obtener más información, consulte el manual *Identity Manager 6.0 Upgrade*.

Identity Install Pack 2005Q4M3 SP4 se puede actualizar a partir de las siguientes versiones anteriores:

- Identity Manager 6.0 (cualquier nivel de paquete de servicios)
- Identity Auditor 1.7 (cualquier nivel de paquete de servicios)

Nota Si su actual instalación de Identity Manager tiene una gran cantidad de trabajo personalizado, debería ponerse en contacto con Sun Professional Services para recibir asistencia en el proceso de planificación y ejecución de la actualización.

Utilice la información y los procedimientos que se indican a continuación para actualizar Identity Manager.

Nota En algunos entornos, incluido HP-UX, puede que necesite o prefiera seguir los procedimientos de actualización manual alternativos. En ese caso, vaya directamente a la sección *Actualización manual de Identity Manager*.

Nota Identity Manager 6.0 implica un cambio de esquema que introduce tablas nuevas para tareas, grupos, organizaciones y la tabla de syslog. Debe crear estas nuevas estructuras de tablas y trasladar a ellas los datos existentes. Consulte el *Paso 2: Actualice el esquema de la base de datos del repositorio* de la sección *Anexos a la documentación y correcciones* de este documento.

Nota Si edita la plantilla de correo electrónico de aviso de revisión de acceso en la versión 6.0 de Identity Manager, deberá guardar la plantilla antes de actualizar Identity Manager o bien deberá editarla después de realizar la actualización. (El proceso de actualización sobrescribe la plantilla con los valores predeterminados.) (ID-13216)

Paso 1: Actualice el software de Identity Manager

Utilice la información y los procedimientos que se indican a continuación para actualizar Identity Manager.

Notas:

- En algunos entornos, incluido HP-UX, puede que necesite o prefiera seguir los procedimientos de actualización manual alternativos. En ese caso, vaya directamente a la sección *Actualización manual de Identity Manager*.
- En entornos UNIX, asegúrese de que exista el directorio `/var/opt/sun/install` y de que pueda escribir en él.
- Durante la actualización, necesitará conocer la ubicación en la que se encuentra instalado su servidor de aplicaciones.
- Cualquier parche anteriormente instalado se archivará en el directorio `$WSHOME/patches/`*`NombreParche`*.
- Los comandos que figuran en las páginas siguientes son específicos de instalaciones Windows y del servidor de aplicaciones Tomcat. Los comandos utilizados en realidad diferirán en función del entorno específico.

Para actualizar Identity Manager:

1. Cierre la sesión del servidor de aplicaciones.
2. Si está ejecutando la Puerta de enlace de Sun Identity Manager en el servidor Identity Manager, detenga el servicio de puerta de enlace con este comando:

   ```
   gateway -k
   ```
3. Ejecute el comando `install` para iniciar el proceso de instalación.

   Identity Manager muestra el panel de bienvenida.
4. Haga clic en **Siguiente**. Identity Manager muestra el panel Select Installation Directory (Seleccione el directorio de instalación). Seleccione Upgrade (Actualizar) y haga clic en Siguiente.
5. Introduzca una ubicación (o haga clic en **Examinar** para localizarla) para el directorio de instalación de Identity Manager y, a continuación, haga clic en **Siguiente**.
6. Haga clic en **Siguiente** para iniciar la actualización.

   Identity Manager muestra el panel de resumen de la instalación.

Nota Para obtener información detallada sobre la instalación, haga clic en **Details** (Detalles). En función de la cantidad de información capturada durante el proceso de instalación, no todos los mensajes se mostrarán aquí. Consulte el archivo de registro (identificado en Details) para obtener más información. Cuando finalice, haga clic en **Cerrar** para salir del instalador.

7. Suprima todos los archivos compilados de Identity Manager del directorio de trabajo del servidor de aplicaciones.
8. Si el proceso de actualización no lo ha hecho aún, traslade cualquier archivo de clase de parches del directorio `WEB-INF/classes` al directorio `patches/`*`NombreParche`*.

Paso 2: Actualice la Puerta de enlace de Sun Identity Manager

Si está ejecutando la Puerta de enlace de Sun Identity Manager en un sistema remoto, realice los siguientes pasos para actualizarla:

1. Inicie una sesión en el sistema Windows 2000 en el que esté instalada la Puerta de enlace de Sun Identity Manager.
2. Cambie al directorio en el que esté instalada la puerta de enlace.
3. Detenga el servicio de puerta de enlace ejecutando el comando:

   ```
   gateway -k
   ```
4. Si utiliza Windows 2000 o una versión posterior, cierre todas las instancias del plugin Services MMC.
5. Elimine los archivos existentes de la puerta de enlace.
6. Si la puerta de enlace que se acaba de actualizar se instala en un sistema que no sea el servidor de Identity Manager, copie el archivo `gateway.zip` de la ubicación en la que se descomprimió la imagen de instalación.
7. Descomprima el archivo `gateway.zip` en el directorio donde estuviese instalada la puerta de enlace.
8. Ejecute el comando siguiente para iniciar el servicio de puerta de enlace:

   ```
   gateway -s
   ```

También puede iniciar y detener la puerta de enlace realizando los siguientes pasos:

1. Abra el Panel de control de Windows.
2. Abra Servicios. (En Windows 2000, Servicios se encuentra en Herramientas administrativas.)
3. Seleccione Puerta de enlace de Sun Identity Manager.
4. Haga clic en **Start** (Iniciar) o en **Stop** (Detener).

Actualización manual de Identity Manager

En algunos entornos, es posible que deba realizar el procedimiento de actualización de forma manual en lugar de utilizar el programa de instalación y actualización de Identity Manager.

Notas:

- Compruebe que ha configurado la variable de entorno `JAVA_HOME`.
- Asegúrese de que el directorio `bin` de `JAVA_HOME` está definido en las rutas de acceso.
- Cualquier parche anteriormente instalado se archivará en el directorio `$WSHOME/patches/`*`HotfixName`*.
- Antes de realizar la actualización, restaure la cuenta de Configurator incorporada de forma que se llame Configurator y que cuente con la capacidad de importación. Además, se debe configurar la contraseña para esta cuenta. Una vez realizada la actualización, devuelva la cuenta de Configurator al estado en el que se encontraba antes de la actualización. Si es necesario, cambie el nombre de esta cuenta y modifique la contraseña antes de implementarlos en el entorno de producción.

Realice los siguientes pasos para actualizar Identity Manager manualmente:

1. Detenga el servidor de aplicaciones y la Puerta de enlace de Sun Identity Manager.
2. Introduzca la siguiente serie de comandos:

   En plataformas Windows admitidas

   a. Configure su entorno:

   ```
   set SPPATH=Ruta de acceso a los archivos de paquete de servicios
   set WSHOME=Ruta al directorio de instalación de Identity Manager
   O  al directorio de almacenamiento provisional
   set TEMP=Ruta de acceso al directorio temporal
   ```

   b. Ejecute el proceso previo:

   ```
   mkdir %TEMP%
   cd /d %TEMP%
   jar -xvf %SPPATH%\IDPAK2005Q4M3_SP4.jar \
   WEB-INF\lib\idm.jar \ WEB-INF\lib\idmcommon.jar \
   WEB-INF\lib\idmformui.jar
   set TMPLIBPTH=%TEMP%\WEB-INF\lib
   set CLASSPATH=%TMPLIBPTH%\idm.jar;\
   %TMPLIBPTH%\idmcommon.jar;%TMPLIBPTH%\idmformui.jar
   java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
      com.waveset.install.UpgradePreProcess
   ```

c. Instale el software:

```
cd %WSHOME%
jar -xvf %SPPATH%\IDM.jar
```

d. Ejecute el proceso posterior:

```
java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
  com.waveset.install.UpgradePostProcess
```

En plataformas UNIX admitidas

a. Configure su entorno:

`export SPPATH=`***Ruta de acceso a los archivos extraídos de paquete de servicios***
`export WSHOME=`***Ruta al directorio de instalación de Identity Manager***
`O` ***al directorio de almacenamiento provisional***
`export TEMP=`***Ruta de acceso al directorio temporal***

b. Ejecute el proceso previo:

```
mkdir $TEMP
cd $TEMP
jar -xvf $SPPATH/IDPAK2005Q4M3_SP4.jar \
WEB-INF/lib/idm.jar WEB-INF/lib/idmcommon.jar \
WEB-INF/lib/idmformui.jar
CLASSPATH=$TEMP/WEB-INF/lib/idm.jar:\
$TEMP/WEB-INF/lib/idmcommon.jar:\
$TEMP/WEB-INF/lib/idmformui.jar
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME \
com.waveset.install.UpgradePreProcess
```

c. Instale el software:

```
cd $WSHOME
jar -xvf $SPPATH/IDM.jar
```

d. Ejecute el proceso posterior:

```
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME
  com.waveset.install.UpgradePostProcess
```

3. Cambie al directorio `$WSHOME/bin/solaris` o `$WSHOME/bin/linux` y configure los permisos sobre los archivos del directorio para que sean ejecutables.
4. Si ha realizado la instalación en un directorio de montaje, cree un archivo `.war` para la implantación en el servidor de aplicaciones.

Nota Consulte el capítulo correspondiente en Instalación de *Sun Java™ System Identity Manager* para obtener las instrucciones específicas del servidor de aplicaciones.

5. Suprima los archivos de Identity Manager del directorio de trabajo del servidor de aplicaciones.

6. Si el proceso de actualización no lo ha hecho aún, traslade cualquier archivo de clase de parches del directorio `WEB-INF/classes` al directorio `patches/`*`NombreParche`*.
7. Inicie el servidor de aplicaciones.
8. Actualice la base de datos de Identity Manager. Consulte la anterior sección *Paso 2: Actualice la Puerta de enlace de Sun Identity Manager* para obtener instrucciones detalladas.
9. Actualice y, a continuación, reinicie la Puerta de enlace de Sun Identity Manager. Consulte la anterior sección *Paso 2: Actualice la Puerta de enlace de Sun Identity Manager* para obtener instrucciones detalladas.

Anexos a la documentación y correcciones

Acerca de las guías de software del sistema Identity

La documentación de software del sistema Identity está organizada en varias guías, que se suministran en formato de Acrobat (`.pdf`) en el CD Identity Install Pack. La versión incluye las siguientes guías.

Software del sistema Identity

Install Pack Installation (`Identity_Install_Pack_Installation_2005Q4M3.pdf`) — Describe cómo instalar y actualizar el software del sistema Identity.

Identity Manager

- *Identity Manager Administration* (`IDM_Administration_2005Q4M3.pdf`) — Ofrece una introducción a las interfaces de usuario y administrador de Identity Manager.
- *Identity Manager Upgrade* (`IDM_Upgrade_2005Q4M3.pdf`) — Proporciona información que facilita la planificación y ejecución de actualizaciones.

Nota Para esta versión, los documentos *Identity Manager Technical Deployment* e *Identity Manager Technical Reference* se han reorganizado de la forma siguiente:

- *Identity Manager Technical Deployment Overview* (`IDM_Deployment_Overview_2005Q4M3.pdf`) — Resumen conceptual del producto Identity Manager (incluidas arquitecturas de objeto), con una introducción básica a los componentes del producto.
- *Identity Manager Workflows, Forms, and Views* (`IDM_Workflows_Forms_Views_2005Q4M3.pdf`) — Información de referencia y de procedimiento en la que se describe cómo utilizar los flujos de trabajo, los formularios y las vistas de Identity Manager, incluida información sobre las herramientas necesarias para personalizar estos objetos.
- *Identity Manager Deployment Tools* (`IDM_Deployment_Tools_2005Q4M3.pdf`) — Información de referencia y de procedimiento en la que se describe cómo utilizar distintas herramientas de implementación de Identity Manager; también incluye reglas y bibliotecas de reglas, tareas y procesos comunes, compatibilidad con el diccionario y la interfaz del servicio Web basada en SOAP que ofrece el servidor de Identity Manager.

- *Identity Manager Resources Reference* (`IDM_Resources_Reference_2005Q4M3.pdf`) — Información de referencia y de procedimiento en la que se describe cómo cargar y sincronizar datos de cuentas de un recurso en Sun Java™ System Identity Manager. En `ResourcesRef_Addendum_2005Q4M3SP1.pdf` se documentan adaptadores adicionales.
- *Identity Manager Audit Logging* (`IDM_Audit_Logging_2005Q4M3.pdf`) — Información de referencia y de procedimiento en la que se describe cómo cargar y sincronizar datos de cuentas de un recurso en Sun Java™ System Identity Manager.
- *Identity Manager Tuning, Troubleshooting, and Error Messages* (`IDM_Troubleshooting_2005Q4M3.pdf`) — Información de referencia y de procedimiento en la que se describen los mensajes de error y las excepciones de Identity Manager; también proporciona instrucciones para realizar un seguimiento y solucionar problemas que puedan surgir durante el trabajo.

Identity Auditor

Identity Auditor Administration (`IDA_Administration_2005Q4M3.pdf`) - Ofrece una introducción a la interfaz del administrador de Identity Auditor.

Identity Manager Service Provider Edition

- *Identity Manager Service Provider Edition Administration Addendum* (`SPE_Administration_Addendum_2005Q4M3SP1.pdf`) – Presenta las funciones de Identity Manager SPE.
- *Identity Manager Service Provider Edition Deployment* (`SPE_Deployment_2005Q4M3_SP1.pdf`) – Proporciona información para implementar Identity Manager SPE.

Utilización de las guías en línea

Para desplazarse por las guías, utilice la función Marcadores de Acrobat. Haga clic en el nombre de una sección en el panel de marcadores para desplazarse a la posición que ocupa dicha sección en el documento.

La serie de documentos de Identity Manager se puede consultar desde cualquier instalación de Identity Manager desplazándose hasta `idm/doc` en el explorador Web.

Install Pack Installation

Correcciones

Prefacio

Se ha eliminado de la sección How to Find Information in this Guide la referencia cruzada errónea al Apéndice H. (ID-12369)

Capítulo 1: Antes de la instalación

- Se ha eliminado de la tabla de recursos admitidos Microsoft Exchange 5.5 como recurso admitido. Se ha invalidado. (ID-12682)
- Se ha añadido Lotus Notes® 6.5.4 (Domino) como recurso admitido a la tabla de recursos admitidos. (ID-12226)
- Se ha añadido JDK 1.5 como versión admitida de Java en varias instancias. (ID-12984)
- Se ha modificado la información de sistemas ERP SAP en la tabla de recursos admitidos de: (ID-12635)
  - SAP® R/3 v4.5, v4.6
  - SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
  - SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
  - SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)
- Se ha modificado la información de Red Hat en la tabla de recursos admitidos de:
  - Red Hat Linux Advanced Server 2.1
  - Red Hat Linux Enterprise Server 3.0, 4.0
- Se ha añadido la sección Servidores de repositorio de bases de datos y la siguiente información en Software y entornos admitidos: (ID-12425)
  - IBM® DB2® Universal Database para Linux, UNIX® y Windows® (Versión 7.x, 8.1, 8.2)
  - Microsoft SQL Server™ 2000
  - MySQL™ 4.1
  - Oracle 9i® y Oracle Database 10g, 10gR1 y 10gR2®

Capítulo 2: Instalación de Identity Install Pack para Tomcat

En el capítulo se proporciona asistencia para el servidor de aplicaciones Apache Tomcat, versiones 4.1.x o 5.0.x.

Capítulo 4: Instalación de Identity Install Pack para WebSphere

- En el capítulo se trata la instalación de Websphere 5.1 Express y 6.0. (ID-12655, 12656) Se han añadido las siguientes notas e información en los puntos indicados:

Nota No es necesario realizar el siguiente paso al instalar Identity Install Pack 6.0 o una versión posterior.

4. Cambiar al directorio de montaje y eliminar los siguientes archivos, si existen:

```
WEB-INF\lib\cryptix-jce-provider.jar
WEB-INF\lib\cryptix-jce-api.jar
```

25. Descargar el `jlog package` más reciente desde WebSphere en:

```
http://www.alphaworks.ibm.com/tech/loggingtoolkit4j
```

Nota El `jlog package` está ya incorporado en WebSphere'6.0. Descárguelo sólo para versiones anteriores.

- Como necesita instalar JDK 1.4.2 en esta versión, la sección *For JDK 1.3.x:* ya no es aplicable. En el mismo capítulo, debe cambiar la sección *For JDK 1.4* por *For JDK 1.4.2*.

Capítulos 7/8: Instalación de Identity Install Pack para Sun ONE/Sun Java System Application Server 7/8

- Se ha añadido la siguiente información corregida en los pasos de instalación > Paso 5: Edite el archivo server.policy > permisos de ejemplo: (ID-12292)

```
permission java.io.FilePermission
"/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/
idm/config/trace1.log", "read,write,delete";

permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",
"read,write,delete";
```

- Se ha añadido la siguiente información en los pasos de instalación > Paso 5: Edite el archivo server.policy > permisos de ejemplo:

  Si desea ejecutar con Identity Manager Service Provider Edition, añada el siguiente permiso a las anteriores entradas del archivo server.policy.

```
permission java.lang.RuntimePermission "shutdownHooks";
```

Capítulo 14: Desinstalación de aplicaciones

Se ha eliminado `_Version_` del ejemplo de sintaxis existente en Suprima el software > en UNIX > Paso 3. (ID-7762)

Capítulo 15: Instalación de las aplicaciones (instalación manual)

Ejemplo de sintaxis corregido en los pasos de instalación > Paso 3: Configure la identidad `Install Pack Index Database Connection > Non-Xwindows Environments > Step 3 to:` (ID-5821)

3. Defina su clave de licencia con los siguientes comandos:

```
cd idm/bin
./lh license set -f LicenseKeyFile
```

Apéndice A: Referencia de las bases de datos de índice

La fila en la que se describe SQL Server se ha cambiado por lo siguiente:

Si su selección es:	Introduzca
SQL Server **Valores predeterminados que se deben utilizar con el controlador JDBC de Microsoft SQL Server 2005:** • **URL:** "jdbc:sqlserver://host.your.com:1433;DatabaseName=dbname" • **Controlador JDBC** com.microsoft.sqlserver.jdbc.SQLServerDriver • **Conectarse como usuario:** waveset Utilice los siguientes valores con el controlador JDBC de Microsoft SQL Server 2000: • **URL:** "jdbc:microsoft:sqlserver://host.your.com:1433;DatabaseName=dbname;SelectMethod=Cursor" • **Controlador JDBC** com.microsoft.jdbc.sqlserver.SQLServerDriver • **Conectarse como usuario:** waveset	Introduzca la ubicación de la base de datos de índice y la contraseña que seleccionó al configurar la base de datos. **Nota:** Todas las conexiones a SQL Server se deben realizar utilizando la misma versión del controlador JDBC. Esto incluye el repositorio y todos los adaptadores de recursos que administren o requieran tablas o cuentas de SQL Server, incluyendo los adaptadores de Microsoft SQL, de Microsoft Identity Integration Server, de tabla de base de datos, de JDBC con secuencia de comandos, así como cualquier adaptador personalizado que se base en estos adaptadores. Se producirán errores por conflictos si intenta utilizar versiones distintas del controlador.

