

Sun Java™ System Identity Manager Notas de la versión

Versión 7.1 Junio de 2007

Referencia 820-2283-10

Estas notas de versión contienen información importante que estaba disponible en el momento del lanzamiento de Sun Java System Identity Manager 7.1. Además de tratarse otros temas, aquí se describen las funciones, las mejoras, las limitaciones y los problemas conocidos del producto. Lea este documento antes de empezar a utilizar Identity Manager 7.1.

Las notas de la versión se han organizado en distintas secciones:

- [Introducción](#)
- [Identity Manager 7.1 Funciones](#)
- [Problemas detectados](#)
- [Notas de instalación y actualización](#)
- [API desaprobada](#)
- [Anexos a la documentación y correcciones](#)

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

NOTA Sun no se hace responsable de la disponibilidad de los sitios web de terceros que se mencionan en este documento. Sun no avala ni se hace responsable del contenido, la publicidad, los productos ni otros materiales disponibles en dichos sitios o recursos, o a través de ellos. Sun tampoco se hace responsable de daños o pérdidas, supuestos o reales, provocados por el uso o la confianza puesta en el contenido, los bienes o los servicios disponibles en dichos sitios o recursos, o a través de ellos.

Introducción

En esta sección de las Notas de la versión de Identity Manager 7.1 se proporciona la siguiente información:

- [Software y entornos admitidos](#)
- [Itinerarios de actualización y política de finalización del periodo de asistencia](#)
- [Archivos redistribuibles](#)
- [Procedimiento para informar de problemas y enviar comentarios](#)
- [Envío de comentarios a Sun](#)
- [Otros recursos de Sun](#)

Software y entornos admitidos

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

- [Sistemas operativos](#)
- [Servidores de aplicación](#)
- [Servidores de repositorio de bases de datos](#)
- [Puerta de enlace de Sun Identity Manager](#)
- [Recursos admitidos](#)
- [Servidores Web](#)
- [Exploradores](#)
- [Software discontinuado](#)

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

Esta versión de Identity Manager es compatible con los siguientes 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 x86
- 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 indicados a continuación). Identity Manager requiere JDK 1.4.2 o superior:

- Apache® Tomcat
 - Versión 4.1.x (con JDK 1.4.2)
 - Versión 5.0.x (con JDK 1.4.2)
 - Versión 5.5.x (con JDK 1.5)
- BEA WebLogic® Express 8.1 (con JDK 1.4.2 o superior)
- BEA WebLogic® Server™ 8.1 (con JDK 1.4.2 o superior)
- BEA WebLogic® Server™ 9.1, 9.2
- IBM WebSphere® 6.0, 6.1
- IBM WebSphere® Application Server - Express 5.1.1 (con JDK 1.4.2)
- JBoss Application Server 4.0.x
- 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

- Sun Java™ System Application Server Enterprise Edition 8.2

NOTA Si el servidor de aplicación actual no admite JDK 1.4.2 o superior, póngase en contacto con el distribuidor para analizar las consecuencias de actualizar a uno que sí lo admita antes de instalar Identity Manager 7.1.

Servidores de repositorio de bases de datos

Identity Manager es compatible con los siguientes 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™ 2005
- MySQL™ 5.0

NOTA Identity Manager sólo es compatible con MySQL en un entorno de desarrollo. No admite MySQL en entornos de producción.

- Oracle 9i® y Oracle Database 10g, 10g Release 1 y 10g Release 2®

NOTA Oracle RAC (Real Application Cluster) puede utilizarse en una configuración de dos nodos activo-pasivo, es decir, una configuración donde el parámetro `active_instance_count` esté definido en 1. En combinación con el control de fallos de conexión para el controlador JDBC, proporciona capacidad de control de fallos para el repositorio. (Consulte cómo configurarlo para su entorno en la documentación de Oracle.)

De momento Oracle RAC no se admite en ninguna otra configuración.

Puerta de enlace de Sun Identity Manager

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

NOTA Se ha desaprobadado el adaptador Novell GroupWise, que dejará de ser compatible en la próxima versión principal de Identity Manager. Sin embargo, en su lugar puede utilizarse el adaptador NetWare NDS, que admite cuentas de GroupWise.