Apéndice C: Configuración de las fuentes de datos para Identity Manager

- No se admiten múltiples URL IIOP. (ID-12499) Se ha eliminado la siguiente información incorrecta en Configuración de una fuente de datos de WebSphere para Identity Manager > Configuración de una fuente de datos de Websphere 5 > Configure la fuente de datos en un clúster de Websphere:

  Si los servidores de aplicaciones no tienen el mismo puerto especificado en la propiedad **BOOTSTRAP_ADDRESS**, se podrán especificar múltiples URL mediante java.naming.provider.url, por ejemplo:

  `iiop://localhost:9812,iiop://localhost:9813.`

- Todas las propiedades j2c.properties utilizadas en la versión 5 de WebSphere forman parte ahora del archivo resources.xml en la versión 6 de WebSphere. Se ha añadido información sobre la configuración de una fuente de datos de Websphere 5.1/6.x y sobre la configuración de los datos de autenticación de 6.x. Se ha eliminado información de configuración de una fuente de datos de Websphere 4.x. (ID-12767) Los cambios afectan a las siguientes secciones:

Configuración de un proveedor de JDBC

Utilice la consola de administración de WebSphere para configurar un proveedor de JDBC nuevo.

1. Haga clic en la ficha **Resources** del panel izquierdo para mostrar una lista de tipos de recursos.
2. Haga clic en **JDBC Providers** para mostrar la tabla de proveedores de JDBC configurados.
3. Haga clic en el botón **Nuevo** situado sobre la tabla de proveedores de JDBC configurados.
4. Seleccione en la lista de tipos de base de datos JDBC, el tipo jdbc y el tipo de implementación. Haga clic en Siguiente.

   En este ejemplo se utilizará la fuente de datos de grupo de conexión, controlador de JDBC de Oracle y Oracle.
5. Continúe con la configuración de las propiedades generales.
   - Especifique el nombre.
   - Especifique en el campo **Classpath** la ruta al JAR que contiene el controlador de JDBC. Por ejemplo, para especificar el controlador fino de Oracle, especifique una ruta similar a la siguiente:

     ```
     /usr/WebSphere/AppServer/installedApps/idm/idm.ear/idm.war/WEB-INF/lib/oraclejdbc.jar
     ```

     Nota Puede utilizar la consola de administración para especificar la ruta al JAR que contiene el controlador de JDBC. En el menú **Environment**, seleccione el elemento de menú **WebSphere Variable**. En ese panel, elija primero la **celda**, el **nodo** y el **servidor** para los que se va a definir esta variable de entorno. A continuación, especifique la ruta al JAR como valor de esta variable.

   - Especifique el nombre totalmente cualificado de la clase de controlador de JDBC en el campo **Implementation ClassName**.
     - Para el controlador fino de Oracle, este valor es `oracle.jdbc.pool.OracleConnectionPoolDataSource`.
     - Para el controlador db2 jcc, este valor es com.ibm.db2.jcc.DB2ConnectionPoolDataSource.
   - Puede cambiar también el nombre o descripción del proveedor a lo que elija.

     Cuando termine, haga clic en el botón **Aceptar** de la parte inferior de la tabla. El proveedor que se ha añadido debe aparecer en el panel derecho.

Para configurar una fuente de datos que utilice este proveedor de JDBC, consulte “Señale el repositorio de Identity Manager a la fuente de datos”.

Configuración de una fuente de datos de JDBC Websphere

1. Utilice la consola de administración de WebSphere para definir una fuente de datos con un proveedor de JDBC existente. Si es necesario definir un proveedor de JDBC nuevo para utilizarlo con Identity Install Pack, consulte “Configuración de un proveedor de JDBC”.

Para poder finalizar la configuración de la fuente de datos, debe configurar los datos de autenticación. Estos alias contienen credenciales que se utilizan para conectarse al sistema de gestión de base de datos (DBMS).

Configure los datos de autenticación de 5.1

1. Haga clic en la ficha **Seguridad** del panel izquierdo para mostrar una lista de tipos de configuración de seguridad.
2. Haga clic en la ficha **JAAS Configuration** del panel izquierdo para mostrar una lista de tipos de configuración de JAAS.
3. Haga clic en la ficha **J2C Authentication Data** del panel izquierdo. En el panel derecho se muestra una tabla de entradas de datos de autenticación.
4. Haga clic en el botón **Nuevo** situado sobre la tabla de entradas de datos de autenticación. En el panel derecho aparece una tabla de propiedades generales que se pueden configurar.
5. Configure las propiedades generales relativas a la nueva entrada de datos de autenticación. Tenga en cuenta lo siguiente:
   - **Alias** es el nombre que se mostrará en la lista de selección cuando alguien configure las credenciales del DBMS para una fuente de datos.
   - **UserID** es el nombre utilizado para conectarse al DBMS.
   - **Password** es la contraseña utilizada para conectarse al DBMS.

A continuación, configure la fuente de datos.

Configure los datos de autenticación de 6.x

1. Haga clic en **Security > Global security**.
2. En Authentication, haga clic en **JAAS configuration > J2C authentication data**. Aparece el panel **J2C Authentication Data Entries**.
3. Haga clic en **Nuevo**.
4. Introduzca un alias exclusivo, un ID de usuario válido, una contraseña válida y una descripción breve (opcional).
5. Haga clic en **Aceptar** o en **Apply**. No es necesario validar el ID de usuario ni la contraseña.

6. Haga clic en **Save**.

Nota La entrada recién creada se puede ver sin necesidad de reiniciar el proceso del servidor de aplicaciones para utilizarla en la definición de la fuente de datos. No obstante, la entrada sólo será efectiva tras reiniciar el servidor.

Configure la fuente de datos

Nota Si va a configurar una fuente de datos en un clúster de Websphere 5.x, consulte “Configure la fuente de datos en un clúster de Websphere” para obtener más información.

1. Haga clic en la ficha **Resources** del panel izquierdo para mostrar una lista de tipos de recursos.
2. Haga clic en **JDBC Providers** para mostrar la tabla de proveedores de JDBC configurados.
3. Haga clic en el nombre de un proveedor de JDBC de la tabla. En el panel derecho se muestra una tabla de propiedades generales configuradas para el proveedor de JDBC seleccionado.
4. Desplácese hacia abajo a una tabla de propiedades adicionales. Haga clic en **Data Sources**. En el panel derecho se muestra una tabla de fuentes de datos configuradas para utilizarlas con este proveedor de JDBC.

Nota Tenga en cuenta el campo **Scope** situado en la parte superior del marco existente en la consola de administración de WebSphere. Compruebe que **Node** y **Server** están en blanco de forma que aparezca la información de celda para la configuración debajo de los botones **Nuevo** y **Borrar**.

5. Haga clic en el botón **Nuevo** situado sobre la tabla de fuentes de datos. En el panel derecho aparece una tabla de propiedades generales para configurarlas.
6. Configure las propiedades generales relativas a la nueva fuente de datos. Tenga en cuenta lo siguiente:
   - **JNDI Name** (Nombre de JNDI) es la ruta al objeto DataSource en el servicio de directorio.
     Debe especificar este mismo valor como argumento `-f` en `setRepo -t`*`dbms`* `-i`*`initCtxFac`* `-f`*`rutaarchivo`*.
   - **Container-managed persistence** (Persistencia gestionada por contenedores) no debe marcarse. Identity Install Pack no utiliza EJB (Enterprise Java Beans).
   - **Component-managed Authentication Alias** (Alias de autenticación gestionado por componentes) señala a los credenciales que se utilizarán para acceder al DBMS (al que señala esta fuente de datos).
   - Seleccione en la lista desplegable el alias que contiene el conjunto adecuado de credenciales de DBMS. Para obtener más información, consulte *Configure los datos de autenticación de 5.1*.

- **Container-managed Authentication Alias** (Alias de autenticación gestionado por contenedores) no se utiliza. Defina este valor como `(none)`. Identity Install Pack realiza su propia conexión al DBMS (al que señala esta fuente de datos).
- Haga clic en **Aceptar** cuando haya configurado este panel. Aparece la página Data Sources.

7. Haga clic en la fuente de datos que ha creado. A continuación, desplácese hacia abajo a la tabla de propiedades adicionales situada cerca de la parte inferior. Haga clic en el vínculo **Custom Properties**.

   En el panel derecho se muestra una tabla de propiedades específicas del DBMS.

8. Configure las propiedades personalizadas para esta fuente de datos. Haga clic en el vínculo de cada propiedad para definir su valor. Tenga en cuenta lo siguiente:
   - **URL** es la única propiedad necesaria. Esta URL de base de datos identifica la instancia de base de datos y contiene los valores driverType, serverName, portNumber y databaseName. Puede especificar también algunos de estos valores como propiedades individuales.
   - **driverType** en este ejemplo es fino.
   - **serverName** es un nombre de host (o una dirección IP).
   - **databaseName** es normalmente un nombre corto de base de datos.
   - **portNumber** es 1521 de forma predeterminada para Oracle.
   - Puede resultar adecuado configurar **preTestSQLString** en un valor tal como SELECT 1 FROM USEROBJ. Esta consulta SQL confirma que la tabla USERJOB existe y que se puede acceder a ella.
9. En la tabla de propiedades adicionales, también puede hacer clic en el vínculo **Connection Pool** si desea configurar estas propiedades para ajustar el rendimiento.

Apéndice E: Configuración de JCE

Debe aparecer una nota como se indica a continuación:

Nota Como debe instalar JDK 1.4.2 en esta versión, todos los entornos admitidos deberían incluir una extensión criptográfica de Java (JCE) 1.2. La información de este apéndice ya no sirve.

Información añadida

Capítulo 1: Antes de la instalación

- Se ha añadido la siguiente nota en Setup Task Flow > Bullet Install y configure el software de Identity Install Pack: (ID-8431)

Nota En sistemas Unix o Linux:

  - Al instalar Identity Install Pack, versiones 5.0 - 5.0 SP1, `/var/tmp` debe existir y el usuario que ejecute el instalador debe poder escribir en él.
  - Al instalar Identity Install Pack, versiones 5.0 SP2 y posteriores, `/var/opt/sun/install` debe existir y el usuario que ejecute el instalador debe poder escribir en él.

- Se ha añadido la siguiente nota a Prerequisite Tasks > Set Up an Index Database > Setting Up SQL Server > paso 3b: (ID-11835)

Nota Los siguiente archivos deben estar en el directorio `$WSHOME/WEB-INF/lib`:

```
db2jcc
db2jcc_license_cisuz.jar or db2jcc_license_cu.jar
```

- Se ha añadido la siguiente nota en Software y entornos admitidos > Servidores de aplicaciones: (ID-12385)

Nota El contenedor actual de servidores de aplicaciones debe admitir UTF-8.

Capítulo 2: Instalación de Identity Install Pack para Tomcat

- Se ha añadido el siguiente paso a los pasos de instalación > Paso 1: Instale el software Tomcat > Instalación en UNIX: (ID-12487)

  2. Añada los archivos Java `mail.jar` y `activation.jar` al directorio `./tomcat/common/lib`. Los archivos jar de correo y activación se encuentran en:

```
http://java.sun.com/products/javamail
http://java.sun.com/products/beans/glasgow/jaf.html
```

- Se han añadido los siguientes pasos a los pasos de instalación > Paso 1: Instale el software Tomcat > Instalación en UNIX: (ID-12462)

3. Al configurar Tomcat para admitir UTF-8, añada el atributo `URIEncoding="UTF-8"` al elemento *conector* del *`DIR TOMCAT`*`\`, `archivo conf/server.xml`, por ejemplo:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on the port
specified during installation -->
<Connector port="8080"
            maxThreads="150"
            minSpareThreads="25"
            maxSpareThreads="75"
            enableLookups="false" redirectPort="8443"
            acceptCount="100" debug="0" connectionTimeout="20000"
            disableUploadTimeout="true"
            URIEncoding="UTF-8" />
```

4. Cuando configure Tomcat para admitir UTF-8, añada también `-Dfile.encoding=UTF-8` en las opciones Java VM.

Capítulo 13: Actualización de Identity Manager

Se ha añadido una referencia cruzada a la actualización de Identity Manager para facilitar a los usuarios la búsqueda de información completa de actualización. (ID-12366)

Capítulo 15: Instalación de las aplicaciones (instalación manual)

Se ha añadido la siguiente nota en los pasos de instalación > Paso 2: Instale el software de aplicación: (ID-8344)

Nota A partir de la versión 5.0 SP3, las clases de adaptador se incluyen ahora en el archivo `idmadapter.jar`. Si dispone de un adaptador personalizado, es posible que deba actualizar la ruta de la clase.

Apéndice B: Configuración de MySQL

Se ha añadido la siguiente información en Configuración de MySQL > paso 3 Inicie el proceso de MySql: (ID-12461)

Si este proceso no se ha iniciado, utilice los siguientes pasos para registrar e iniciar MySQL.
En Windows, si está realizando la instalación en un directorio distinto de `c:\mysql`, cree un archivo llamado `c:\my.cnf` con el siguiente contenido:

```
[mysqld]
basedir=d:/mysql/
default-character-set=utf8
default-collation=utf8_bin
```

En Windows, instale e inicie el servicio:

```
cd <MySQL_Install_Dir>/bin
mysqld-nt --install
net start mysql
```

Apéndice C: Configuración de las fuentes de datos para Identity Manager

Se ha añadido la siguiente información en Configuración de una fuente de datos de WebSphere para Identity Manager > Señale el repositorio de Identity Manager a la fuente de datos: (ID-12071)

8. Señale el repositorio a la nueva ubicación. Por ejemplo:

```
lh -Djava.ext.dirs=$JAVA_HOME/jre/lib/ext:$WAS_HOME/lib setRepo
-tdbms -iinitCtxFac
-frutaarchivo -uiiop://localhost:bootstrap_port
-Unombreusuario
-Pcontraseña
-toracle icom.ibm.websphere.naming.WsnInitialContextFactory -
fRutaFuenteDatos
```

En el anterior ejemplo, la variable *RutaFuenteDatos* podría ser `jdbc/jndiname`. `bootstrap_port` es el puerto de dirección del código de inicio del servidor WebSphere.

La opción `-Djava.ext.dirs` añade a la CLASSPATH todos los archivos JAR de los directorios `lib/` y `java/jre/lib/ext/` de WebSphere. Esto es necesario para que el comando setrepo se ejecute con normalidad.

Cambie la opción `-f` a fin de que coincida con el valor especificado para el campo **JNDI Name** (Nombre JNDI) al configurar la fuente de datos. Consulte la referencia setrepo para obtener más información sobre este comando.

Actualización de Identity Manager

Información añadida

Capítulo 1: Descripción general de la actualización

Se ha añadido el siguiente elemento a la sección *Example Upgrade*: (ID-12467)

Tenga cuidado al editar el campo de super rol en el formulario Role. El super rol en sí puede ser un rol anidado. Los campos de super rol y subrol indican un anidamiento de roles y sus grupos de recursos o recursos asociados. Cuando se aplica a un usuario, el super rol incluye los recursos asociados a algún subrol designado. El campo de super rol se muestra para indicar los roles que incluyen el rol mostrado.

Capítulo 3: Desarrollo del plan de actualización

Se ha añadido lo siguiente a la sección Upgrade the Environment Upgrade From Identity Manager 5.x to 6.x. (ID-12361)

Paso 2: Actualice el esquema de la base de datos del repositorio

Identity Manager 6.0 implica un cambio de esquema que introduce tablas nuevas para tareas, grupos, organizaciones y la tabla de syslog. Debe crear estas nuevas estructuras de tablas y trasladar a ellas los datos existentes.

Nota Antes de actualizar el esquema del repositorio, haga una copia de seguridad completa de las tablas que contiene.

1. Identity Manager utiliza dos tablas para almacenar objetos de usuario. Se pueden utilizar secuencias de comandos de ejemplo (en el directorio `sample`) para realizar cambios de esquema.

   Consulte la secuencia de comandos `sample/upgradeto2005Q4M3.`*`NombreBaseDatos`* para actualizar las tablas del repositorio.

Nota La actualización de las bases de datos de MySQL tiene que ver bastante con este proceso. Consulte `sample/upgradeto2005Q4M3.mysql` para obtener más información.

Guía de Identity Manager Administration

Información añadida

- Cuando se configura la provisión, al crear un usuario se genera un elemento de trabajo que se puede ver mediante la ficha **Approvals**. Cuando se aprueba este elemento, se anula la fecha de provisión y se crea la cuenta. La creación de la cuenta se cancela si se rechaza el elemento.
- Cuando programe la reconciliación, podrá proporcionar el nombre de la regla que quiera utilizar para personalizar el programa. Por ejemplo, la regla puede retrasar las reconciliaciones programadas para un sábado hasta el lunes siguiente. (ID-11391)

Capítulo 4: Administración

- Se ha añadido información sobre la función de delegación de aprobaciones. (ID-12754)

Delegación de aprobaciones

Si dispone de capacidades de aprobador, podrá delegar sus futuras solicitudes de aprobación a uno o más usuarios (delegados) durante un determinado periodo de tiempo. No es necesario que los usuarios dispongan de capacidades de aprobador para ser delegados.

La función de delegación se aplica solamente a futuras solicitudes de aprobación. Las solicitudes existentes (las enumeradas en la ficha En espera de aprobación) se reenvían mediante la función de reenvío.

Para configurar delegaciones, seleccione la ficha **Delegar mis aprobaciones** en el área **Aprobaciones**.

Notas

- Podrá acceder a la función de delegación si se le ha asignado alguna capacidad que le conceda el derecho a delegar a WorkItem o cualquier extensión de authType de WorkItem, incluyendo Approval, OrganizationApproval, ResourceApproval y RoleApproval; o cualquier subtipo personalizado que amplíe WorkItem o uno de sus authTypes.
- También puede delegar aprobaciones en la ficha de formulario Seguridad de las páginas Crear, Editar o Ver usuario, y en el menú principal de interfaz de usuario.

Los delegados pueden aprobar solicitudes durante el periodo de delegación efectivo en su nombre. En las solicitudes de aprobación delegadas se incluye el nombre del delegado.

Entradas de registro de auditoría para solicitudes

En las entradas de registro de auditoría de solicitudes de aprobación aprobadas y rechazadas se incluirá su nombre (del delegador) si la solicitud se ha delegado. Los cambios realizados en la información del aprobador delegado de un usuario se registrarán en la sección de cambios detallados de la entrada de registro de auditoría cuando se crea o se modifica un usuario.

Capítulo 5: Configuración

- Se ha añadido información sobre la configuración de atributos de identidad al crear o actualizar un recurso. (ID-12606)

Configuración de atributos de identidad desde cambios de recursos

Los atributos de identidad definen cómo se relacionan entre sí los atributos en recursos. Cuando un recurso se crea o se modifica, estas relaciones entre atributos pueden verse afectadas.

Cuando se guarda un recurso, Identity Manager muestra la página ¿Configurar Atributos de identidad?. Aquí, puede elegir lo siguiente:

- Pasar a la configuración de atributos de identidad desde la página Resource Changes y configurar atributos. Haga clic en **Sí** para continuar.
- Volver a la lista de recursos. Haga clic en **No** para volver.
- Inhabilitar esta página para futuras actualizaciones de recursos. Haga clic en **No preguntar de nuevo** para inhabilitar la página.

Nota El botón **No preguntar de nuevo** sólo lo pueden ver los usuarios que disponen de capacidades para modificar la metavista.

Página Re-enabling the Configure Identity Attributes?

Si esta página está inhabilitada, utilice uno de estos métodos para volver a habilitarla:

- Utilizar la función de depuración de Identity Manager para editar el objeto WSUser del usuario que haya iniciado la sesión. Cambie el valor de la propiedad `idm_showMetaViewFromResourceChangesPage` a un valor `true`.
- Añadir al formulario de usuario un campo similar al siguiente ejemplo (por ejemplo, el formulario de usuario con fichas) y, a continuación, utilizar la página Edit User para cambiar el valor de esta configuración:

```
<Field name='accounts[Lighthouse].properties.displayMetaViewPage'>
  <Display class='Checkbox'>
    <Property name='label' value='Display Meta View?'/>
  </Display>
</Field>
```

Configuración de atributos

Utilice la función de configuración de atributos de identidad en la página Resource Changes para seleccionar atributos de los mapas de esquema de recursos modificados a fin de utilizarlos como fuentes y destinos para los atributos de identidad. En algunos casos, no es posible seleccionar atributos en las columnas Source (Origen) y Target (Destino). No podrá seleccionar un atributo como fuente si:

- Está marcado como cifrado en el mapa de esquema
- Está marcado como sólo escritura en el mapa de esquema

No podrá seleccionar un atributo como destino si:

- Hay un atributo de identidad almacenado globalmente con el mismo nombre. Por ejemplo, si hay un atributo de identidad global llamado “nombredepila”, se seleccionará la opción de destino de nombre de pila y no se podrá anular la selección.
- El atributo está marcado como sólo lectura en el mapa de esquema.
- Las funciones de creación y actualización de cuentas del recurso están inhabilitadas o no son admitidas por el recurso.

Capítulo 7: Seguridad

- Se ha añadido la siguiente nota a la sección “Configuring Authentication for Common Resources”. (ID-16805)

  Todos los recursos enumerados en un grupo de recursos comunes se deben incluir también en la definición del módulo de inicio de sesión. Si no aparece también una lista completa de recursos comunes en la definición del módulo de inicio de sesión, la funcionalidad de recursos comunes no funcionará correctamente.

- Se ha añadido información sobre limitaciones de inicio de sesiones concurrentes. (ID-12778)

Limitación de inicio de sesiones concurrentes

De forma predeterminada, un usuario de Identity Manager puede tener sesiones concurrentes iniciadas. No obstante, es posible limitar las sesiones concurrentes a una por aplicación de inicio de sesión cambiando el valor del atributo de configuración `security.authn.singleLoginSessionPerApp` en el objeto de configuración del sistema. Este atributo es un objeto que contiene un atributo por cada nombre de aplicación de inicio de sesión (por ejemplo, la interfaz de administrador, la interfaz de usuario o BPE). Al cambiar el valor de este atributo a `true`, se garantiza una sola sesión por cada usuario.

Si se aplica, un usuario se podrá conectar a más de una sesión; no obstante, sólo la última sesión iniciada estará activa y será válida. Si el usuario realiza una acción en una sesión no válida, el sistema le expulsará automáticamente de la sesión y ésta terminará.

Capítulo 8: Informes

En la sección Summary Reports, la descripción de informe de usuario incluye ahora la capacidad de buscar usuarios por administrador: (ID-12690)

- **User**: ver usuarios, los roles que tienen asignados y los recursos a los que pueden acceder. Al definir un informe de usuario, puede seleccionar los usuarios que se deben incluir por nombre, administrador asignado, rol, organización o asignación de recursos.

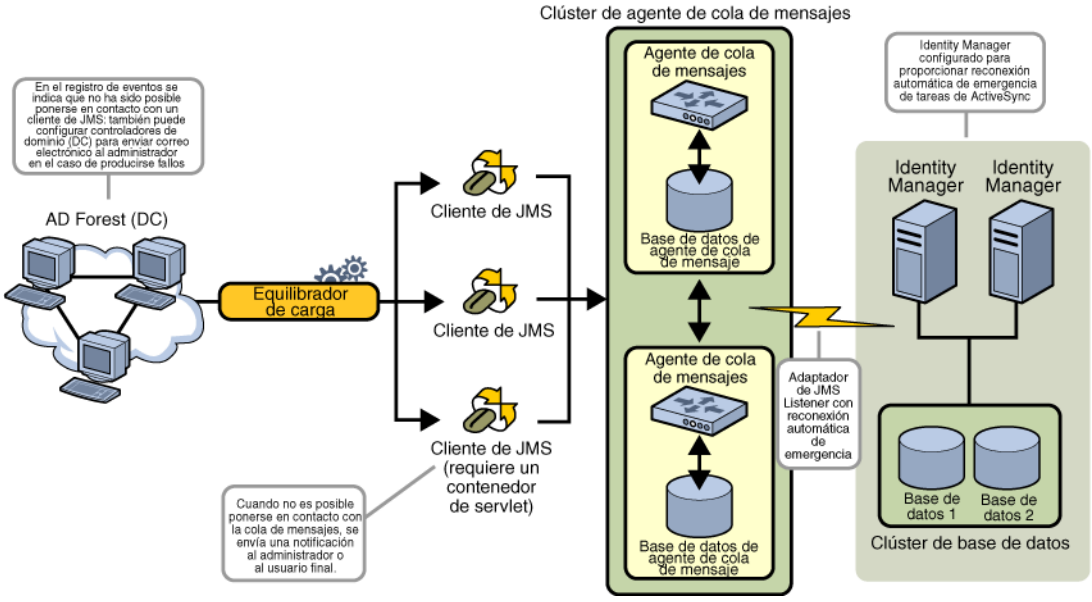
Capítulo 10: PasswordSync

- Se han añadido instrucciones para configurar PasswordSync de Windows con un servidor Sun JMS. Consulte el documento *Configuring PasswordSync with a Sun JMS Server* que se suministra con estas notas de la versión. (ID-11788)
- Se ha añadido la siguiente sección para describir la arquitectura de alta disponibilidad con reconexión de emergencia para PasswordSync. (ID-12634)
- Se ha añadido una sección en la que se describe cómo implementar PasswordSync sin utilizar Java Messaging Server. (ID-14974)

Implantación de la reconexión de emergencia para PasswordSync de Windows

La arquitectura de PasswordSync permite eliminar los puntos de fallos en la implantación de sincronización de contraseñas de Windows para Identity Manager.

Si configura cada controlador Active Directory Domain Controller (ADC) para conectarse a uno en una serie de clientes de JMS a través de un equilibrador de carga (consulte la siguiente figura), los clientes de JMS podrán enviar mensajes a un clúster de agente de cola de mensajes (Message Queue Broker), lo que garantiza que no se pierda ningún mensaje si falla alguna cola de mensajes.



Nota El clúster de cola de mensajes requerirá probablemente una base de datos para la persistencia de mensajes. (Las instrucciones para configurar un clúster de agente de cola de mensajes se deben proporcionar en la documentación del producto de su distribuidor.)

El servidor de Identity Manager que ejecuta el adaptador de JMS Listener configurado para la reconexión automática de emergencia se pondrá en contacto con el clúster de agente de cola de mensajes. Aunque el adaptador se ejecuta sólo en un Identity Manager cada vez, si falla el servidor de ActiveSync principal, el adaptador comenzará a interrogar con respecto a mensajes relacionados con contraseñas en un servidor de Identity Manager secundario y a propagar cambios de contraseña a recursos de flujo inferior.

Implementación de PasswordSync sin Java Messaging Service

Para implementar PasswordSync sin JMS, inicie la aplicación de configuración con el siguiente indicador:

```
Configure.exe -direct
```

Cuando se especifica el indicador `-direct`, la aplicación de configuración muestra la ficha User. Configure PasswordSync mediante los procedimientos descritos en “Configuración de PasswordSync”, con las siguientes excepciones:

- No configure las fichas JMS Settings y JMS Properties.

- En la ficha User, especifique el ID de cuenta y la contraseña que se utilizarán para conectarse a Identity Manager.

Si implementa PasswordSync sin JMS, no será necesario crear un adaptador de JMS Listener. Por tanto, deberá omitir los procedimientos indicados en “Implementación de PasswordSync”. Si desea configurar notificaciones, es posible que deba modificar el flujo de trabajo de Cambiar contraseña de usuario.

Nota Si posteriormente ejecuta la aplicación de configuración sin especificar elindicador `-direct`, PasswordSync requerirá que se configure un JMS. Vuelva a iniciar la aplicación con el indicador `-direct` para omitir de nuevo el JMS.

Correcciones

Capítulo 5: Recursos

En la tabla de clases de recursos personalizados, la clase de recurso personalizado para el adaptador de recurso ClearTrust se ha corregido de la siguiente forma: (ID-12681)

```
com.waveset.adapter.ClearTrustResourceAdapter
```

Capítulo 10: PasswordSync

En la sección Configuring PasswordSync, en JMS Settings Dialog, la siguiente descripción de Queue Name (Nombre de cola) se ha corregido como se indica a continuación:

- **Queue Name** especifica el nombre de búsqueda del destino (Destination Lookup Name) para los eventos de sincronización de contraseñas. (ID-12621)

Referencia lh

La sintaxis de comandos se ha actualizado para indicar correctamente un espacio después de opciones especificadas. (ID-12798)

Al utilizar la opción -p, por motivos de seguridad, *Password* se debe especificar como ruta a un archivo de texto que contenga una contraseña, en lugar de especificarse directamente en la línea de comandos.

Ejemplos

- `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 de licencia

Utilización

```
license [options] { status | set {parameters} }
```

Opciones

- `-U nombreusuario` (si se cambia el nombre de la cuenta de Configurator)
- `-P RutaaContraseña.txt` (si se cambia la contraseña de Configurator)

Los parámetros de la opción `set` deben tener el formato `-f` *Archivo*.

Identity Manager Workflows, Forms, and Views

Capítulo 1: Flujos de trabajo

El tratamiento de acciones manuales de este capítulo debe contener la siguiente información:

Si el tipo `itemType` de un elemento de trabajo se define como asistente, el elemento de trabajo omitirá de forma predeterminada obtener aprobadores de reenvío al comprobar la vista WorkItem. Si el tipo itemType se define en un valor distinto al asistente, Identity Manager recuperará aún así los aprobadores de reenvío, a menos que `CustomUserList` se defina en el valor “true” como propiedad del formulario que se utiliza con la acción manual. (ID-10777)

Para ello, incluya el siguiente código en el formulario:

```
<Formulario>
   <Properties>
      Property name='CustomUserLists' value='true'/>
   </Properties>
```

Capítulo 2: Servicios de flujo de trabajo

- La tabla de argumentos del servicio de flujo de trabajo de sesión `createView` es incorrecta. En la tabla siguiente se describen los argumentos disponibles en este servicio.

Nombre	Requerido	Valores válidos	Descripción
op	sí	`createView`	
viewid	sí		Especifica el tipo de vista que se crea.
options	no		Indica las opciones específicas de la vista. Los valores posibles dependen de la vista utilizada. La más frecuente es la vista de usuario. Las opciones se halan en `session.UserViewConstants`. Las vistas más simples deben declarar sus constantes de opción en el archivo `Viewer.java`. Posiblemente, la segunda vista de flujo de trabajo más utilizada sea ProcessViewer, seguida de PasswordViewer, DisableViewer, EnableViewer y RenameViewer. En comparación tienen pocas opciones.

- Identity Manager proporciona el método de servicio de flujo de trabajo `checkStringQualityPolicy`, que comprueba el valor de una cadena designada frente a una directiva de cadena. (ID-12428, 12440)

Nombre	Requerido	Valores válidos	Descripción
directiva	sí		Identifica la directiva (Cadena)
map	no		Proporciona un mapa de los datos que la cadena no debe contener (Mapa). `returnNull` (opcional): si se define en “true”, el método devolverá un objeto nulo al ejecutarse correctamente.
value	sí		Especifica el valor de la cadena que se comprobará. (Objeto)
historialcontraseñas	no		Enumera las contraseñas anteriores del usuario en mayúsculas y en formato cifrado.
propietario	sí		Identifica el usuario cuyo valor de cadena se está comprobando.

  El método devuelve un objeto `checkPolicyResult`. El valor `true` indica que la cadena supera la prueba de directiva. Si la cadena no supera la prueba de directiva, el método devolverá un mensaje de error. Si ha definido la opción `returnNull` en el valor “true” en el parámetro `map`, el método devolverá un objeto nulo al ejecutarse correctamente.

- Identity Manager proporciona ahora el servicio de flujo de trabajo auditPolicyScan (ID-12615). Utilice este servicio de flujo de trabajo para explorar un usuario a fin de detectar infracciones de directivas de auditoría en función de las directivas asignadas al usuario. Si no se ha asignado ninguna directiva al usuario, Identity Manager utilizará una directiva asignada a la organización, si existe alguna.

  Este método incluye un argumento, *vista*, que especifica la vista del usuario especificado. Devuelve la variable de flujo de trabajo checkPolicyResult. Esta variable incluirá:

  - una lista de infracciones
  - o un valor nulo, si no se produce ninguna infracción

Capítulo 3: Formularios

Identity Manager puede identificar en pantalla si es necesario un atributo en el mapa de esquema de un recurso. El formulario Edit User identifica estos atributos mediante un asterisco (*). De forma predeterminada, Identity Manager muestra este asterisco después del campo de texto que sigue al nombre de atributo. (ID-10662)

Para personalizar la colocación del asterisco, siga estos pasos:

1. Mediante el BPE de Identity Manager o su editor de XML, abra el objeto de configuración de propiedades de componentes (Component Properties).
2. Añada `EditForm.defaultRequiredAnnotationLocation=left` a la etiqueta `<SimpleProperties>`.

   Entre los valores válidos para `defaultRequiredAnnotationLocation` se incluyen left (izquierda), right (derecha) y none (ninguno).
3. Guarde los cambios y reinicie el servidor de aplicaciones.

Capítulo 4: Métodos FormUtil

- Identity Manager proporciona el nuevo método FormUtil `checkStringQualityPolicy`, que comprueba el valor de una cadena designada frente a una directiva de cadena. (ID-12428, 12440)

  checkStringQualityPolicy(ContextoLighthouse s, Cadena directiva, Objeto valor, Mapa mapa, Lista historialcontraseñas, Cadena propietario)

Parámetro	Descripción
ContextoLighthouse	Especifica el contexto de Lighthouse del usuario actual.
directiva	(Necesario) Especifica el nombre de la directiva con respecto a la que se comprobará la cadena.
value	(Necesario) Identifica el valor de cadena para su comprobación.
map	(Opcional) Proporciona un mapa de los datos que no deben incluirse en la cadena. `returnNull` (opcional): si se define en `true`, el método devolverá un objeto nulo al ejecutarse correctamente
historialcontraseñas	(Opcional) Enumera las contraseñas anteriores del usuario en mayúsculas y en formato cifrado.
propietario	(Necesario) Identifica el usuario cuyo valor de cadena se está comprobando.

Este método devuelve el valor “true” que indica que la cadena supera la prueba de directiva. Si la cadena no supera la prueba de directiva, el método devolverá un mensaje de error. Si ha definido la opción `returnNull` en el valor “true” en el parámetro `map`, el método devolverá un objeto nulo al ejecutarse correctamente.

- Identity Manager proporciona ahora el método FormUtil `controlsAtLeastOneOrganization`. (ID-9260)

  controlsAtLeastOneOrganization(ContextoLighthouse s, Lista organizaciones)

  devuelve WavesetException {

  Determina si un usuario actualmente autenticado controla alguna de las organizaciones especificadas en una lista de uno o varios nombres de organizaciones (ObjectGroup). En la lista admitida de organizaciones se incluyen las que se han devuelto al enumerar todos los objetos del tipo ObjectGroup.

Parámetro	Descripción
s	Especifica el contexto (sesión) de Lighthouse del usuario actual.
organizations	Especifica una lista de uno o varios nombres de organizaciones. En la lista admitida de organizaciones se incluyen las que se han devuelto al enumerar todos los objetos del tipo ObjectGroup.

Este método devuelve:

`true`: indica que el usuario de Identity Manager actual autenticado controla alguna de las organizaciones de la lista.

`false`: indica que el usuario de Identity Manager actual autenticado no controla ninguna de las organizaciones de la lista.

Capítulo 5: Vistas

Tipos de cuenta

Esta versión de Identity Manager proporciona compatibilidad para asignar a los usuarios varias cuentas en un recurso con *tipos de cuenta*. (ID-12697) Opcionalmente, puede asignar ahora un tipo de cuenta en un recurso al asignar recursos a un usuario, con las siguientes limitaciones:

- Todas las cuentas de un recurso pueden ser de un tipo (y sólo de uno).
- Los usuarios tienen normalmente sólo una cuenta de un determinado tipo.

Un administrador debe definir primero un tipo de cuenta en un recurso para poder asociarlo a un recurso. Se debe definir también una regla de identidad. (Consulte el archivo samples/identityRules.xml para obtener ejemplos de reglas de identidad.)

Identity Manager utiliza el subtipo de regla de identidad para asociar una regla a un tipo de cuenta. Esta regla genera `accountIds` según sea necesario. (Estas reglas funcionan de forma similar a la plantilla de identidad, pero se implementan en XPRESS y pueden acceder a la API de LighthouseContext).

Consulte *Identity Manager Administration* para obtener información sobre cómo utilizar la interfaz de administrador de Identity Manager para asignar tipos de cuenta a recursos.

Omisión del tipo de cuenta

Si omite un tipo de cuenta en un recurso, Identity Manager asignará el tipo de cuenta predeterminado, que proporciona compatibilidad con versiones anteriores. No obstante, si ningún recurso tiene un tipo de cuenta definido, esta función se inhabilitará.

El tipo de cuenta predeterminado utiliza la plantilla de identidad. No obstante, puede especificar también que el tipo predeterminado utilice una regla especificada en lugar de la plantilla de identidad.

El tipo de cuenta predeterminado es exclusivo, ya que el usuario puede asignar múltiples cuentas de ese tipo. No obstante, se recomienda no asignar múltiples cuentas del mismo tipo.

Cambios relacionados con vistas

Los siguientes cambios en las vistas de Identity Manager admiten tipos de cuenta.

- La vista de recursos cuenta ahora con un atributo `accountType` (Lista). Cada entrada es un objeto con un atributo `identityRule`, que asigna un nombre a la regla utilizada para generar `ID de cuenta` para este tipo.

- El atributo `resources` de las vistas de roles y de aplicaciones permite ahora utilizar asignaciones de recursos cualificadas. La sintaxis de estas asignaciones cualificadas es `<resource name>|<account type>`.

- La vista de usuario contiene ahora el atributo `waveset.resourceAssignments`, que toma asignaciones de recursos cualificadas. (`waveset.resources` contiene sólo referencias no cualificadas.) Puede cambiar cualquiera de los atributos, pero se recomienda utilizar sólo `waveset.resourceAssignment` para actualizaciones y `waveset.resources` para sólo lectura.)

La forma de acceder a los objetos del atributo `accounts` de la vista de usuario no ha cambiado con la adición de esta nueva función. Utilice nombres de recursos cualificados para indexar la lista `accounts` (por ejemplo, `accounts[resource|type]` selecciona la cuenta de recursos para esa combinación de recurso y tipo. Si no especifica un tipo, podrá acceder de todas formas a estos objetos a través de `accounts[resource]`.)

- Las vistas relacionadas, incluidas Deprovision y Change Password, utilizan también este tipo de tratamiento. Los objetos de esta lista tienen ahora también un nuevo `accountType` de atributo, que especifica el tipo de cuenta de recurso.

Vista de aprobadores delegados

Utilice esta vista para asignar uno o varios usuarios de Identity Manager como aprobadores delegados a un aprobador existente. Ello permite que un aprobador delegue sus capacidades de aprobación durante un determinado periodo de tiempo a usuarios que pueden no ser aprobadores. Entre los atributos de alto nivel se incluye: (ID-12754)

Nota La vista de usuario contiene estos mismos atributos (con la excepción del atributo de nombre). Estos nuevos atributos se incluyen en las cuentas[Lighthouse]. namespace.

name

Identifica al usuario que delega aprobaciones.

delegateApproversTo

Especifica a quién delega aprobaciones el usuario donde los valores válidos incluyen manager, selectedUsers o delegateApproversRule.

delegateApproversSelected

- Si `selectedUsers` es el valor de `delegateApproversRule`, enumerará los nombres de los usuarios seleccionados.
- Cuando el valor de `delegateApproversTo` es `delegatedApproversRule`, identifica la regla seleccionada.
- Este atributo no tiene valor cuando `manager` es el valor de `delegateApproversTo`.

delegateApproversStartDate

Especifica la fecha de inicio de la delegación de aprobaciones. De forma predeterminada, la hora de la fecha de inicio seleccionada es 12:01 de la noche de ese día.

delegateApproversEndDate

Especifica la fecha de finalización de la delegación de aprobaciones. De forma predeterminada, la hora de la fecha de finalización seleccionada es 11:59 de la noche de ese día.

La documentación de la vista de roles se ha actualizado de la siguiente forma. (ID-12390)

Vista de roles

Se utiliza para definir objetos de rol de Identity Manager.

Cuando se marca, esta vista inicia el flujo de trabajo de administración de roles. De forma predeterminada, este flujo de trabajo sencillamente asigna los cambios de la vista al repositorio, pero también proporciona conexiones para aprobaciones y demás personalizaciones.

En la siguiente tabla se enumeran los atributos de alto nivel de esta vista.

Atributo	¿Editable?	Tipo de datos	Requerido
`name`	Leer/Escribir	Cadena	Sí
`resources`	Leer/Escribir	Lista	No
`applications`	Leer/Escribir	Lista	No
`roles`	Leer/Escribir	Lista	No
`assignedResources`	Leer/Escribir	Lista	No
`notifications`	Leer/Escribir	Lista	No
`approvers`	Leer/Escribir	Lista	No
`properties`	Leer/Escribir	Lista	
`organizations`	Leer/Escribir	Lista	Sí

Tabla 1. Atributos de la vista de roles

name

Identifica el nombre del rol. Se corresponde con el nombre de un objeto de rol del repositorio de Identity Manager.

resources

Especifica los nombres de recursos asignados localmente.

applications

Especifica los nombres de aplicaciones asignadas localmente (grupos de recursos).

roles

Especifica los nombres de roles asignados localmente.

assignedResources

Lista sencilla de todos los recursos asignados mediante recursos, aplicaciones y roles.

Atributo	¿Editable?	Tipo de datos
`resourceName`		Cadena
`name`		Cadena
`attributes`		Objeto

resourceName

Identifica el nombre del recurso asignado.

name

Identifica el nombre o ID de recurso (preferiblemente ID).

attributes

Identifica las características del recurso. Todos los subatributos son cadenas y se pueden editar.

Atributo	Descripción
`name`	Nombre de atributo de recursos
`valueType`	Tipo de valor definido para este atributo. Entre los valores permitidos se incluye Rule, text o none.
`requirement`	Tipo de valor definido por este atributo. Entre los valores permitidos se incluye Rule, Text, None, Value, Merge with Value, Remove with Value, Merge with Value clear existing, Authoritative set to value. Authoritative merge with value, Authoritative merge with value clear existing.
`rule`	Especifica el nombre de regla si el tipo de valor es Rule.
`value`	Especifica el valor si el tipo de regla es Text.

Tabla 2. Opciones de atributo (vista de roles)

- `notifications`: enumera los nombres de administradores que deben aprobar la asignación de este rol a un usuario.
- `approvers`: especifica los nombres de los aprobadores que deben aprobar la asignación de este rol a un usuario.
- `properties`: identifica las propiedades definidas por el usuario que están almacenadas en este rol.
- `organizations`: enumera organizaciones de las que este rol es miembro.
- Las vistas de cuentas de recursos (vistas Deprovision, Disable, Enable, Password, Rename User, Reprovision y Unlock) admiten ahora dos nuevas opciones que se pueden utilizar a fin de obtener atributos de cuentas de recursos para el usuario. (ID-12482)
  - `fetchAccounts` (booleano): permite que la vista incluya atributos de cuenta para los recursos asignados al usuario.
  - `fetchAccountResources`: enumera nombres de recursos para elegirlos. Si no se especifica, se utilizarán todos los recursos asignados.

  Puede definir estas opciones con mayor facilidad como propiedades de formulario. (Para obtener más información, consulte la sección dedicada a la vista de listas de elementos de trabajo (WorkItem List) en el capítulo de vistas de esta guía.)

Capítulo 6: Lenguaje XPRESS

- La función `instanceOf` no está actualmente documentada en el capítulo de lenguaje XPRESS. Esta función identifica si un objeto es una instancia del tipo especificado en el parámetro `name`. (ID-12700)

  `name`: identifica el tipo de objeto con respecto al que se está realizando la comprobación.

  Esta función devuelve 1 o 0 (“true” o “false”) dependiendo de si el objeto de subexpresión es una instancia del tipo especificado en el parámetro `name`.

  La siguiente expresión devuelve 1 al ser ArrayList una lista.