Recursos admitidos

El software Identity Manager admite estos recursos:

- [Gestión de las relaciones con los clientes \(CRM\)](#)
- [Bases de datos](#)
- [ERP \(Planificación de recursos empresariales\)](#)
- [Servicio de asistencia](#)
- [Plataformas de mensajes](#)
- [Misceláneo](#)
- [Sistemas operativos](#)
- [Sistema de administración de roles](#)
- [Gestores de seguridad](#)
- [Control de acceso Web](#)

Gestión de las relaciones con los clientes (CRM)

- Software CRM Siebel, versiones 6.2, 7.0.4, 7.7, 7.8.

Bases de datos

- Tabla de base de datos genérica
- 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, 2005
- MySQL™ 4.1.x, 5.x
- Oracle 9i®
- Oracle Database 10g Release 1®
- Sybase Adaptive Server® 12.x
- JDBC con secuencia de comandos

Directorios

- LDAP v3
- RACF LDAP
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory en Novell NetWare 5.1, 6.0 y 6.5
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java(TM) SystemDirectory 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(TM) 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 E-Business Suite en Oracle Applications 11.5.9, 11.5.10
- Peoplesoft® PeopleTools 8.1 a 8.48 con HRMS 8.0 a 9.0
- 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)
- SAP® GRC (Governance, Risk, and Compliance) Access Enforcer

Servicio de asistencia

- Remedy Help Desk 4.5, 5.0, 6.0
- BMC Remedy Action Request System Server 6.0, 6.03 y and 7.0
- BMC Remedy Service Desk Application 7.0

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, 7.0 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 6.0, 6.5 y 7.0 (con el adaptador Novell NDS)

NOTAS

- Microsoft Exchange 2000 y 2003 se administran a través de los recursos de Microsoft Windows Active Directory 2000 y 2003.
 - Es posible que en próximas versiones no se incluya soporte para BlackBerryResourceAdapter. Las futuras implementaciones que requieran adaptadores de recursos para Blackberry Enterprise Server Versión 4+ deberían basarse en ScriptedGatewayResourceAdapter.
 - Se ha desaprobado el adaptador Novell GroupWise, que dejará de ser compatible en la próxima versión principal de Identity Manager. Sin embargo, en su lugar puede utilizarse el adaptador NetWare NDS, que admite cuentas de GroupWise.
-

Misceláneo

- Archivos sin formato
- 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
- Secuencia de comandos de shell genérica UNIX
- 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

Sistema de administración de roles

- BridgeStream SmartRoles

Gestores de seguridad

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Host de secuencia de comandos
- INISafe Nexess 1.1.5
- RSA ClearTrust 5.5.2, 5.5.3
- 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 (Realms se admite desde 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

Exploradores

Identity Manager es compatible con los siguientes exploradores:

- Microsoft Internet Explorer 5.x y posterior
- Safari v2.0 y posterior para Mac OS X 10.3.3 y posterior
- Mozilla 1.78 (con JRE 1.5)
- Firefox 1.0x, 1.5 (con JRE 1.5), 2.0 y posterior

Software discontinuado

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.

Categoría de software	Paquete de software
Sistemas operativos	<ul style="list-style-type: none"> • IBM AIX 4.3.3
Servidores de aplicación	<ul style="list-style-type: none"> • Apache Tomcat 4.1.x • BEA Weblogic Express 8.1 • BEA Weblogic Server 8.1 • IBM Websphere Application Server - Express 5.1.1 • IBM Websphere 6.0 • Sun ONE Application Server 7
Servidores de repositorio de bases de datos	<ul style="list-style-type: none"> • MySQL 4.1 • Microsoft SQL 2000
Recursos	<ul style="list-style-type: none"> • ActivCard 5.0 • Lotus Notes (Domino) 5.0.x, 6.0.x • Microsoft Windows NT 4.0 • Puerta de enlace de Sun Identity Manager en Microsoft Windows NT 4.0 • MySQL 4.1 • Novell® GroupWise 5.x, 6.0, 6.5 • Novell® eDirectory en Novell NetWare 5.1, 6.0 • Oracle 8i (con el adaptador de recursos de Oracle) • Red Hat Linux 8.0 • Remedy® Help Desk 4.5, 5.0. • SAP R/3 v4.5, v4.6 • Siebel 6.2 • Sun ONE Identity Server 6.0