```
<instanceof name='List'>
   <new class='java.util.ArrayList'/>
</instanceof>
```

Capítulo 8: Componentes de visualización HTML

- La descripción del componente SortingTable se ha revisado de la siguiente forma:

  Utilícelo para crear una tabla cuyo contenido se pueda ordenar por cabecera de columna. Los componentes secundarios determinan el contenido de esta tabla. Cree un componente secundario por columna (definido por la propiedad `columns`). Las columnas están normalmente incluidas en un bucle de campo.

  Este componente respeta las propiedades `align`, `valign` y `width` de los componentes secundarios al generar las celdas de la tabla. (ID-12606)

- Identity Manager proporciona ahora el componente de visualización InlineAlert. (ID-12606)

  Muestra un cuadro de alerta informativo, de error, de advertencia o de ejecución correcta. Este componente se encuentra normalmente en la parte superior de una página. Se pueden visualizar varias alertas en un solo cuadro definiendo componentes secundarios de tipo `InlineAlert$AlertItem`.

  Las propiedades para este componente de visualización incluyen:

  - `alertType`: especifica el tipo de alerta para su visualización. Esta propiedad determina los estilos e imágenes que se utilizarán. Los valores válidos son error, warning, success e info. El valor predeterminado de esta propiedad es info. Esta propiedad es sólo válida para `InlineAlert`.
  - `header`: especifica el título que se muestra para el cuadro de alerta. Puede ser una cadena o un objeto de mensaje. Esta propiedad es válida para `InlineAlert` o `InlineAlert$AlertItem`.
  - `value`: especifica el mensaje de alerta que se muestra. Este valor puede ser una cadena o un objeto de mensaje. Esta propiedad es válida para `InlineAlert` o `InlineAlert$AlertItem`.
  - `linkURL`: especifica una URL opcional que aparece en la parte inferior de la alerta. Esta propiedad es válida para `InlineAlert` o `InlineAlert$AlertItem`.
  - `linkText`: especifica el texto para la `linkURL`. Puede ser una cadena o un objeto de mensaje. Esta propiedad es válida para `InlineAlert` o `InlineAlert$AlertItem`.
  - `linkTitle`: especifica el título para la `linkURL`. Puede ser una cadena o un objeto de mensaje. Esta propiedad es válida para `InlineAlert` o `InlineAlert$AlertItem`.

Ejemplos

Mensaje de alerta único

```
<Field>
   <Display class='InlineAlert'>
      <Property name='alertType' value='warning'/>
      <Property name='header' value='Data not Saved'/>
      <Property name='value' value='The data entered is not yet saved.
          Please click Save to save the information.'/>
   </Display>
</Field>
```

Mensajes de alerta múltiples

Defina `alertType` sólo en la propiedad `InlineAlert`. Puede definir otras propiedades en `InlineAlert$AlertItems`.

```
<Field>
   <Display class='InlineAlert'>
      <Property name='alertType' value='error'/>
   </Display>
   <Field>
     <Display class='InlineAlert$AlertItem'>
        <Property name='header' value='Server Unreachable'/>
        <Property name='value' value='The specified server could not
       be contacted. Please view the logs for more information.'/>
        <Property name='linkURL' value='viewLogs.jsp'/>
        <Property name='linkText' value='View logs'/>
        <Property name='linkTitle' value='Open a new window with
           the server logs'/>
     </Display>
  </Field>
  <Field>
     <Display class='InlineAlert$AlertItem'>
        <Property name='header' value='Invalid IP Address'/>
        <Property name='value' value='The IP address entered is
       in an invalid subnet. Please use the 192.168.0.x subnet.'/>
     </Display>
  </Field>
</Field>
```

- Identity Manager proporciona ahora el componente de visualización Selector. (ID-12729)

  Proporciona un campo con uno o varios valores (similar a los componentes Text o ListEditor, respectivamente) con campos de búsqueda debajo. Tras realizar una búsqueda, Identity Manager muestra los resultados debajo de los campos de búsqueda e introduce los resultados en el campo de valor.

  A diferencia de otros componentes de contenedor, `Selector` cuenta con un valor (el campo que se rellena con los resultados de `search`). Los campos incluidos son normalmente campos de criterios de búsqueda. `Selector` implementa una propiedad para mostrar el contenido de los resultados de la búsqueda.

  Las propiedades incluyen:

  - `fixedWidth`: especifica si el componente debe tener un ancho fijo (el mismo comportamiento que Multiselect). (Booleano)
  - `multivalued`: indica si el valor es una lista o una cadena. (El valor de esta propiedad determina si el campo ListEditor o Text se representa para el valor.) (Booleano)
  - `allowTextEntry`: indica si los valores se deben seleccionar en la lista suministrada o si se pueden introducir manualmente. (Booleano)
  - `valueTitle`: especifica la etiqueta que se utiliza en el componente `value`. (Cadena)
  - `pickListTitle`: especifica la etiqueta que se utiliza en el componente `picklist`. (Cadena)
  - `pickValues`: valores disponibles en el componente picklist (si es nulo, el picklist no se mostrará). (Lista)
  - `pickValueMap`: mapa de etiquetas de visualización para los valores incluidos en el picklist. (Mapa o Lista)
  - `sorted`: indica que los valores se deben ordenar en el picklist (si hay varios valores y no están ordenados, la lista de valores se ordenará también). (Booleano)
  - `clearFields`: enumera los campos que deben reinicializarse cuando se selecciona el botón Clear. (Lista)

  Las siguientes propiedades son sólo válidas en un componente de varios valores:

  - `ordered`: indica que el orden de los valores es importante. (Booleano)
  - `allowDuplicates`: indica si la lista de valores puede contener duplicados. (Booleano)
  - `valueMap`: proporciona un mapa de etiquetas de visualización para los valores de la lista. (Mapa)

Estas propiedades son válidas solamente en un componente de un solo valor:

- `nullLabel`: especifica una etiqueta que se utiliza para indicar un valor nulo. (Cadena)

- Las descripciones de los componentes `Select` y `MultiSelect` se han revisado de la siguiente forma para incluir información sobre la propiedad `caseInsensitive`. (ID-13364)

Componente MultiSelect

Muestra un objeto de selección múltiple, que Identity Manager muestra como dos teclas de selección de texto, una al lado de la otra, en las que un conjunto definido de valores en un cuadro se puede desplazar a otro cuadro. Los valores del cuadro izquierdo se definen mediante la propiedad `allowedValues`; los valores se obtienen a menudo dinámicamente llamando a un método Java tal como `FormUtil.getResources`. Los valores mostrados en el cuadro derecho de selección múltiple se rellenan a partir del valor actual del atributo de vista asociado, que se identifica mediante el nombre de campo.

Puede definir los títulos de formulario para cada cuadro de este objeto de selección múltiple mediante las propiedades `availabletitle` y `selectedtitle`.

Si desea un componente `MultiSelect` que no utilice un applet, defina la propiedad `noApplet` en el valor “true”.

Nota Si ejecuta Identity Manager en un sistema que utilice el explorador Safari, deberá personalizar todos los formularios que contengan componentes MultiSelect para definir la opción noApplet. Defina esta opción como se indica a continuación:

```
<Display class='MultiSelect'>
      <Property name='noApplet' value='true'/>
 ...
```

Las propiedades para este componente de visualización incluyen:

- `availableTitle`: especifica el título del cuadro disponible.
- `selectedTitle`: especifica el título del cuadro seleccionado.
- `ordered`: define si los elementos seleccionados se pueden desplazar hacia arriba o hacia abajo en la lista de elementos del cuadro de texto. El valor `true` indica que se representarán botones adicionales para poder desplazar los elementos seleccionados hacia arriba o hacia abajo.
- `allowedValues`: especifica los valores asociados al cuadro izquierdo del objeto de selección múltiple. Este valor debe ser una lista de cadenas. **Nota**: El elemento `<Constraints>` se puede utilizar para rellenar este cuadro, pero su uso se ha invalidado.

- `sorted`: especifica que los valores de ambos cuadros se ordenarán alfabéticamente.
- `noApplet`: especifica si el componente MultiSelect se implementará con un applet o con dos cuadros de selección HTML estándar. El valor predeterminado es utilizar una miniaplicación, que puede administrar mejor listas largas de valores. Consulte la nota anterior para obtener información sobre la utilización de esta opción en sistemas que utilicen el explorador Safari.
- `typeSelectThreshold` (disponible solamente cuando la propiedad `noApplet` se define en el valor “true”): controla si aparece un cuadro de selección de escritura anticipada en la lista `allowedValue`. Cuando el número de entradas del cuadro de selección izquierdo alcanza el umbral definido por esta propiedad, aparece un campo de entrada de texto adicional debajo del cuadro de selección. Al introducir caracteres en este campo de texto, el cuadro de selección se desplaza para mostrar la entrada coincidente si existe alguna. Por ejemplo, si introduce **w**, el cuadro de selección se desplazará a la primera entrada que empiece por **w**.
- `width`: especifica el ancho del cuadro seleccionado en píxeles. El valor predeterminado es 150.
- `height`: especifica el ancho del cuadro seleccionado en píxeles. El valor predeterminado es 400.
- `caseInsensitive`: utilícelo para realizar comparaciones sin que se distinga entre mayúsculas y minúsculas.

Componente Select

Muestra un objeto de selección única. Los valores del cuadro de lista se deben proporcionar mediante la propiedad `allowedValues`.

Las propiedades para este componente de visualización son:

- `allowedValues`: especifica la lista de valores que se pueden seleccionar para su visualización en el cuadro de lista.
- `allowedOthers`: cuando se define, especifica que los valores iniciales que no se encuentran en la lista `allowedValues` deben tolerarse y añadirse a la lista.
- `autoSelect`: cuando se define en el valor `true`, esta propiedad hace que el primer valor de la lista `allowedValues` se seleccione automáticamente si el valor inicial del campo es nulo.
- `caseInsensitive`: utilícelo para realizar comparaciones sin que se distinga entre mayúsculas y minúsculas.
- `multiple`: cuando se define en el valor `true`, permite seleccionar más de un valor.

- `nullLabel`: especifica el texto que aparece en la parte superior del cuadro de lista cuando no se selecciona ningún valor.
- `optionGroupMap`: permite que el selector represente opciones en grupos utilizando la etiqueta `<optgroup>`. Asigne formato al mapa de forma que las teclas de los mapas sean las etiquetas de grupo, y los elementos sean listas de elementos que puedan seleccionarse. (Los valores deben ser miembros de `allowedValues` para representarlos.)
- `size` (opcional): especifica el número máximo de filas que se muestran. Si el número de filas supera este tamaño, se añadirá una barra de desplazamiento.
- `sorted`: cuando se define en el valor `true`, los valores de la lista se ordenan.
- `valueMap`: asigna valores originales a valores mostrados.

El componente admite las propiedades `command` y `onChange`.

- En la información sobre el componente `DatePicker` se deben describir las siguientes propiedades nuevas. (ID-14802)

  El componente HTML `DatePicker` permite ahora seleccionar fechas discretas. Puede especificar un conjunto de rango de fechas que permita seleccionar determinadas fechas en el calendario.

  `DatePicker` implementa las dos nuevas propiedades siguientes:

  `SelectAfter`: limita las fechas que se pueden seleccionar, mostradas en el calendario, a fechas correspondientes a la fecha introducida o posteriores. Este valor de propiedad puede ser una cadena de fecha o un objeto de fecha Java.

```
<Property name='SelectAfter' value='**/**/****'/>
```

  `SelectBefore`: limita las fechas que se pueden seleccionar, mostradas en el calendario, a fechas correspondientes a la fecha introducida o anteriores. Este valor de propiedad puede ser una cadena de fecha o un objeto de fecha Java.

```
<Property name='SelectBefore' value='**/**/****'/>
```

  Cuando utilice un formulario que implemente la etiqueta `<Display class='DatePicker'>`, añada estas variables al formulario para configurar el rango de fechas. Si no define estas propiedades, el calendario no se limitará a las fechas que pueden seleccionarse.

Identity Manager Technical Deployment Overview

El análisis de los flujos de trabajo, los formularios y las páginas JSP relacionados pertenece a la descripción de la arquitectura incluida en *Identity Manager Technical Deployment Overview* (ID-7332).

Ejecución del proceso

Cuando un usuario introduce datos en un campo de una página y hace clic en Save, las vistas, los flujos de trabajo y los formularios interactúan a fin de permitir que se ejecuten los procedimientos necesarios para procesar los datos.

Cada página de Identity Manager tiene una vista, un flujo de trabajo y un formulario asociado que realiza el proceso necesario. En las dos tablas siguientes se enumeran estos flujos de trabajo, vistas y formularios.

Procesos de la interfaz de usuario de Identity Manager

En las tablas siguientes se indican los formularios, las vistas y los flujos de trabajo que están involucrados en los procesos iniciados desde las siguientes páginas de la interfaz de usuario de Identity Manager:

Interfaz de usuario Página	Formulario	Vista	autenticación
Menú principal	• endUserMenu • predeterminado Menú de usuario final	User La vista es de sólo lectura. No se pueden realizar modificaciones en esta página.	ninguno
Cambiar contraseña	• endUserChangePassword • predeterminado Formulario de cambio de contraseña	Contraseña	• changeUserPassword • predeterminado Cambiar contraseña de usuario
Change Other Account Attributes	• endUserForm • predeterminado Formulario de usuario final	User	Actualizar usuario
Check Process Status	• endUserTaskList • predeterminado Lista de tareas de usuario final	Lista La vista incluye información sobre los objetos TaskInstance iniciados por el usuario.	ninguno

Interfaz de usuario Página	Formulario	Vista	autenticación
Estado del proceso La clase TaskViewResults genera la página.	ninguno	ninguno	ninguno
Procesos disponibles	• endUserLaunchList • predeterminado Lista de inicio de usuario final	Lista La vista incluye información sobre los objetos TaskDefinition a los que puede acceder el usuario.	ninguno
Iniciar proceso Inicia una TaskDefinition seleccionada.	Definido por TaskDefinition	Process	ninguno
Cambiar las respuestas a las preguntas de autenticación	• changeAnswers • predeterminado Formulario de cambio de respuestas de usuario	ChangeUserAnswers	ninguno
Self Discovery Sólo puede vincularse con cuentas de recursos existentes.	• selfDiscovery • predeterminado Self Discovery	User	Actualizar usuario
Inbox	• endUserWorkItemList • predeterminado Lista de elementos de trabajo de usuario final	Lista La vista contiene información acerca de elementos de trabajo que pertenecen directamente al usuario actual.	ninguno
Inbox Item Edit	Especificado por WorkItem o autogenerado	WorkItem	ninguno

Procesos de la interfaz del administrador

En las tablas siguientes se indican los formularios, las vistas y las páginas JSP que están involucrados en los procesos iniciados desde las siguientes páginas de la interfaz del administrador de Identity Manager:

Página de interfaz del administrador	Formulario	Vista	autenticación
Crear y editar organización	Asignación de configuración al sistema Dependiendo del contexto, puede tratarse de uno de los distintos formularios, incluidos los siguientes: • Formulario de organización • Formulario de cambio de nombre de la organización • Formulario de enlace de directorio • Formulario de organización virtual • Formulario de actualización de organización virtual	Org	ninguno
Crear usuario	• userForm • predeterminado Formulario de usuario con fichas	User	• createUser • predeterminado Crear usuario
Actualizar usuario	• userForm • predeterminado Formulario de usuario con fichas	User	• updateUser • predeterminado Actualizar usuario
Disable User's Resource Accounts	• disableUser • predeterminado Inhabilitar usuario	Disable	• disableUser • predeterminado Inhabilitar usuario

Página de interfaz del administrador	Formulario	Vista	autenticación
Cambiar nombre de usuario	• renameUser • predeterminado Formulario de cambio de nombre de usuario	RenameUser	• renameUser • predeterminado Cambiar nombre de usuario
Update User's Resource Accounts	• reprovisionUser • predeterminado Formulario de reaprovisionamiento	Reprovision	• updateUser • predeterminado Actualizar usuario
Unlock User's Resource Accounts	• unlockUser • predeterminado Desbloquear usuario	Desbloquear	• unlockUser • predeterminado Desbloquear usuario
Delete User's Resource Accounts	• deprovisionUser • predeterminado Formulario de desprovisión	Deprovision	• deleteUser • predeterminado Eliminar usuario
Cambiar contraseña de usuario Mismo flujo de trabajo que la GUI de usuario final, pero distinto formulario	• changePassword • predeterminado Formulario de cambio de contraseña de usuario	ChangeUserPassword	• changeUserPassword • predeterminado Cambiar contraseña de usuario
Reinicializar contraseña de usuario	• resetPassword • predeterminado Formulario de reinicialización de contraseña de usuario	ResetUserPassword	• changeUserPassword • predeterminado Cambiar contraseña de usuario
Cambiar mi contraseña Vista, formulario y flujo de trabajo igual que End-User Change Password, pero JDP distinta	• endUserChangePassword • predeterminado Formulario de cambio de contraseña	Contraseña	• changeUserPassword • predeterminado Cambiar contraseña de usuario

Página de interfaz del administrador	Formulario	Vista	autenticación
Change My Answers Vista, formulario y flujo de trabajo igual que End-User Change Answers, pero JDP distinta	• changeAnswers • predeterminado Formulario de cambio de respuestas de usuario	ChangeUser Answers	ninguno
Aprobaciones	• workItemList • predeterminado Lista de elementos de trabajo • el formulario predeterminado incluye confirmación de elementos de trabajo	WorkItemList	ninguno
Edit WorkItem La protección de la vista WorkItem hace que se reanude el flujo de trabajo que la ha creado, pero no se genera ningún flujo de trabajo sólo para procesar la protección del elemento de trabajo.	Especificado por WorkItem o autogenerado	WorkItem	ninguno
Iniciar tarea Inicia una TaskDefinition seleccionada.	Definido por TaskDefinition	Process	ninguno
Create and Update Scheduled Tasks	Ninguna asignación de configuración; formulario Task Schedule predeterminado fusionado con el formulario TaskDefinition Este formulario se genera combinando el formulario TaskDefinition con el formulario Task Schedule como un programa de ajuste.	TaskSchedul e	ninguno

Página de interfaz del administrador	Formulario	Vista	autenticación
Crear rol y Editar rol	Ninguna asignación de configuración al sistema El formulario Role predeterminado y el formulario Role Rename dependen del contexto.	Rol	• manageRole • predeterminado Administrar rol
Edit Resource	Ninguna asignación de configuración al sistema. Dependiendo del contexto, incluye formularios: • Formulario de cambio de contraseña de cuenta de recursos • Formulario de reinicialización de contraseña de cuenta de recursos • Formulario de edición de directiva de recursos • Formulario de cambio de nombre de recurso • Asistente de recursos <tipo de recurso> • Asistente de recursos. Admite formularios de asistente específico, predeterminado para el asistente de recursos.	Resource	• manageResource • predeterminado Administrar recurso
Editar capacidad	changeCapabilities, predeterminado Formulario de cambio de capacidades de usuario	ChangeUser Capabilities	ninguno

Páginas de Java Server (JSP) y su función en Identity Manager

En las tablas siguientes se describen las páginas JSP que se suministran con el sistema, así como las páginas de interfaz de usuario y administrador asociadas a ellas.

JSP para interfaz de usuario de Identity Manager

Página	JPS asociada
Menú principal	user/main.jsp
Cambiar contraseña	user/changePassword.jsp
Change Other Account Attributes	user/changeAll.jsp
Check Process Status	user/processStatusList.jsp
Estado del proceso	user/processStatus.jsp
Procesos disponibles	user/processList.jsp
Iniciar proceso	user/processLaunch.jsp
Cambiar las respuestas a las preguntas de autenticación	user/changeAnswers.jsp
Self Discovery	user/selfDiscover.jsp
Inbox	user/workItemList.jsp
Inbox Item Edit	user/workItemEdit.jsp

JSP para interfaz de administración

Página	JPS asociada
Crear y editar organización	security/orgedit.jsp
Crear usuario	account/modify.jsp
Actualizar usuario	account/modify.jsp
Disable User’s Resource Accounts	account/resourceDisable.jsp
Cambiar nombre de usuario	account/renameUser.jsp

Página	JPS asociada
Update User's Resource Accounts	account/resourceReprovision.jsp
Unlock User's Resource Accounts	admin/resourceUnlock.jsp
Delete User's Resource Accounts	account/resourceDeprovision.jsp
Cambiar contraseña de usuario	admin/changeUserPassword.jsp
Reinicializar contraseña de usuario	admin/resetUserPassword.jsp
Cambiar mi contraseña	admin/changeself.jsp
Change My Answers	admin/changeAnswers.jsp
Aprobaciones	approval/approval.jsp
Edit WorkItem	approval/itemEdit.jsp
Iniciar tarea	task/taskLaunch.jsp
Create and Update Scheduled Tasks	task/editSchedule.jsp
Crear rol y Editar rol	roles/applicationmodify.jsp
Edit Resource	resources/modify.jsp
Editar capacidad	account/modifyCapabilities.jsp

Apéndice A, Edición de los objetos de configuración

En la página A-4, la lista de QueryableAttrNames predeterminados debe incluir también el `idmManager`.

Referencia de recursos de Identity Manager 6.0

- La lista de atributos de cuenta admitidos en Resources Reference > Active Directory > Account Attributes > Account Attribute Support es más corriente en la versión PDF del documento que la versión HTML. Consulte la versión PDF. (ID-12630)
- El nodo de nivel superior de Identity Manager 6.0 Resources Reference 2005Q4M3 en la siguiente URL no contiene ningún vínculo a la sección Domino: (ID-12636)

`http://docs.sun.com/app/docs/doc/819-4520`

Localice la sección Domino abriendo Contents en este nodo o en la siguiente URL:

`http://docs.sun.com/source/819-4520/Domino_Exchange.html#wp999317`

Adaptador de Access Manager

En el paso 5 del procedimiento “General Configuration” se debe indicar lo siguiente:

5. Añada las siguientes líneas al archivo `java.security` si aún no existen:

   ```
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.net.ssl.internal.ssl.Provider
   ```

   El número que sigue a security.provider en cada línea especifica el orden en el que Java consulta las clases de proveedor de seguridad y debe ser exclusivo. Los números de secuencia pueden variar según el entorno. Si ya tiene varios proveedores de seguridad en el archivo java.security, introduzca los nuevos proveedores de seguridad en el orden indicado anteriormente y renumere los proveedores de seguridad existentes. No elimine los proveedores de seguridad existentes ni los duplique. (ID-12044)

Adaptador de Active Directory

Active Directory admite ahora los atributos binarios `thumbnailPhoto` (Windows 2000 Server y superior) y `jpegPhoto` (Windows 2003).

Adaptador de SmartRoles de BridgeStream

Identity Manager proporciona ahora un adaptador de recurso de SmartRoles de BridgeStream que aprovisiona a los usuarios en SmartRoles. Este adaptador sitúa a los usuarios en las organizaciones adecuadas dentro de SmartRoles para que éste pueda determinar los roles comerciales que dichos usuarios deben tener.

Al recuperar un usuario desde SmartRoles, el adaptador recupera los roles comerciales del usuario. Estos roles comerciales se pueden utilizar en Identity Manager para determinar los roles, recursos, atributos y acceso de Identity Manager que se le deben asignar al usuario.

Además, SmartRoles puede ser una fuente de cambios de usuario utilizando Active Sync. Puede cargar usuarios de SmartRoles en Identity Manager y reconciliarlos.

Para obtener información detallada sobre este adaptador, consulte *Sun Java™ System Identity Manager Resources Reference Addendum*. (ID-12714)

Adaptador de ClearTrust

- El adaptador de recurso de ClearTrust admite ahora la versión 5.5.2 de ClearTrust.
- En los pasos 2 y 3 del procedimiento de las notas de instalación de Identity Manager se debe indicar lo siguiente (ID-12906):

1. Copie el archivo `ct_admin_api.jar` del CD de instalación de Clear Trust al directorio `WEB-INF\lib`.
2. Si utiliza SSL, copie al directorio `WEB-INF\lib` los archivos que se indican a continuación.

Nota Si está aprovisionando para un recurso RSA Clear Trust 5.5.2, no se requerirán bibliotecas adicionales para la comunicación con SSL.

- `asn1.jar`
- `certj.jar`
- `jce1_2-do.jar`
- `jcert.jar`
- `jnet.jar`
- `jsafe.jar`
- `jsaveJCE.jar`
- `jsse.jar`
- `rsajsse.jar`
- `sslj.jar`

Adaptador de tabla de base de datos

Este adaptador admite tipos de datos binarios, incluyendo BLOB, en Oracle. Los correspondientes atributos se deben marcar como binarios en el mapa de esquema. Entre los atributos binarios de ejemplo se incluyen archivos de gráficos, archivos de audio y certificados.

Adaptador de Flat File Active Sync

- El usuario administrativo debe disponer de acceso de lectura y escritura al directorio que contiene el archivo Flat File. Este usuario debe contar también con acceso de eliminación si el parámetro de Active Sync **Procesar diferencias únicamente** está habilitado.

  Además, la cuenta de administrador debe contar con permisos de lectura, escritura y eliminación en el directorio especificado en el campo **Ruta de fichero de registro** de Active Sync. (ID-12477)
- Si el formato del archivo Flat File es LDIF, se podrán especificar atributos binarios, tales como archivos de gráficos, archivos de audio y certificados. No se admiten atributos binarios para archivos CSV y delimitados por canal de comunicación.

Adaptador de HP OpenVMS

Identity Manager proporciona ahora un adaptador de recurso de HP OpenVMS que admite la versión 7.0 de VMS y posteriores. Para obtener información detallada sobre este adaptador, consulte *Sun Java™ System Identity Manager Resources Reference Addendum*. (ID-8556)

Adaptador de JMS Listener

El adaptador de JMS Listener admite ahora el procesamiento síncrono de mensajes en lugar del procesamiento asíncrono. Como resultado, en el segundo párrafo de la sección de conexiones de las notas de utilización se debe indicar lo siguiente:

El adaptador de JMS Listener funciona en modo síncrono. Establece un consumidor síncrono de mensajes en la cola o en el destino de temas especificado mediante el campo **JNDI name of Destination**. Durante cada intervalo de interrogación, el adaptador recibe y procesa todos los mensajes disponibles. Opcionalmente, los mensajes se pueden cualificar de forma adicional definiendo una cadena válida de selector de mensajes JMS para el campo **Selector de mensaje**.

La sección Message Mapping debe contener lo siguiente:

Cuando el adaptador procesa un mensaje cualificado, el mensaje JMS recibido se convierte primero a un mapa de valores nombrados utilizando el mecanismo especificado mediante el campo **Asignación de mensaje**. Refiérase a este mapa resultante como mapa de valores de *mensaje*.

El mapa de valores de mensaje se traduce a continuación al mapa de Active Sync utilizando el mapa de esquema de atributos de cuenta. Si el adaptador tiene atributos de cuenta especificados, realizará una búsqueda en el mapa de valores de mensaje

para encontrar nombres clave que aparezcan también como atributo de usuario de recursos en el mapa de esquema. Si existen, el valor se copiará al mapa de Active Sync, pero el nombre de entrada de dicho mapa se traducirá al nombre especificado en la columna de atributos de usuarios del sistema Identity del mapa de esquema.

Si el mapa de valores de mensaje contiene una entrada que no se pueda traducir utilizando el mapa de esquema de atributos de cuenta, la entrada del mapa de valores de mensaje se copiará sin modificarse al mapa de Active Sync.

Adaptador de LDAP

Admisión de atributos de cuentas binarias

Se admiten ahora los siguientes atributos de cuentas binarias de la clase de objeto inetOrgPerson:

Atributo de usuario de recursos	Sintaxis de LDAP	Descripción
audio	Audio	Archivo de audio.
jpegPhoto	JPEG	Imagen en formato JPEG.
userCertificate	certificado	Certificado, en formato binario.

Es posible que se admitan otras cuentas binarias, pero no se han comprobado.

Inhabilitación y habilitación de cuentas

El adaptador de LDAP proporciona varias formas para inhabilitar cuentas en un recurso de LDAP. Utilice una de las siguientes técnicas para inhabilitar cuentas.

Cambie la contraseña a un valor desconocido

Para inhabilitar cuentas cambiando la contraseña a cuentas con valor desconocido, deje en blanco los campos **Método de activación de LDAP** y **Parámetro de activación de LDAP**. Este es el método predeterminado para inhabilitar cuentas. La cuenta se puede habilitar de nuevo asignando una nueva contraseña.

Asigne el rol `nsmanageddisabledrole`

Para utilizar el rol `nsmanageddisabledrole` de LDAP a fin de inhabilitar y habilitar cuentas, configure el recurso de LDAP como se indica a continuación:

1. En la página Parámetros de recurso, defina el campo **Método de activación de LDAP** como `nsmanageddisabledrole`.
2. Defina el campo **Parámetro de activación de LDAP** como *`AtributoIDM`*`=CN=nsmanageddisabledrole,`*`Contextobase`*. (El *`AtributoIDM`* se especificará en el esquema en el siguiente paso.)
3. En la página Atributos de cuenta, añada el *AtributoIDM* como atributo de usuario de Identity System. Defina el atributo de usuario de recurso como `nsroledn`. El atributo debe ser de tipo cadena.
4. Cree un grupo llamado nsAccountInactivationTmp en el recurso de LDAP y asigne `CN=nsdisabledrole,`*`Contextobase`* como miembro.

Las cuentas de LDAP ahora se pueden inhabilitar. Para realizar la verificación utilizando la consola de LDAP, compruebe el valor del atributo `nsaccountlock`. El valor `true` indica que la cuenta está bloqueada.

Si la cuenta se vuelve a habilitar posteriormente, perderá el rol.

Defina el atributo `nsAccountLock`

Para utilizar el atributo `nsAccountLock` a fin de inhabilitar y habilitar cuentas, configure los recursos de LDAP como se indica a continuación:

1. En la página Parámetros de recurso, defina el campo **Método de activación de LDAP** como `nsaccountlock`.
2. Defina el campo **Parámetro de activación de LDAP** como *`AtributoIDM`*`=true`. (El *`AtributoIDM`* se especificará en el esquema en el siguiente paso.) Por ejemplo, `accountLockAttr=true`.
3. En la página Atributos de cuenta, añada el valor especificado en el campo **Parámetro de activación de LDAP** como atributo de usuario de Identity System. Defina el atributo de usuario de recurso como `nsaccountlock`. El atributo debe ser de tipo cadena.
4. Defina el atributo de LDAP `nsAccountLock` del recurso como `true`.

   Identity Manager define `nsaccountlock` como true al inhabilitar una cuenta. Asume también que los usuarios de LDAP preexistentes que tienen `nsaccountlock` definido como true están inhabilitados. Si `nsaccountlock` tiene algún valor que no sea true (incluido nulo), el sistema concluirá que el usuario está habilitado.

Inhabilite cuentas sin los atributos `nsmanageddisabledrole` **y** `nsAccountLock`

Si los atributos `nsmanageddisabledrole` y `nsAccountLock` no se encuentran disponibles en el servidor de directorios, pero el servidor cuenta con un método similar para inhabilitar cuentas, introduzca uno de los siguientes nombres de clase en el campo **Método de activación de LDAP**. El valor que se introduce en el campo **Parámetro de activación de LDAP** varía en función de la clase.

Nombre de clase	Cuándo utilizar:
com.waveset.adapter.util. ActivationByAttributeEnableFalse	El servidor de directorios habilita una cuenta definiendo un atributo en el valor “false”, e inhabilita una cuenta definiendo el atributo en el valor “true”. Añada el atributo al mapa de esquema. A continuación, introduzca el nombre de Identity Manager para el atributo (definido en el lado izquierdo del mapa de esquema) en el campo **Parámetro de activación de LDAP**.
com.waveset.adapter.util. ActivationByAttributeEnableTrue	El servidor de directorios habilita una cuenta definiendo un atributo en el valor “true”, e inhabilita una cuenta definiendo el atributo en el valor “false”. Añada el atributo al mapa de esquema. A continuación, introduzca el nombre de Identity Manager para el atributo (definido en el lado izquierdo del mapa de esquema) en el campo **Parámetro de activación de LDAP**.
com.waveset.adapter.util. ActivationByAttributePullDisablePushEnable	Identity Manager debe inhabilitar cuentas extrayendo un par de atributo/valor de LDAP y debe habilitar cuentas introduciendo un par de atributo/valor en LDAP. Añada el atributo al mapa de esquema. A continuación, introduzca el par de atributo/valor en el campo **Parámetro de activación de LDAP**. Utilice el nombre de Identity Manager para el atributo como se ha definido en el lado izquierdo del mapa de esquema.
com.waveset.adapter.util. ActivationByAttributePushDisablePullEnable	Identity Manager debe inhabilitar cuentas introduciendo un par de atributo/valor en LDAP y debe habilitar cuentas extrayendo un par de atributo/valor de LDAP. Añada el atributo al mapa de esquema. A continuación, introduzca el par de atributo/valor en el campo **Parámetro de activación de LDAP**. Utilice el nombre de Identity Manager para el atributo como se ha definido en el lado izquierdo del mapa de esquema.
com.waveset.adapter.util. ActivationNsManagedDisabledRole	El directorio utiliza un rol específico para determinar el estado de la cuenta. Si se asigna este rol a una cuenta, ésta se inhabilitará. Añada el nombre de rol al mapa de esquema. A continuación, introduzca un valor en el campo **Parámetro de activación de LDAP** utilizando el siguiente formato: *AtributoIDM*=CN=*Nombrerol*,*Contextobase* El *AtributoIDM* es el nombre de Identity Manager para el rol como se ha definido en el lado izquierdo del mapa de esquema.

Adaptadores de mainframe (ACF2, Natural, RACF, Top Secret)

Reflection de Attachmate correspondiente a la biblioteca de clases de emulador web (ECL de Reflection) se puede utilizar para conectarse a un recurso de mainframe. Esta biblioteca es compatible con la API de IBM Host on Demand. Siga todas las instrucciones de instalación proporcionadas con el producto. A continuación, realice los procedimientos descritos en “Notas de instalación” y “Configuración de SSL”.

Notas de instalación

Realice los siguientes pasos para configurar conexiones utilizando la ECL de Reflection de Attachmate:

1. Añada el recurso a la lista de recursos de Identity Manager como se describe en la *Identity Manager Resources Reference*.
2. Copie los archivos JAR correspondientes al directorio `WEB-INF/lib` de la instalación de Identity Manager.
   - `RWebSDK.jar`
   - `wrqtls12.jar`
   - `profile.jar`
3. Añada las siguientes definiciones al archivo `Waveset.properties` para definir el servicio que administra la sesión del terminal:

   `serverSettings.`*`IDservidor`*`.mainframeSessionType=`*`Valor`*
   `serverSettings.default.mainframeSessionType=`*`Valor`*

   El *Valor* se puede definir como se indica a continuación:
   - 1 — IBM Host On--Demand (HOD)
   - 3 — Attachmate WRQ

   Si estas propiedades no se definen explícitamente, Identity Manager intentará utilizar WRQ primero y, a continuación, HOD.
4. Si las bibliotecas de Attachmate se instalan en WebSphere Application Server, agregue la propiedad `com.wrq.profile.dir=`*`LibraryDirectory`* al archivo `WebSphere/AppServer/configuration/config.ini`.

   Ello permite que el código de Attachmate encuentre el archivo de licencia.
5. Reinicie el servidor de aplicación para que surtan efecto las modificiones realizadas en el archivo `Waveset.properties`.

Realice los pasos descritos en *Configuración de SSL*.

Configuración de SSL

Reflection de Attachmate correspondiente a la biblioteca de clases de emulador web (ECL de Reflection) es compatible con la API de IBM Host on Demand. Siga todas las instrucciones de instalación proporcionadas con el producto. A continuación, realice los siguientes pasos en Identity Manager.

1. Si aún no existe un atributo de recurso llamado Session Properties para el recurso, utilice las páginas de depuración o de IDE de Identity Manager para añadir el atributo al objeto de recurso. Añada la siguiente definición en la sección `<ResourceAttributes>`:

   ```
   <ResourceAttribute name='Session Properties' displayName='Session
   Properties' description='Session Properties' multi='true'>
   </ResourceAttribute>
   ```

2. Vaya a la página Parámetros de recurso correspondiente al recurso y añada los siguientes valores al atributo de recurso Session Properties:

   ```
   encryptStream
   true
   hostURL
   tn3270://nombrehost:puertoSSL
   keystoreLocation
   Path_To_Trusted_ps.pfx_file
   ```

Adaptadores de Oracle/Oracle ERP

El capítulo de Oracle/Oracle ERP de *Identity Manager Resources Reference* se ha dividido en dos capítulos independientes en esta versión. Consulte *Sun Java™ System Identity Manager Resources Reference Addendum* para ver estos dos capítulos nuevos. (ID-12758)

Adaptador de Oracle

- La admisión de Oracle 8i se eliminó erróneamente de la tabla de adaptadores y de la sección del adaptador de Oracle del capítulo 1 de Identity Manager Resources Reference. Identity Manager admite Oracle 8*i* como recurso. (ID-13078)
- El nombre de sección `updateableAttributes` se ha corregido a *`updatableAttributes`* en el paso 1 de la sección Cascade Deletes de este capítulo como se indica a continuación (ID-13075):
- El atributo de cuenta noCascade indica si se deben realizar eliminaciones en cascada al eliminar usuarios. De forma predeterminada, se realizan eliminaciones en cascada. Para inhabilitar las eliminaciones en cascada, añada una entrada a la sección `updatableAttributes` del objeto de configuración del sistema (System Configuration Object):

- La descripción del atributo de cuenta `oracleTempTSQuota` debe ser como se indica a continuación:

  La máxima cantidad de espacio de tablas temporal que puede asignar el usuario. Si el atributo aparece en el mapa de esquemas, la cuota siempre se establece en el espacio de tablas temporal. Si el atributo se suprime del mapa de esquemas, no se establece ninguna cuota en el espacio de tablas temporal. El atributo debe suprimirse para los adaptadores que se comunican con recursos de Oracle 10gR2. (ID-12843)

Adaptador de Oracle ERP

- El adaptador de Oracle ERP proporciona ahora un atributo de cuenta `employee_number` que representa un `employee_number` de la tabla `per_people_f` (ID-12796):
  - Al introducir un valor en el proceso de creación, el adaptador intenta buscar un registro de usuario en la tabla `per_people_f`, recupera el `person_id` *en* la API de creación e inserta el `person_id` en la columna `employee_id` de la tabla `fnd_user`.
  - Si no se introduce ningún número de empleado (`employee_number`) en el proceso de creación, el sistema no intentará crear vínculos.
  - Si introduce un número de empleado (`employee_number`) en el proceso de creación y ese número no se encuentra, el adaptador devolverá una excepción.
  - El adaptador intentará devolver el `employee_number` en un `getUser` si el `employee_number` está en el esquema del adaptador.
- El atributo de cuenta `npw_number` admite trabajadores eventuales. Funciona de la misma manera que `employee_number`. Los atributos `employee_number` y `npw_number` son autoexcluyentes. Si se introducen ambos al crear, tiene prioridad `employee_number`. (ID-16507)

Auditoría de responsabilidades

Se han añadido múltiples atributos al adaptador de Oracle ERP para que admita funciones de auditoría. (ID-11725)

Para auditar los subelementos (tales como formularios y funciones) de responsabilidades asignadas a usuarios, añada el objeto `auditorObject` al mapa de esquema. El objeto `auditorObject` es un atributo complejo que contiene un conjunto de objetos de responsabilidad. Los siguientes atributos se devuelven siempre en un objeto de responsabilidad:

- responsibility
- userMenuNames
- menuIds

- userFunctionNames
- functionIds
- formIds
- formNames
- userFormNames
- readOnlyFormIds
- readWriteOnlyFormIds
- readOnlyFormNames
- readOnlyUserFormNames
- readWriteOnlyFormNames
- readWriteOnlyUserFormNames
- functionNames
- readOnlyFunctionNames
- readWriteOnlyFunctionNames

Nota Los atributos readOnly y ReadWrite se identifican consultando la columna PARAMETERS de la tabla fnd_form_functions para encontrar uno de los siguientes valores:

- QUERY_ONLY= YES
- QUERY_ONLY= “YES”
- QUERY_ONLY = YES
- QUERY_ONLY = “YES”
- QUERY_ONLY= Y
- QUERY_ONLY= “Y”
- QUERY_ONLY = Y
- QUERY_ONLY = “Y”

Si el parámetro de recurso **Devolver conjunto de libros y/u organización** se define en el valor TRUE, se devolverán también los siguientes atributos:

- setOfBooksName
- setOfBooksId
- organizationalUnitName
- organizationalUnitId

Con la excepción de los atributos de responsabilidad, setOfBooksName, setOfBooksId, organizationalUnitId y organizationalUnitName, los nombres de atributo se corresponden con los nombres de atributos de cuenta que se pueden

añadir al mapa de esquema. Los atributos de cuenta contienen un conjunto agregado de valores que se asignan al usuario. Los atributos incluidos en los objetos `responsibility` son específicos de la responsabilidad.

La vista auditorResps[] proporciona acceso a los atributos de responsabilidad. El siguiente formulario snippet devuelve todas las responsabilidades activas (y sus atributos) asignadas a un usuario.