El siguiente software dependiente dejará de ser compatible con Identity Manager 7.1:

Categoría de software	Paquete de software
Servidores de repositorio de bases de datos	<ul style="list-style-type: none"> • Oracle 8i • IBM DB2 Universal Database para Linux, UNIX y Windows 7.0
Sistemas operativos	<ul style="list-style-type: none"> • Solaris 7, Microsoft Windows NT 4.0
Recursos	<ul style="list-style-type: none"> • Microsoft Exchange 5.5 • IBM DB2 7.0 • Novell® GroupWise 5.x

Compatibilidad API

La Interfaz de programación de aplicaciones (API) de Identity Manager 7.1 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
Sesión	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
Adaptador	com.waveset.adapter.*
	com.waveset.util.Trace
Directiva	com.waveset.policy.PolicyImplementation
	com.waveset.policy.StringQualityPolicy
Informe	com.waveset.report.BaseReportTask
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.* 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 desaprobadas

En la sección [“API desaprobada”](#) de estas Notas de la versión se enumeran todas las interfaces de programación de aplicaciones de Identity Manager que se han desaprobado en esta versión y las alternativas (si existen).

Itinerarios de actualización y política de finalización del periodo de asistencia

En esta sección se proporciona información sobre los itinerarios de actualización de Identity Manager y se describe la política de finalización del periodo de asistencia de Identity Manager.

Itinerarios de actualización de Identity Manager

Utilice la tabla siguiente para conocer el itinerario de actualización que deberá seguir cuando quiera cambiar a una nueva versión de Identity Manager.

Versión actual	Versión de destino				
	5.0	2005Q3M1	2005Q4M3	7.0	7.1
Waveset Lighthouse 4.1 SPx	5.0	5.0 > 2005Q3M1	5.0 > 2005Q4M3	5.0 > 2005Q4M3 > 7.0	5.0 > 2005Q4M3 > 7.1
Identity Manager 5.0 SPx		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q1M3 Identity Auditor 1.0		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q3M1 Identity Manager 5.5			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q3M3 Identity Manager SPE 1.0			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q4M3 Identity Manager 6.0				7.0	7.1
Identity Manager 7.0					7.1

NOTAS

- Cuando se actualiza Identity Manager no es necesario instalar los Paquetes de servicios de las versiones principales en otras versiones principales. Por ejemplo, si sustituye Identity Manager 5.0 por la versión 6.0, no tiene que instalar ninguno de los Paquetes de servicios de la versión 5.0.
 - Los Paquetes de servicios de las versiones principales son acumulativos. Después de la actualización, puede instalar el último paquete sin tener que instalar todos los paquetes de esa versión. Por ejemplo, si ha actualizado a la versión Identity Manager 5.0, la instalación del paquete SP6 proporciona toda la funcionalidad de los paquetes anteriores (del SP1 al SP5).
-

Las actualizaciones de la documentación de Identity Manager se suministran de la forma siguiente:

- **En cada versión** (incluidos los Paquetes de servicios): Se suministran Notas de la versión para describir correcciones de errores, mejoras del producto, nuevas funciones y otros datos de interés.
- **Para las versiones principales (x.0)**: Se actualiza y reedita la documentación completa de Identity Manager.
- **Para las versiones y los paquetes de servicios secundarios**: Se actualizan y reeditan determinados documentos o se suministra un Anexo a la documentación.

Fin del periodo de servicio de asistencia del software

Durante el periodo de finalización del servicio (End of Service Life o EOSL), la asistencia técnica correspondiente al software de Identity Manager se proporciona en dos fases:

- *Fase 1: Asistencia completa*
- *Fase 2: Asistencia limitada*

NOTA La duración de la fase de asistencia completa varía según el producto.

Fase de asistencia completa

Durante la fase de asistencia completa, Sun Microsystems, Inc. proporciona 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, cuando se anuncie la fecha de obsolescencia (End of Life o EOL) de un producto de software, el cliente dejará de tener acceso a actualizaciones de ese producto.