```
<defvar name='audObj'>
   <invoke name='get'>
      <ref>accounts[Oracle ERP 11i VIS].auditorObject</ref>
   </invoke>
</defvar>
<!-- this returns list of responsibility objects -->
<defvar name='respList'>
   <invoke name='get'>
      <ref>audObj</ref>
      <s>auditorResps[*]</s>
   </invoke>
</defvar>
```

Por ejemplo:

- `auditorResps[0].responsibility` devuelve el nombre del primer objeto de responsabilidad.
- `auditorResps[0].formNames` devuelve los nombres de formulario del primer objeto de responsabilidad.

Compatibilidad con Oracle EBS 12

El adaptador de Oracle ERP es compatible con Oracle E-Business Suite (EBS) versión 12. Ya no es preciso editar ni inhabilitar secciones del formulario OracleERPUserForm según la versión de ERP instalada, como se explica en *Identity Manager Resources Reference*.

El atributo FormRef ahora admite las propiedades siguientes:

- RESOURCE_NAME — Especifica el nombre del recurso de ERP.
- VERSION – Especifica la versión del recurso de ERP. Se admiten los valores 11.5.9, 11.5.10, 12.
- RESP_DESCR_COL_EXISTS — Determina si la tabla fnd_user_resp_groups_direct incluye la columna de descripción. Esta propiedad es necesaria con las versiones 11.5.10 y 12. Admite los valores TRUE y FALSE.

Estas propiedades deben introducirse siempre que se referencie el formulario de usuario. Por ejemplo, es posible que el formulario de usuario Tabbed User Form necesite algo como lo siguiente para ser compatible con la versión 12.

```
<FormRef name='Oracle ERP User Form'>
   <Property name='RESOURCE_NAME' value='Oracle ERP R12'/>
   <Property name='VERSION' value='12'/>
   <Property name='RESP_DESCR_COL_EXISTS' value='TRUE'/>
</FormRef>
```

Adaptador de SAP

- En la sección Account Attributes, se ha corregido la tabla que describe los tipos de información iDoc predeterminados que admite el adaptador de SAP HR Active Sync. El subtipo admitido que se enumera para el tipo de información de comunicación 0105 se ha cambiado de EMAIL a *MAIL* como se indica a continuación (ID-12880):

  De forma predeterminada, se admiten los siguientes tipos de información:

Tipo de información	Nombre	Subtipos admitidos
0000	Actions	No aplicable
0001	Organizational Assignment	No aplicable
0002	Personal Data	No aplicable
0006	Addresses	01 (residencia permanente), 03 (casa)
0105	Communication	MAIL (dirección de correo electrónico), 0010 (dirección de Internet)

El adaptador SAPHRActiveSyncAdapter admite ahora mySAP ERP ECC 5.0 (SAP 5.0). Como resultado, se han realizado los siguientes cambios en las notas de configuración de recursos. (ID-12769):

Adaptador de recursos de SAP

Las siguientes notas de configuración de recursos se aplican al adaptador de recursos de SAP solamente.

Para que un usuario pueda cambiar su propia contraseña SAP, realice los siguientes pasos:

1. Defina el atributo de recurso **El usuario debe especificar la contraseña al cambiarla**.
2. Añada **`WS_USER_PASSWORD`** a ambos lados del mapa de esquema. No es necesario modificar el formulario de usuario ni demás formularios.

Adaptador de SAP HR Active Sync

Las siguientes notas de configuración de recursos se aplican al adaptador de SAP HR Active Sync solamente.

La tecnología Application Link Enabling (ALE) de SAP posibilita la comunicación entre SAP y sistemas externos como Identity Manager. El adaptador de SAP HR Active Sync utiliza una interfaz ALE de salida. En una interfaz ALE de salida, el sistema lógico base se convierte en el emisor de mensajes de salida y en el receptor de mensajes de entrada. Un usuario SAP se conectará probablemente al cliente/sistema lógico base al realizar cambios en la base de datos (por ejemplo, para contratar un empleado, actualizar datos de posición, dar de baja a un empleado, etc.). Se debe definir también un cliente/sistema lógico para el cliente de recepción. Este sistema lógico actuará como receptor de mensajes de salida. Con respecto al tipo de mensaje entre los dos sistemas, el adaptador de Active Sync utiliza un tipo de mensaje `HRMD_A`. El tipo de mensaje caracteriza los datos que se envían en los sistemas y se relaciona con la estructura de los datos, que se conoce también como tipo IDoc (por ejemplo, `HRMD_A05`).

Los siguientes pasos proporcionan las configuraciones necesarias en SAP para que el adaptador de Active Sync reciba datos obligatorios de SAP HR:

Nota Debe configurar los parámetros del sistema SAP para habilitar el procesamiento de Application Link Enabling (ALE) de IDocs `HRMD_A`. Esto permite realizar la distribución de datos entre dos sistemas de aplicación, proceso conocido también como *mensajería*.

Creación de un sistema lógico

En función de su entorno SAP actual, puede no ser necesario crear un sistema lógico. Es posible que sólo deba modificar un modelo de distribución existente añadiendo el tipo de mensaje `HRMD_A` a una vista de modelos anteriormente configurada. No obstante, es importante que siga las recomendaciones de SAP sobre sistemas lógicos y para configurar la red ALE. En las siguientes instrucciones se asume que está creando nuevos sistemas lógicos y una vista nueva de modelos.

1. Introduzca el código de transacción **SPRO** y, a continuación, muestre el proyecto SAP Reference IMGproject (o el proyecto aplicable a su organización).
2. En función de la versión SAP que utilice, realice uno de los siguientes procedimientos:
   - Para SAP 4.6, haga clic en **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
   - Para SAP 4.7, haga clic en **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
   - Para SAP 5.0, haga clic en **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Define Logical System**.
3. Haga clic en **Edit** > `New Entries`.
4. Introduzca un nombre y una descripción para el sistema lógico que desea crear (IDMGR).
5. Guarde la entrada.

Asignación de un cliente al sistema lógico

1. Introduzca el código de transacción SPRO y, a continuación, muestre el proyecto SAP Reference IMGproject (o el proyecto aplicable a su organización).
2. En función de la versión SAP que utilice, realice uno de los siguientes procedimientos:
   - Para SAP 4.6, haga clic en **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.
   - Para SAP 4.7, haga clic en **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.
   - Para SAP 5.0, haga clic en **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Assign Client to Logical System**.

3. Seleccione el cliente.
4. Haga clic en **GOTO > Details** para mostrar el cuadro de diálogo Client Details.
5. En el campo Logical System, introduzca el sistema lógico que desea asignar a este cliente.
6. En la sección Changes and Transports for Clients, haga clic en **Automatic Recording of Changes**.
7. Guarde la entrada.

Creación de un modelo de distribución

Para crear un modelo de distribución:

1. Verifique que está conectado al cliente/sistema de envío.
2. Introduzca el código de transacción `BD64`. Compruebe que está en el modo de cambio.
3. Haga clic en **Edit > Model View > Create**.
4. Introduzca los nombres cortos y técnicos para la vista, así como la fecha de inicio y finalización y, a continuación, haga clic en **Continuar**.
5. Seleccione la vista que ha creado y haga clic en **Add Message Type**.
6. Defina el nombre del sistema lógico/emisor.
7. Defina el nombre del receptor/servidor.
8. En la sección Protection Client Copier and Comparison Tool, haga clic en **Protection Level: No Restriction**.
9. Defina el tipo de mensaje que desea utilizar (HRMD_A) y haga clic en **Continuar**.
10. Haga clic en **Save**.

Registro del módulo de servidor RFC con la puerta de enlace de SAP

Durante la inicialización, el adaptador de Active Sync se registra con la puerta de enlace de SAP. Utiliza “IDMRFC” para su ID. Este valor debe coincidir con el valor definido en la aplicación SAP. Debe configurar la aplicación SAP de forma que el módulo de servidor RFC pueda crear un identificador para ella. Para registrar el módulo de servidor RFC como destino RFC:

1. En la aplicación SAP, acceda a la transacción SM59.
2. Expanda el directorio de conexiones TCP/IP.
3. Haga clic en **Create (F8)**.
4. En el campo de destino RFC, introduzca el nombre del sistema de destino RFC. (IDMRFC).
5. Defina el tipo de conexión como `T` (inicie un programa externo mediante TCP/IP).

6. Introduzca una descripción para el nuevo destino RFC y haga clic en **Guardar**.
7. Haga clic en el botón Registro para el tipo de activación.
8. Defina el ID de programa. Se recomienda que utilice el mismo valor que el destino RFC (IDMRFC); a continuación, haga clic en Enter.
9. Si el sistema SAP es Unicode, el puerto se deberá configurar para Unicode. Haga clic en la ficha **Special Options** y busque la sección Character Width In Target System. Hay una configuración para Unicode y no Unicode.
10. Mediante los botones de la parte superior (**Conexión de prueba** y **Unicode Test**), compruebe la conexión al recurso de Identity Manager. Debe haber iniciado el adaptador para realizar la prueba correctamente.

Creación de una definición de puerto

El puerto es el canal de comunicación al que se envían IDocs. El puerto describe el enlace técnico entre los sistemas de envío y recepción. Debe configurar un puerto RFC para esta solución. Para crear una definición de puerto:

1. Introduzca el código de transacción **`WE21`**.
2. Seleccione Transactional RFC y haga clic en el icono **Create**. Introduzca **`IDMRFC`** para el destino RFC.
3. Guarde los cambios.

Modificación de la definición de puerto

Al generar un perfil de partner, es posible que la definición de puerto se introduzca incorrectamente. Para que el sistema funcione correctamente, deberá modificar la definición de puerto.

1. Introduzca el código de transacción **`WE20`**.
2. Seleccione **Partner Type LS**.
3. Seleccione el perfil de partner de recepción.
4. Seleccione **Outbound Parameters** y haga clic en **Display**.
5. Seleccione el tipo de mensaje **`HRMD_A`**.
6. Haga clic en **Outbound Options** y, a continuación, modifique el puerto receptor para que se corresponda con el nombre de puerto RFC que ha creado (IDMGR).
7. En el modo de salida, seleccione **Transfer IDoc Immediately** para enviar IDocs inmediatamente después de crearlos.
8. En la sección IDoc Type, seleccione un tipo básico:
   - Para SAP 4.6, seleccione **HRMD_A05**
   - Para SAP 4.7 o 5.0, seleccione **HRMD_A06**
9. Haga clic en **Continuar**/**Guardar**.

Adaptador de Scripted JDBC

Identity Manager proporciona ahora un adaptador de recurso de Scripted JDBC que permite administrar cuentas de usuario en cualquier esquema de base de datos y en cualquier base de datos accesible mediante JDBC. Este adaptador admite también Active Sync para interrogar sobre cambios de cuenta en la base de datos. Para obtener información detallada sobre este adaptador, consulte Sun Java™ System *Identity Manager Resources Reference Addendum*. (ID-12506)

Adaptador de Shell Script

Identity Manager proporciona ahora un adaptador de recurso de Shell Script que permite administrar recursos controlados mediante secuencias de shell que se ejecutan en el sistema que incluye el recurso. Este adaptador es de uso general, por lo que es altamente configurable.

Adaptador de Siebel CRM

Ahora se pueden crear y actualizar objetos Siebel que requieren navegación por el componente comercial principal/secundario. Se trata de una función avanzada que normalmente no se implementa en Identity Manager.

La función de navegación avanzada permite especificar opcionalmente la siguiente información necesaria para crear y actualizar componentes comerciales secundarios:

- nombre de objeto comercial
- nombre de componente comercial principal
- atributo de búsqueda principal
- componente comercial destino
- atributo de búsqueda destino
- atributos en ámbito (los atributos del componente comercial que se deben definir/actualizar)
- co-acción opcional

Se puede utilizar una regla de navegación avanzada durante acciones de creación y actualización. No se puede utilizar para otros tipos de acciones.

Para implementar la función de navegación avanzada del adaptador de Siebel CRM, debe realizar las siguientes tareas:

- Añada un atributo al mapa de esquema en el que el atributo de usuario de recurso (lado derecho) se llame PARENT_COMP_ID.

- Utilice la página de depuración para añadir manualmente el siguiente atributo de recurso al XML del recurso

```
<ResourceAttribute name='AdvancedNavRule'
   displayName='Advanced Nav Rule'
   value='MY_SIEBEL_NAV_RULE'>
</ResourceAttribute>
```

  Sustituya *MY_SIEBEL_NAV_RULE* por un nombre de regla válido.

- Escriba la regla de navegación avanzada. Debe haber dos variables para la regla:

  `resource.action`: el valor debe ser `create` o `update`.

  `resource.objectType`: para el mantenimiento normal de la cuenta, este valor será `account`.

  La regla debe devolver un mapa con uno o varios de los siguientes pares de nombre/valor:

Atributo	Definición
`busObj`	Nombre del objeto comercial.
`parentBusComp`	Nombre del componente comercial principal para `busObj`. El contexto del objeto comercial se actualiza al desplazarse al primer registro cualificado (consulte `parentSearchAttr`) de este componente comercial
`parentSearchAttr`	Atributo que se debe utilizar como campo de búsqueda en `parentBusComp`. El valor de búsqueda debe existir como valor del atributo cuyo nombre de atributo de usuario de recurso es PARENT_COMP_ID.
`busComp`	Nombre del componente comercial final para crear o actualizar. Si se crea, se creará un registro de este componente comercial en el objeto comercial. Si se actualiza, el registro del componente comercial que se debe actualizar se selecciona desplazándose al primer registro cualificado (consulte `searchAttr`) de este componente comercial.
`searchAttr`	Atributo que se debe utilizar como campo de búsqueda en `busComp`. El valor de búsqueda es el ID de cuenta del usuario.
`attributes`	Lista de cadenas que especifica el conjunto de campos incluidos en `busComp` que se definirán o actualizarán. Esta lista sustituye a los atributos definidos en el mapa de esquema del recurso para la acción que se está realizando.
`coAction`	Si la acción solicitada (`resource.action`) es `create`, especifique un valor `coAction` de `update` para indicarle al adaptador que realice también una actualización inmediatamente después de la creación. Esto puede ser necesario si la creación no puede definir todos los campos necesarios, por lo que debe producirse también una actualización para completar lógicamente la creación. Este atributo se ignorará a menos que `resource.action` sea `create` y `coAction` se defina como `update`.

En `$WSHOME/sample/rules/SiebelNavigationRule.xml` se proporciona una regla de navegación de ejemplo.

Adaptador de Sun Java System Access Manager

- Este adaptador admite el modo antiguo sólo para Access Manager 7 y versiones posteriores. No se admite la función de dominios.

Instalación y configuración de Sun Java System Access Manager (versiones anteriores a Access Manager 7.0)

En los pasos 4 y 8 del procedimiento “Instalación y configuración de Sun Java System Access Manager” debe indicarse lo siguiente (ID-13087):

1. Cree un directorio para incluir los archivos que se copiarán desde el servidor de Sun Java System Access Manager. Este directorio se denominará *CfgDir* en este procedimiento. La ubicación de Sun Java System Access Manager se denominará *AccessMgrHome*.
2. Copie los siguientes archivos de *AccessMgrHome* a *CfgDir*. No copie la estructura del directorio.
   - `lib/*.*`
   - `locale/*.properties`
   - `config/serverconfig.xml`
   - `config/SSOConfig.properties` (Identity Server 2004Q2 y versiones posteriores)
   - `config/ums/ums.xml`
3. En UNIX, puede ser necesario cambiar los permisos de los archivos jar incluidos en *CfgDir* para permitir el acceso de lectura universal. Ejecute el siguiente comando para cambiar permisos:

   `chmod a+r CfgDir/*.jar`
4. Preceda la ruta de clase JAVA con lo siguiente:
   - **Windows**: *CfgDir*`;`*CfgDir*`/am_sdk.jar;`*CfgDir*`/am_services.jar;`*CfgDir*`/am_logging.jar`
   - **UNIX**: *CfgDir*`:`*CfgDir*`/am_sdk.jar:`*CfgDir*`/am_services.jar:`*CfgDir*`/am_logging.jar`
5. Si utiliza la versión 6.0, defina la propiedad de sistema Java para que señale a su directorio *CfgDir*. Utilice un comando similar a lo siguiente:

   `java -Dcom.iplanet.coreservices.configpath=CfgDir`

6. Si utiliza la versión 6.1 o una posterior, añada o edite las siguientes líneas en el archivo *CfgDir*/AMConfig.properties:

   ```
   com.iplanet.services.configpath=CfgDircom.iplanet.security.
   SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFact
   oryImpl
   com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.
   factory.JSSESocketFactory
   com.iplanet.security.encryptor=com.iplanet.services.util.
   JCEEncryption
   ```

   La primera línea define la ruta de configuración (configpath). Las tres últimas líneas cambian configuraciones de seguridad.

7. Copie los archivos *CfgDir*/am_*.jar a $WSHOME/WEB-INF/lib. Si utiliza la versión 6.0, copie también el archivo jss311.jar al directorio $WSHOME/WEB-INF/lib.
8. Si Identity Manager se ejecuta en Windows y utiliza Identity Server 6.0, copie *IdServer*\lib\jss*.dll a *CfgDir* y añada *CfgDir* a la ruta de su sistema.

Nota En un entorno en el que Identity Manager esté instalado en un sistema distinto de Sun Java System Access Manager, compruebe las siguientes condiciones de error. Si al intentar conectarse al recurso de Sun Java System Access Manager se devuelve un error java.lang.ExceptionInInitializerError, seguido de java.lang.NoClassDefFoundError, en intentos posteriores, compruebe si los datos de configuración son incorrectos o si faltan.

Asimismo, compruebe el archivo jar con respecto a la clase indicada por el error java.lang.NoClassDefFoundError. Preceda la ruta de clase del archivo jar que contiene la clase a la ruta de clase JAVA en el servidor de aplicaciones.

Instalación y configuración de Sun Java System Access Manager (versiones 7.0 y posteriores en modo antiguo)

Realice los siguientes pasos para instalar y configurar el adaptador de recursos para el modo antiguo.

1. Siga las instrucciones indicadas en *Sun Java™ System* Access Manager 7 2005Q4 Developer's Guide para compilar el SDK de cliente a partir de la instalación de Sun Access Manager.
2. Extraiga los archivos AMConfig.properties y amclientsdk.jar del archivo war que se genera.
3. Incluya una copia de AMConfig.properties en el directorio:

   InstallDir/WEB-INF/classes

4. Incluya una copia de amclientsdk.jar en el directorio:

   InstallDir/WEB-INF/lib

Adaptador de servicios de comunicaciones de sistemas Sun Java

- La secuencia de comandos de ejemplo que se puede ejecutar en el recurso Proxy tras crear un usuario se ha enumerado incorrectamente. En su lugar, se deberá utilizar la siguiente secuencia de comandos: (ID-12536)

```
SET PATH=c:\Sun\Server-Root\lib
SET SYSTEMROOT=c:\winnt
SET CONFIGROOT=C:/Sun/Server-Root/Config
mboxutil -c -P user/%WSUSER_accountId%.*
```

- Se admiten ahora los siguientes atributos de cuentas binarias de la clase de objeto inetOrgPerson:

Atributo de usuario de recursos	Sintaxis de LDAP	Descripción
audio	Audio	Archivo de audio.
jpegPhoto	JPEG	Imagen en formato JPEG.
userCertificate	certificado	Certificado, en formato binario.

  Es posible que se admitan otras cuentas binarias, pero no se han comprobado.

Adaptador de Top Secret

En *Identity Manager Resources Reference* se indica incorrectamente que el adaptador de Top Secret permite cambiar el nombre de las cuentas. El adaptador no permite cambiar el nombre de las cuentas de Top Secret.

Capítulo 3: Adición de acciones a recursos

En la sección “Windows NT Examples”, los nombres de `Field` se han definido incorrectamente en los tres ejemplos. Sustituya instancias de `accounts[NT].attributes.` por `resourceAccounts.currentResourceAccounts[NT].attributes.` Por ejemplo, en la sección “Example 3: Action that Follows the Deletion of a User”, el nombre de `Field` del paso 4 se debe definir de la siguiente forma:

```
<Field name=
'resourceAccounts.currentResourceAccounts[NT].attributes.delete after
action'>
```

Ajuste, solución de problemas y mensajes de error en Identity Manager

Información añadida

- Ahora puede utilizar la función de seguimiento estándar de com.waveset.task.Scheduler para realizar un seguimiento del programador de tareas si una tarea presenta problemas.

  Para obtener más información, consulte *Tracing the Identity Manager Server* en Ajuste, solución de problemas y mensajes de error en *Sun Java™ System Identity Manager*.

- Para depurar un problema que se produzca en un nivel inferior a un método de entrada específico, realice un seguimiento en el nivel de método. Identity Manager proporciona ahora la capacidad de realizar el seguimiento de un método solamente y de sus subllamadas directas e indirectas. (ID-14967)

  Para habilitar esta función, defina el nivel de seguimiento para un ámbito con el modificador `subcalls`, como se muestra a continuación:

```
trace 4,subcalls=2
com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
```

  De esta forma se realizará el seguimiento del método `reconcileAccount()` en el nivel 4 y de todas las subllamadas en el nivel 2.

  Para obtener más información, consulte *Defining a Trace Configuration* en Ajuste, solución de problemas y mensajes de error en *Sun Java™ System Identity Manager*.

Correcciones

Como necesita instalar JDK 1.4.2 en esta versión, las instrucciones para eliminar los archivos Cryptix jar (`cryptix-jceapi.jar` y `cryptix-jce-provider.jar`) del directorio `idm\WEB-INF\lib` que se proporcionan en el capítulo 1: *Performance Tuning, Optimizing the J2EE Environment*, ya no sirven (a menos que actualice una versión anterior de Identity Manager).

Identity Manager Deployment Tools

Correcciones

Capítulo 7: Utilización de servicios Web en Identity Manager

El ejemplo launchProcess proporcionado en la sección ExtendedRequest Examples se ha corregido como se indica a continuación (ID-13044):

launchProcess

El siguiente ejemplo muestra un formato habitual para la solicitud `launchProcess`. (Vista — Vista de proceso).

```
ExtendedRequest req = new ExtendedRequest();
req.setOperationIdentifier("launchProcess");
req.setAsynchronous(false);
req.setAttribute("process", "Custom Process Name");
req.setAttribute("taskName", "Custom Process Display Name");
SpmlResponse res = client.request(req);
```

Utilización de helpTool

En Identity Manager 6.0 se ha añadido una nueva función que permite realizar búsquedas en la ayuda en línea y los archivos de documentación, que se encuentran en formato HTML. El motor de búsqueda se basa en la tecnología de motor de búsqueda SunLabs “Nova”.

El motor Nova funciona en dos fases: *indexación* y *recuperación*. Durante la fase de indexación se analizan los documentos introducidos y se crea un índice que se utiliza durante la fase de recuperación. Durante la recuperación es posible extraer “fragmentos” incluidos en el contexto en el que se encontraron los términos de la consulta. El proceso de recuperación de fragmentos requiere que los archivos HTML originales estén presentes, motivo por el cual deben residir en una ubicación del sistema de archivos a la que pueda acceder el motor de búsqueda.

helpTool es un programa de Java que realiza dos funciones básicas:

- Copia los archivos de origen en formato HTML en una ubicación que conoce el motor de búsqueda.
- Crea el índice que se va a utilizar durante la fase de recuperación.

helpTool se ejecuta desde la línea de comandos como sigue:

```
$ java -jar helpTool.jar
usage: HelpTool
 -d    Destination directory
 -h    This help information
 -i    Directory or JAR containing input files, no wildcards
 -n    Directory for Nova index
 -o    Output file name
 -p    Indexing properties file
```

Reconstrucción/recreación del índice de la ayuda en línea

Los archivos HTML de la ayuda en línea se empaquetan en un archivo JAR. Para que el motor de búsqueda funcione, debe extraerlos a un directorio. Realice el siguiente procedimiento:

1. Descomprima helpTool en un directorio temporal. (Detalles TBD)

   En este ejemplo, los archivos se van a extraer en `/tmp/helpTool`.

2. En el intérprete de comandos de UNIX o en la ventana de comandos de Windows, cambie el directorio a la ubicación del contenedor Web en el que se ha implementado la aplicación Identity Manager.

   Por ejemplo, el siguiente podría ser un directorio de Sun Java System Application Server:

   `/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm`

3. Cambie el directorio de trabajo actual a `help/`.

Nota Es importante ejecutar helpTool desde este directorio. De lo contrario, el índice no se generará correctamente. Además, debería borrar los archivos de índice anteriores eliminando el contenido del subdirectorio `index/help/`.

4. Recopile la siguiente información para los argumentos de la línea de comandos:

• **Directorio de destino**:	`html/help/en_US` **Nota**: Utilice la cadena de configuración regional adecuada.
• **Archivos de entrada**:	`../WEB-INF/lib/idm.jar`
• **Directorio de índice Nova**:	`index/help`
• **Nombre de archivo de salida**:	`index_files_help.txt` **Nota**: El nombre del archivo no es importante, pero la herramienta se cerrará si ya existe.
• **Archivo de propiedades de indexación**:	`index/index.properties`

5. Ejecute el comando siguiente:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/help/en_US -i ../
WEB-INF/lib/idm.jar -n index/help -o help_files_help.txt -p
index/index.properties
Extracted 475 files.
[15/Dec/2005:13:11:38] PM Init index/help AWord 1085803878
[15/Dec/2005:13:11:38] PM Making meta file: index/help/MF: 0
[15/Dec/2005:13:11:38] PM Created active file: index/help/AL
[15/Dec/2005:13:11:40] MP Partition: 1, 475 documents, 5496 terms.
[15/Dec/2005:13:11:40] MP Finished dumping: 1 index/help 0.266
[15/Dec/2005:13:11:40] IS 475 documents, 6.56 MB, 2.11 s, 11166.66 MB/h
[15/Dec/2005:13:11:40] PM Waiting for housekeeper to finish
[15/Dec/2005:13:11:41] PM Shutdown index/help AWord 1085803878
```

Reconstrucción/recreación del índice de la documentación

Para reconstruir o volver a crear el índice de la documentación, realice el siguiente procedimiento:

1. Descomprima helpTool en un directorio temporal. (Detalles TBD)

   En este ejemplo, los archivos se van a extraer en `/tmp/helpTool`.

2. En el intérprete de comandos de UNIX o en la ventana de comandos de Windows, cambie el directorio a la ubicación del contenedor Web en el que se ha implementado la aplicación Identity Manager.

   Por ejemplo, el siguiente podría ser un directorio de Sun Java System Application Server:

   `/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm`

3. Cambie el directorio de trabajo actual a `help/`.

Nota helpTool se debe ejecutar desde este directorio. De lo contrario, el índice no se generará correctamente. Además, debería borrar los archivos de índice anteriores eliminando el contenido del subdirectorio `index/docs/`.

4. Recopile la siguiente información para los argumentos de la línea de comandos:

• **Directorio de destino**:	`html/docs`
• **Archivos de entrada**:	`../doc/HTML/en_US` **Nota**: La herramienta copiará el directorio en_US/ y los subdirectorios en el destino.
• **Directorio de índice Nova**:	`index/docs`
• **Nombre de archivo de salida**:	`index_files_docs.txt` **Nota**: El nombre del archivo no es importante, pero la herramienta se cerrará si ya existe.
• **Archivo de propiedades de indexación**:	`index/index.properties`