Fase de asistencia limitada

Durante la fase de asistencia limitada, Sun Microsystems, Inc. proporciona todos los servicios de asistencia enumerados 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 Microsystems, Inc. y, como en el caso de la fase de asistencia completa, cuando se anuncie la obsolescencia del producto, no tendrán acceso a actualizaciones del mismo.

La tabla siguiente proporciona información sobre las fechas de obsolescencia y finalización del servicio de asistencia previstas para las versiones anteriores de Identity Manager.

Nombre del producto	Estado del producto	Fecha del último envío	Fin de la fase 1	Fin de la fase 2 (EOSL)	Anuncio de obsolescencia
Sun Java System Identity Manager 7.0	Post-RR				
Sun Java System Identity Manager 6.0 2005Q4	Post-RR	05/25/2007	05/25/2008	05/2012	11/20/06
Sun Java System Identity Auditor 1.0 2005Q1	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager Service Provider Edition 1.0 2005Q3	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager 5.0 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.0 SPx 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.5	EOL	08/11/2006	08/2007	08/2011	02/07/06
Waveset Lighthouse 4.1			03/2006	03/2010	

Archivos redistribuibles

Sun Java System Identity Manager 7.1 no contiene ningún archivo que pueda redistribuirse.

Procedimiento para informar de problemas y enviar comentarios

Si experimenta algún problema con Sun Java System Identity Manager, póngase en contacto con el servicio de atención al cliente de Sun mediante uno de estos procedimientos:

- Servicios de asistencia de software en línea disponibles en <http://www.sun.com/service/sunone/software>

Este sitio incluye vínculos con la base de datos de conocimiento, el centro de asistencia en línea (Online Support Center) y la herramienta ProductTracker, así como con programas de mantenimiento y números para contactar con el personal de asistencia técnica.

- El número de asistencia telefónica asociado a su contrato de mantenimiento

Para ayudarle a resolver cualquier problema con eficacia, tenga la siguiente información a mano cuando se ponga en contacto con el servicio de asistencia:

- La descripción del problema, lo que incluye el contexto en el que se ha producido y el impacto que ha tenido sobre el funcionamiento del sistema.
- El tipo de máquina, la versión del sistema operativo y la versión del producto, incluido cualquier parche o paquete de software que pueda estar implicado en el problema.
- Una descripción pormenorizada del procedimiento que ha seguido para reproducir el problema.
- Los archivos de registro o volcado del núcleo.

Envío de comentarios a Sun

En Sun estamos interesados en mejorar nuestra documentación y, por tanto, agradecemos sus comentarios y sugerencias.

Para enviarnos sus comentarios, entre en <http://docs.sun.com> y haga clic en Enviar comentarios. En el formulario que aparece, especifique el título y el número de referencia del documento. El número de referencia es un número de siete o nueve dígitos que se encuentra en la portada del libro o en la parte superior del documento. Por ejemplo, el título de este documento es Sun Java System Identity Manager Junio de 2007 Notas de la versión, y el número de referencia es 820-2283-10.

Otros recursos de Sun

En las siguientes direcciones de Internet encontrará información útil sobre Sun Java System :

- Documentación de Sun Java™ System Identity Manager
<http://docs.sun.com/app/docs/coll/1514.1>
- Documentación de Sun Java System
<http://docs.sun.com/prod/java.sys>
- Sun Java System Professional Services
<http://www.sun.com/service/sunps/sunone>
- Productos y servicios correspondientes al software de Sun Java System
<http://www.sun.com/software>
- Servicios de asistencia para el software Sun Java System
<http://www.sun.com/service/sunone/software>
- Base de datos de conocimiento y asistencia técnica de Sun Java System
<http://www.sun.com/service/support/software>
- Servicios de formación y asistencia de Sun
<http://training.sun.com>
- Servicios profesionales y de consultoría relacionados con Sun Java System
<http://www.sun.com/service/sunps/sunone>
- Información de Sun Java System para desarrolladores
<http://developers.sun.com>
- Servicios de asistencia para desarrolladores
<http://www.sun.com/developers/support>
- Formación sobre Sun Java System
<http://www.sun.com/software/training>
- Hojas de producto del software de Sun
<http://www.sun.com/software>

Copyright © 2007 Sun Microsystems, Inc. Reservados todos los derechos.