5. Ejecute el comando siguiente:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/docs -i
../doc/HTML/en_US -n index/docs -o help_files_docs.txt -p
index/index.properties
Copied 84 files.
Copied 105 files.
Copied 1 files.
Copied 15 files.
Copied 1 files.
Copied 58 files.
Copied 134 files.
Copied 156 files.
Copied 116 files.
Copied 136 files.
Copied 21 files.
Copied 37 files.
Copied 1 files.
Copied 13 files.
Copied 2 files.
Copied 19 files.
Copied 20 files.
Copied 52 files.
Copied 3 files.
Copied 14 files.
Copied 3 files.
Copied 3 files.
Copied 608 files.
[15/Dec/2005:13:24:25] PM Init index/docs AWord 1252155067
[15/Dec/2005:01:24:25] PM Making meta file: index/docs/MF: 0
[15/Dec/2005:01:24:25] PM Created active file: index/docs/AL
[15/Dec/2005:01:24:28] MP Partition: 1, 192 documents, 38488 terms.
[15/Dec/2005:01:24:29] MP Finished dumping: 1 index/docs 0.617
[15/Dec/2005:01:24:29] IS 192 documents, 14,70 MB, 3,81 s,
13900,78 MB/h
[15/Dec/2005:01:24:29] PM Waiting for housekeeper to finish
[15/Dec/2005:13:24:30] PM Shutdown index/docs AWord 1252155067
```

API desaprobadas

En este capítulo se enumeran todas las interfaces de programación de aplicaciones (API) de Identity Manager que se han desaprobado en Identity Manager 6.0 2005Q4M3 SP1 y las alternativas (si existen). El capítulo se divide en las secciones siguientes:

- Constructores invalidados
- Métodos y campos invalidados

Constructores invalidados

En la tabla siguiente se incluyen los constructores invalidados y los que se pueden utilizar en su lugar, si están disponibles.

Constructor invalidado	Alternativa
com.waveset.adapter.ActiveDirectoryActiveSyncAdapter	com.waveset.adapter.ADSIResourceAdapter
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.AttrParse	com.waveset.object.AttrParse
com.waveset.adapter.ConfirmedSync	
com.waveset.adapter.DblBufIterator	com.waveset.util.BufferedIterator com.waveset.util.BlockIterator com.waveset.adapter.AccountIteratorWrapper
com.waveset.adapter.DominoActiveSyncAdapter	com.waveset.adapter.DominoResourceAdapter
com.waveset.adapter.LDAPChangeLogActiveSyncAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.exception.ConfigurationError	com.waveset.util.ConfigurationError

Constructor invalidado	Alternativa
com.waveset.exception.IOException	com.waveset.util.IOException
com.waveset.exception.XmlParseException	com.waveset.util.XmlParseException
com.waveset.object.IAPI	com.waveset.adapter.iapi.IAPI
com.waveset.object.IAPIProcess	com.waveset.adapter.iapi.IAPIFactory
com.waveset.object.IAPIUser	com.waveset.adapter.iapi.IAPIUser
com.waveset.object.RemedyTemplate	
com.waveset.object.ReportCounter	
com.waveset.object.SourceManager	com.waveset.view.SourceAdapterManageView
com.waveset.security.authn.LoginInfo	com.waveset.object.LoginInfo
com.waveset.security.authn.SignedString	com.waveset.util.SignedString
com.waveset.security.authn.Subject	com.waveset.object.Subject
com.waveset.security.authz.Permission	com.waveset.object.Permission
com.waveset.security.authz.Right	com.waveset.object.Right
com.waveset.util.Debug	com.sun.idm.logging.Trace
com.waveset.util.HtmlUtil	com.waveset.ui.util.html.HtmlUtil
com.waveset.util.ITrace	com.sun.idm.logging.Trace

Métodos y campos desaprobados

En las tablas de esta sección se recogen todos los métodos y campos que se han invalidado en esta versión. Los métodos y los campos aparecen ordenados según el nombre de clase.

Los datos que aparecen en la columna **Alternativa** pueden contener los siguientes tipos de información:

- Si la columna está vacía, no existe un campo o método alternativo.
- Si no incluye un nombre de clase, el método o campo alternativo se define en la misma clase que el método o campo desaprobado.
- Si el método o campo alternativo se define en una clase diferente, la alternativa se indica con la sintaxis de Javadoc. Por ejemplo, el método `getBaseContextAttrName()` de la clase

com.waveset.adapter.ADSIResourceAdapter se ha desaprobado.
El método alternativo aparece como
`com.waveset.adapter.ResourceAdapter#ResourceAdapter()`

donde:

- `com.waveset.adapter` es el nombre del paquete.
- `ResourceAdapter` es el nombre de la clase.
- `ResourceAdapter()` es el método y la lista de argumentos.

com.waveset.adapter.AccessManagerResourceAdapter

Método invalidado	Alternativa
handlePDException(Exception)	handlePDException(PDException)

com.waveset.adapter.ACF2ResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.ActiveSync

Campo desaprobado	Alternativa
RA_UPDATE_IF_DELETE	

com.waveset.adapter.ActiveSyncUtil

Método invalidado	Alternativa
getLogFileFullPath()	

com.waveset.adapter.ADSIResourceAdapter

Método o campo desaprobado	Alternativa
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.AgentResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.AIXResourceAdapter.BlockAcctIter

Método invalidado	Alternativa
BlockAcctIter(AIXResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.AuthSSOResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.ClearTrustResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.DatabaseTableResourceAdapter

Campo desaprobado	Alternativa
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.DB2ResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.DominoResourceAdapter

Método o campo desaprobado	Alternativa
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.DominoResourceAdapterBase

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.ExampleTableResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.GenericScriptResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.GetAccessResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.HostConnectionPool

Método invalidado	Alternativa
getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool#getAffinityConnection(HostAccessLogin)
releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(HostAccess)

com.waveset.adapter.HostConnPool

Método invalidado	Alternativa
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	

com.waveset.adapter.iapi.IAPIFactory

Método invalidado	Alternativa
getIAPIProcess(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIProcess(Element)	
getIAPIUser(Element)	
getIAPIUser(Map,Map,String,Map)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIUser(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)

com.waveset.adapter.IDMResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.INISafeNexessResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.LDAPResourceAdapterBase

Método o campo desaprobado	Alternativa
addUserToGroup(LDAPObject,String,String)	addUserToGroup(String,String,String)
buildBaseUrl()	
buildBaseUrl(String)	
buildEvent(UpdateRow)	
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
getGroups(Name,String,Vector,Vector)	getGroups(String,String,Vector,Vector)
getLDAPAttributes(String,DirContext[],String)	getLDAPAttributes(String,DirContext,String,String[])
getLDAPAttributes(String,DirContext[])	getLDAPAttributes(String,DirContext,String,String[])
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE
removeNameFromAttribute(DirContext,Name,Attribute)	removeNameFromAttribute(DirContext,String,boolean,Attribute)
removeUserFromAllGroups(Name,String,WavesetResult)	removeUserFromAllGroups(String,boolean,String,WavesetResult)
removeUserFromGroup(DirContext,Name,String,String,Attributes)	removeUserFromGroup(DirContext,String,boolean,String,String,Attributes)
removeUserFromGroups(Name,Vector,String,WavesetResult)	removeUserFromGroups(String,boolean,Vector,String,WavesetResult)

com.waveset.adapter.MySQLResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.NaturalResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.NDSResourceAdapter

Método invalidado	Alternativa
buildEvent(UpdateRow)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.ONTDirectorySmartResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.OS400ResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter

Método o campo desaprobado	Alternativa
DEFAULT_AUDIT_STAMP_FORMAT	
DEFAULT_AUDIT_STAMP_START_DATE	
getAccountAttributes(String)	
getUpdateRows(UpdateRow)	getUpdateRows(UpdateRow)
RA_AUDIT_STAMP_FORMAT	

com.waveset.adapter.RACFResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.RASecureConnection

Método invalidado	Alternativa
ExchangeAuth(boolean)	ExchangeAuth(boolean,byte[])

com.waveset.adapter.RedHatLinuxResourceAdapter.BlockAcctIter

Método invalidado	Alternativa
BlockAcctIter(int,CaptureList)	BlockAcctIter(SVIDResourceAdapter,CaptureList)

com.waveset.adapter.RequestResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.ResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceAdapterBase

Método invalidado	Alternativa
getAccountAttributes(String)	
getAdapter(Resource,LighthouseContext)	getAdapterProxy(Resource,LighthouseContext)
getAdapter(Resource,ObjectCache,WSUser)	getAdapterProxy(Resource,ObjectCache)
getAdapter(Resource,ObjectCache)	getAdapterProxy(Resource,LighthouseContext)
getBaseContextAttrName()	getBaseContexts()
isExcludedAccount(String,Rule)	com.waveset.adapter.ResourceAdapterProxy #isExcludedAccount(String, Map,ResourceOperation,Rule)
isExcludedAccount(String)	com.waveset.adapter.ResourceAdapterProxy #isExcludedAccount(String, Map,ResourceOperation,Rule)

com.waveset.adapter.ResourceAdapterProxy

Método invalidado	Alternativa
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceManager

Método invalidado	Alternativa
getResourceTypes()	getResourcePrototypes() getResourcePrototypes(ObjectCache,boolean)
getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

com.waveset.adapter.SAPHRActiveSyncAdapter

Campo desaprobado	Alternativa
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.SAPResourceAdapter

Método invalidado	Alternativa
unexpirePassword(String,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)

com.waveset.adapter.ScriptedConnection

Subclase	Método invalidado	Alternativa
Secuencia de comandos	hasNextToken()	
Secuencia de comandos	nextToken()	
ScriptedConnection	disConnect()	com.waveset.adapter.ResourceConnection#disconnect()
ScriptedConnectionFactory	getScriptedConnection(String,HashMap)	com.waveset.adapter.ScriptedConnectionPool#getConnection(HashMap,String,long,boolean)
SSHConnection	disConnect()	disconnect()
TelnetConnection	disConnect()	disconnect()

com.waveset.adapter.ScriptedHostResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SkeletonResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SMEResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SQLServerResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SunAccessManagerResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter

Método o campo desaprobado	Alternativa
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(SVIDResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.SybaseResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.TestResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.TopSecretResourceAdapter

Método invalidado	Alternativa
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)

com.waveset.adapter.VerityResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.XMLResourceAdapter

Método invalidado	Alternativa
getAccountAttributes(String)	

com.waveset.msgcat.Catalog

Método invalidado	Alternativa
getMessage(String,Object[],Locale)	format (Locale,String,Object[])
getMessage(Locale,String,Object[])	format (Locale,String,Object[])

Método invalidado	Alternativa
getMessage(Locale,String)	format (Locale,String)
getMessage(String,Locale)	format (Locale,String)
getMessage(String,Object[])	format (Locale,String,Object[])

com.waveset.object.Account

Método invalidado	Alternativa
getUnowned()	hasOwner()
setUnowned(boolean)	setOwner(WSUser)

com.waveset.object.AccountAttributeType

Método invalidado	Alternativa
getAttrType()	getSyntax()
setAttrType(String)	setSyntax(String) setSyntax(Syntax)

com.waveset.object.Attribute

Método o campo desaprobado	Alternativa
BLOCK_SIZE	BLOCK_ROWS_GET BLOCK_ROWS_LIST
EVENTDATE	EVENT_DATETIME
EVENTTIME	EVENT_DATETIME
getDbColumnLength()	
getDbColumnName()	

Método o campo desaprobado	Alternativa
STARTUP_TYPE_AUTO	com.waveset.object.Resource#STARTUP_TYPE_AUTO
STARTUP_TYPE_AUTO_FAILOVER	com.waveset.object.Resource#STARTUP_TYPE_AUTO_FAILOVER
STARTUP_TYPE_DISABLED	com.waveset.object.Resource#STARTUP_TYPE_DISABLED
STARTUP_TYPE_MANUAL	com.waveset.object.Resource#STARTUP_TYPE_MANUAL
STARTUP_TYPES	com.waveset.object.Resource#STARTUP_TYPES
STARTUP_TYPES_DISPLAY_NAMES	com.waveset.object.Resource#STARTUP_TYPES_DISPLAY_NAMES

com.waveset.object.AttributeDefinition

Método invalidado	Alternativa
AttributeDefinition(String,String)	AttributeDefinition(String,Syntax)
setAttrType(String)	setSyntax(Syntax)

com.waveset.object.AuditEvent

Método invalidado	Alternativa
setAttributeMap(Map)	setAuditableAttributes(Map)
addAuditableAttributes(AccountAttributeType[],WSAttributes)	setAuditableAttributes(Map)
getAttributeMap()	getAuditableAttributes()
getAttributeValue(String)	getAuditableAttributes()
setAccountAttributesBlob(Map)	setAccountAttributesBlob(Map,Map)
setAccountAttributesBlob(WSAttributes,List)	setAccountAttributesBlob(WSAttributes, WSAttributes,List)

com.waveset.object.CacheManager

Método invalidado	Alternativa
getAllObjects(Type,AttributeCondition[])	listObjects(Type,AttributeCondition[])
getAllObjects(Type,WSAttributes)	listObjects(Type,WSAttributes)
getAllObjects(Type)	listObjects(Type)

com.waveset.object.Constants

Campo desaprobado	Alternativa
MAX_SUMMARY_STRING_LENGTH	

com.waveset.object.EmailTemplate

Método o campo desaprobado	Alternativa
setToAddress(String)	setTo(String)
getFromAddress()	getFrom()
getToAddress()	getTo()
setFromAddress(String)	setFrom(String)
VAR_FROM_ADDRESS	VAR_FROM
VAR_TO_ADDRESS	VAR_TO

com.waveset.object.Form

Método o campo desaprobado	Alternativa
EL_HELP	com.waveset.object.GenericObject#toMap(int)
getDefaultDataType()	getDefaultSyntax()
getType()	getSyntax()
setType(String)	setSyntax(Syntax)

com.waveset.object.GenericObject

Método invalidado	Alternativa
toMap(boolean)	toMap(String,int)
toMap(String,boolean)	

com.waveset.object.LoginConfig

Método invalidado	Alternativa
getApp(String)	getLoginApp(String)

com.waveset.object.MessageUtil

Método invalidado	Alternativa
getActionDisplayKey(String)	
getEventParmDisplayKey(String)	
getResultDisplayKey(String)	
getTypeDisplayKey(String)	com.waveset.ui.FormUtil#getTypeDisplayName(LighthouseContext,String)

com.waveset.object.RepositoryResult

Método invalidado	Alternativa
get(int)	next()
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	
seek(int)	hasNext() next()
sort()	

com.waveset.object.RepositoryResult.Row

Método invalidado	Alternativa
getSummaryAttributes()	getAttributes()

com.waveset.object.ResourceAttribute

Método invalidado	Alternativa
setType(String)	setSyntax(Syntax)

com.waveset.object.TaskInstance

Campo desaprobado	Alternativa
DATE_FORMAT	com.waveset.util.Util#stringToDate(String,String) com.waveset.util.Util#getCanonicalDate(Date) com.waveset.util.Util#getCanonicalDate(Date, TimeZone) com.waveset.util.Util#getCanonicalDate(long)
VAR_RESULT_LIMIT	setResultLimit(int) getResultLimit()
VAR_TASK_STATUS	

com.waveset.object.TaskTemplate

Método invalidado	Alternativa
setMode(String)	setExecMode(String)
setMode(TaskDefinition.ExecMode)	setExecMode(TaskDefinition,ExecMode)

com.waveset.object.Type

Método o campo desaprobado	Alternativa
AUDIT_CONFIG	
AUDIT_PRUNER_TASK	
AUDIT_QUERY	
DISCOVERY	
getSubtypes()	getLegacyTypes()
NOTIFY_CONFIG	
REPORT_COUNTER	

Método o campo desaprobado	Alternativa
SUMMARY_REPORT_TASK	
USAGE_REPORT	
USAGE_REPORT_TASK	

com.waveset.object.UserUIConfig

Método invalidado	Alternativa
getCapabilityGroups()	
getAppletColumns()	getAppletColumnDefs()
getCapabilityGroup(String)	
getCapabilityGroupNames()	
getFindMatchOperatorDisplayNameKeys()	
getFindMatchOperators()	
getFindResultsColumns()	
getFindResultsSortColumn()	
getFindUserDefaultSearchAttribute()	
getFindUserSearchAttributes()	
getFindUserShowAttribute(int)	
getFindUserShowCapabilitiesSearch(int)	
getFindUserShowDisabled(int)	
getFindUserShowOrganizationSearch(int)	
getFindUserShowProvisioningSearch(int)	
getFindUserShowResourcesSearch(int)	
getFindUserShowRoleSearch(int)	

com.waveset.object.ViewMaster

Método invalidado	Alternativa
ViewMaster()	ViewMaster(LighthouseContext)
ViewMaster(String,String)	ViewMaster(LighthouseContext)
ViewMaster(Subject,String)	ViewMaster(LighthouseContext)

com.waveset.session

Subclase	Método o campo desaprobado	Alternativa
SesiÃ³n	listApprovers()	getAdministrators(Map)
	listControlledApprovers()	getAdministrators(Map)
	listSimilarApprovers(String adminName)	getAdministrators(Map)
SessionFactory	getApp(String)	getLoginApp(String)
	getApps()	getLoginApps()
WorkflowServices	ARG_TASK_DATE	com.waveset.object.Attribute#DATE

com.waveset.task.TaskContext

Método invalidado	Alternativa
getAccessPolicy()	
getRepository()	

com.waveset.ui.util.FormUtil

Método invalidado	Alternativa
getAdministrators(Session,List)	getUsers(LighthouseContext,Map)
getAdministrators(Session,Map)	getUsers(LighthouseContext,Map)
getApplications(LighthouseContext,List)	getApplications(LighthouseContext,Map)
getApplications(LighthouseContext)	getApplications(LighthouseContext,Map)
getApproverNames(Session,List)	getUsers(LighthouseContext,Map)
getApproverNames(Session)	getUsers(LighthouseContext,Map)
getApprovers(Session,List)	getUsers(LighthouseContext,Map)
getApprovers(Session)	getUsers(LighthouseContext,Map)
getCapabilities(LighthouseContext,List,Map)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,List)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,String,String)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext)	getCapabilities(LighthouseContext,Map)
getObjectNames(LighthouseContext,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getOrganizations(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)

Método invalidado	Alternativa
getOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getSimilarApproverNames(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApproverNames(Session)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session)	getUsers(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,Map)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)

Método invalidado	Alternativa
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,List,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String)	getUnassignedResources(LighthouseContext,Map)

com.waveset.ui.util.html

Subclase	Método o campo desaprobado	Alternativa
Componente	isNoWrap()	
	setHelpKey(String)	
	setNoWrap(boolean)	
HtmlHeader	NORMAL_BODY	
MultiSelect	isLockhart()	
	setLockhart(boolean)	
WizardPanel	setPreviousLabel(String)	setPrevLabel(String)

com.waveset.util.JSSE

Método invalidado	Alternativa
installIfAvailable()	

com.waveset.util.PdfReportRenderer

Método invalidado	Alternativa
render(Element,boolean,String,OutputStream)	render(Element,boolean,String,OutputStream, String,boolean)
render(Element,boolean,String)	render(Element,boolean,String,String,boolean)
render(Report,boolean,String,OutputStream)	render(Report,boolean,String,OutputStream, String,boolean)
render(Report,boolean,String)	render(String,boolean,String,String,boolean)

com.waveset.util.Quota

Método invalidado	Alternativa
getQuota()	

com.waveset.util.ReportRenderer

Método o campo desaprobado	Alternativa
renderToPdf(Report,boolean,String,OutputStream)	renderToPdf(Report,boolean,String,OutputStream,String,boolean)
renderToPdf(Report,boolean,String)	renderToPdf(Report,boolean,String,String,boolean)

com.waveset.util.Trace

Método invalidado	Alternativa
data(long,Object,String,byte[])	com.sun.idm.logging.trace.Trace#data(long,String,byte[])
entry(long,Object,String,Object[])	com.sun.idm.logging.trace.Trace#entry(long,String,Object[])
entry(long,Object,String,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
entry(long,Object,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
exception(long,Object,String,t)	com.sun.idm.logging.trace.Trace#throwing(long,String,Throwable) com.sun.idm.logging.trace.Trace#caught(long,String,Throwable)
exit(long,Object,String,boolean)	com.sun.idm.logging.trace.Trace#exit(long,String,boolean)
exit(long,Object,String,int)	com.sun.idm.logging.trace.Trace#exit(long,String,int)
exit(long,Object,String,long)	com.sun.idm.logging.trace.Trace#exit(long,String,long)
exit(long,Object,String,Object)	com.sun.idm.logging.trace.Trace#exit(long,String,Object)
exit(long,Object,String)	com.sun.idm.logging.trace.Trace#exit(long,String)
getTrace()	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(Class)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(String)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
level1(Class,String)	com.sun.idm.logging.trace.Trace#level1(String)
level1(Object,String)	com.sun.idm.logging.trace.Trace#level1(String)
level2(Class,String)	com.sun.idm.logging.trace.Trace#level2(String)
level2(Object,String)	com.sun.idm.logging.trace.Trace#level2(String)
level3(Class,String)	com.sun.idm.logging.trace.Trace#level3(String)
level3(Object,String)	com.sun.idm.logging.trace.Trace#level3(String)
level4(Class,String)	com.sun.idm.logging.trace.Trace#level4(String)

Método invalidado	Alternativa
level4(Object,String)	com.sun.idm.logging.trace.Trace#level4(String)
variable(long,Object,String,String, boolean)	com.sun.idm.logging.trace.Trace#variable(long,String, String,boolean)
variable(long,Object,String,String,int)	com.sun.idm.logging.trace.Trace#variable(long,String, String,int)
variable(long,Object,String,String, long)	com.sun.idm.logging.trace.Trace#variable(long,String, String,long)
variable(long,Object,String,String, Object)	com.sun.idm.logging.trace.Trace#variable(long,String, String,Object)
void info(long,Object,String,String)	com.sun.idm.logging.trace.Trace#info(long,String,String)

com.waveset.util.Util

Método o campo desaprobado	Alternativa
DATE_FORMAT_CANONICAL	stringToDate(String,String) getCanonicalDate(Date) getCanonicalDate(Date,TimeZone) getCanonicalDate(long)
debug(Object)	
getCanonicalDateFormat()	stringToDate(String,String) getCanonicalDate(Date) getCanonicalDate(Date,TimeZone) getCanonicalDate(long)
getOldCanonicalDateString(Date,boolean)	getCanonicalDateString(Date)
rfc2396URLPieceEncode(String,String)	com.waveset.util.RFC2396URLPieceEncode #encode(String,String)
rfc2396URLPieceEncode(String)	com.waveset.util.RFC2396URLPieceEncode #encode(String)

com.waveset.workflow.WorkflowContext

Campo desaprobado	Alternativa
VAR_CASE_TERMINATED	com.waveset.object.WFProcess#VAR_CASE_TERMINATED