Sun Microsystems, Inc. tiene derechos de propiedad intelectual relacionados con la tecnología del producto que se describe en este documento. Especialmente, aunque sin limitarse a ellos, dichos derechos de propiedad intelectual pueden incluir una o varias de las patentes de EE.UU. que aparecen en <http://www.sun.com/patents>, así como otras patentes adicionales o solicitudes de patentes en EE.UU. y otros países.

INFORMACIÓN CONFIDENCIAL PROPIEDAD DE SUN.

Derechos del gobierno de Estados Unidos: software comercial. Los usuarios gubernamentales están sujetos al acuerdo de licencia estándar de Sun Microsystems, Inc. y a las disposiciones aplicables de la regulación FAR y sus suplementos.

El uso está sujeto a las condiciones de la licencia.

La distribución puede incluir materiales desarrollados por terceras partes.

Partes del software pueden derivarse del sistema Berkeley BSD, concedido mediante licencia por la Universidad de California.

Sun, Sun Microsystems, el logotipo de Sun, Java y Solaris son marcas comerciales o marcas comerciales registradas de Sun Microsystems, Inc. en Estados Unidos y otros países. Todas las marcas registradas SPARC se utilizan bajo licencia y son marcas registradas de SPARC International, Inc. para los EE.UU. y otros países.

Identity Manager 7.1 Funciones

En esta sección de las Notas de la versión de Identity Manager 7.1 se proporciona la siguiente información:

- [Novedades de esta versión](#)
- [Problemas corregidos en esta versión](#)

Novedades de esta versión

En esta sección se proporciona información adicional sobre las nuevas funciones de Identity Manager 7.1. Esta información se ha organizado como sigue:

- [Instalación y actualización](#)
- [Interfaces de administrador y usuario](#)
- [Auditoría](#)
- [Formularios](#)
- [Entorno de desarrollo integrado \(IDE\) de Identity Manager](#)
- [Identity Manager SPE](#)
- [Repositorio](#)
- [Recursos](#)
- [Roles](#)
- [Seguridad](#)
- [Servidor](#)

Instalación y actualización

- Utilice el atributo del sistema `waveset.serverId` para configurar nombres de servidor que no estén repetidos cuando la instalación incluya varias instancias de Identity Manager vinculadas con un solo repositorio de un único servidor físico. (ID-11578)
- La instalación y actualización pueden realizarse en un sistema sin pantalla. (ID-14258)
- En `sample/create_spe_tables.mysql` se proporciona una secuencia de comandos para crear una base de datos de transacciones de Identity Manager Service Provider para MySQL. (ID-14666)

MySQL no se admite como base de datos de transacciones de Service Provider. La secuencia de comandos sólo sirve como ejemplo.

- Para localización: Debido a que se ha eliminado el archivo `RAMessage_110n.jar`, antes imprescindible en el proceso previo de actualización, es preciso descargar traducciones para los adaptadores. (ID-16272)

Puede descargar paquetes de idioma en Sun Download Center, que forma parte del Centro de Soporte Online (<http://www.sun.com/download>). Para acceder al centro de descargas necesita registrarse y disponer de un nombre de cuenta y una contraseña.

Para obtener más información, consulte Instalación de Identity Manager 7.1 y el archivo Léame de Identity Manager L10n, que se suministra con todos los paquetes de idioma de IDM.

Interfaces de administrador y usuario

- Si olvida su ID de usuario, puede seleccionar `Forgot My User ID` en `login.jsp` o `user/login.jsp` para acceder a una página nueva de búsqueda de ID de usuario. En esta página se puede introducir una dirección de correo electrónico para notificaciones junto con algunos datos de identidad adicionales (como el número de teléfono, el nombre, el apellido, el ID de empleado, etc.) para que Identity Manager busque el usuario que posee dichos atributos de identidad. (ID-4924)
 - Si la búsqueda produce resultados satisfactorios, Identity Manager envía un mensaje que contiene el ID de usuario de Identity Manager a la dirección de notificación que se ha especificado. (Con este fin se ha creado una nueva plantilla de correo electrónico que permite recuperar el ID de usuario. Como el asunto y el texto de esta plantilla son claves de mensaje, se pueden personalizar e internacionalizar.)
 - Si la búsqueda no produce resultados, Identity Manager genera un mensaje de error para avisar que no ha encontrado ningún usuario con esas características o que ha encontrado varios usuarios con los mismos datos.

Aunque esta función está habilitada de forma predeterminada, se puede deshabilitar.

- Cuando se modifica un módulo de inicio de sesión de un recurso (ID de usuario/contraseña de sistema no Identity) en el ámbito de un grupo de módulos de inicio de sesión (Seguridad > Ingresar), es posible seleccionar una regla de correlación de inicio de sesión para asignar la información de ingreso proporcionada por el usuario a un usuario de Identity Manager.

Identity Manager emplea la lógica especificada en la regla de correlación de inicio de sesión para buscar usuarios de Identity Manager. La regla debe presentar una lista que contenga uno o varios elementos `AttributeConditions` para que sea posible buscar el usuario de Identity Manager que cumpla estas condiciones.

Por ejemplo, es posible que baste con buscar la coincidencia de ID de usuario de Identity Manager. Si se ha asignado un ID de cuenta de recursos LDAP a los usuarios de Identity Manager, podrán realizarse búsquedas por ID de cuenta y no será necesario que los usuario de Identity Manager dispongan de vínculos con el recurso de Sun Access Manager. La regla de correlación de inicio de sesión debe tener un tipo de autenticación (`authType`) `LoginCorrelationRule`. (ID-8577)

- Ya no se indica el estado de sincronización en la columna de descripción de la tabla del árbol de recursos. En la columna de estado se indica una combinación de los estados de reconciliación y sincronización. (ID-12465, ID-14005)
- 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-14899)

Para obtener más información, consulte *Sun Java(TM) System Identity Manager Administration*.

Auditoría

- Ahora las infracciones de directivas se pueden priorizar asignándoles un nivel de prioridad, de gravedad o ambos. Las infracciones se priorizan en la página de remediaciones. Para obtener más información, consulte “Prioritizing Policy Violations” en *Identity Manager Administration*. (ID-11703)
- Las exploraciones de directivas de auditoría exploran los miembros de las organizaciones dinámicas. (ID-12437)
- Las exploraciones de directivas de auditoría son programables. (ID-12474)
- Las exploraciones de auditoría tienen un modo de prueba, que desactiva la remediación y elimina todas las infracciones al terminar la exploración. (ID-12522)
- El informe resumido de infracciones se ha ampliado para poder seleccionar las infracciones que comete el estado de infracción. Es posible configurar el informe de modo que sólo incluya las infracciones correspondientes a uno o varios estados posibles. (ID-12612)
- Las entradas del registro de auditoría que están relacionadas con la aprobación, la desaprobación y la remediación de revisiones de acceso se pueden firmar digitalmente. (ID-13264)

- Si entra en la página de revisión después de ejecutar una revisión periódica de los accesos, no verá la exploración en la lista a menos que haga clic en el botón Regenerar. (D-14169)
- Los empalmes de directorios y las organizaciones virtuales permiten la asignación de directivas de auditoría. (ID-14591)
- El ámbito de usuario de la exploración de acceso se puede definir en función de los recursos asignados. (ID-14654)
- Ahora se puede ver rápidamente el cumplimiento de Identity Manager si se instala el entorno de demostración. (ID-14970)

El entorno de demostración del cumplimiento se puede instalar importando `sample/auditor demo.xml` o creando un entorno propio mediante las herramientas que ofrece el compilador de reglas de cumplimiento (Compliance/RuleBuilder). Consulte `Compliance/RuleBuilder/README.txt` para obtener más información.

- Los autenticadores y remediadores pueden especificar formularios que muestren exactamente los detalles necesarios para aumentar la eficacia al autenticar y remediar. Para obtener más información, consulte la sección Anexos a la documentación y correcciones de estas Notas de la versión. (ID-14973)
- Durante la remediación se puede volver a evaluar una infracción del cumplimiento para determinar si sigue vigente. Para que no se vuelva a infringir la directiva de auditoría, modifique los datos de usuario. (ID-15019)
- Los derechos de revisión de acceso pendientes se pueden actualizar con datos recientes. (ID-15027)
- El remediador de revisión de acceso puede editar (reaprovisionar) un usuario directamente mediante el nuevo botón de edición del formulario de remediación. (ID-15172)
- El remediador de revisión del cumplimiento puede editar (reaprovisionar) un usuario directamente mediante el nuevo botón de edición del formulario de remediación. (ID-15173)
- En la revisión de acceso se pueden modificar los derechos de usuario de varias maneras: (ID-15180)
 - Mediante el uso de Reexplorar, el autenticador de revisión de acceso puede solicitar una exploración para actualizar y evaluar de nuevo los derechos de usuario.
 - El remediador de revisión de acceso puede hacer clic en Remediada para que los derechos de usuario se actualicen y se vuelvan a evaluar.
- La creación de un derecho de usuario en el estado REMEDIANDO genera automáticamente un elemento de trabajo de remediación. (ID-15423)

Para obtener más información, consulte el capítulo 2, “Working with Rules”, en *Identity Manager Deployment Tools*.

Nota sobre la actualización: El aviso de autenticación masiva y todas las plantillas de correo electrónico se conservan después de una actualización. En el aviso de autenticación masiva del archivo `auditorwfs.xml` se explica la forma de implementar las variables de notificación del nuevo elemento de trabajo de remediación de revisión de acceso.

- En las exploraciones de auditor se pueden especificar recursos de destino para cuentas múltiples de forma más explícita. (ID-15485)
- La página de gestión de objetos de directiva de auditoría ahora se basa en formularios y es personalizable. Es posible seleccionar una vista completa repleta de información o restringir el nivel de detalle a una vista parcial. Para obtener más información, consulte el Anexo a la documentación de estas Notas de la versión. (ID-15486)
- La página de gestión de exploraciones de acceso ahora se basa en formularios y es personalizable. Para obtener más información, consulte el Anexo a la documentación de estas Notas de la versión. (ID-15515)
- Los informes de los registros de auditoría presentan detalles relacionados con los cambios de rol. (ID-15587)
- De manera predeterminada, sólo se registran los siguientes eventos de derechos de usuario (ID-15735):
 - Autenticador aprobado
 - Autenticador rechazado
 - Remediación solicitada
 - Reexploración solicitada
 - Terminar

Formularios

- La clase de presentación `TabPanel` permite ejecutar expresiones de validación en función de la ficha. Cuando se configura la propiedad de presentación `validatePerTab` en **true**, Identity Manager, las expresiones de validación se ejecutan en cuanto el usuario cambia a una ficha diferente. (ID-12442)
- La carpeta `sample/forms` contiene un nuevo formulario VMS de ejemplo. (ID-12835)

Entorno de desarrollo integrado (IDE) de Identity Manager

El Identity Manager Integrated Development Environment (Identity Manager IDE) es una aplicación Java que permite ver, personalizar y depurar objetos de Identity Manager en la implementación.

Las nuevas funciones añadidas (o modificadas) en el Identity Manager IDE en Identity Manager 7.1 son:

NOTA Para obtener más información sobre estas funciones, consulte *Identity Manager Deployment Tools*

- El Identity Manager IDE admite objetos genéricos. (ID-12952, 12991)
- La barra de menús de nivel superior de NetBean incluye ahora un menú IdM, que permite seleccionar acciones adecuadas a los nodos de los objetos seleccionados. (ID-13158)
- El proyecto Identity Manager IDE 7.0 se ha sustituido por los dos tipos siguientes, que son ambos proyectos NetBeans ant: (ID-14587)
 - **Identity Manager Project:** Es un entorno de desarrollo básico para desarrolladores que dispone de todas las funciones, entre ellas:
 - Edición, compilación y depuración en Java/JSP
 - Ejecución de Identity Manager en un servidor de aplicación incrustado en Netbeans
 - Administración de repositorios incrustados

Este tipo de proyecto proporciona un repositorio sencillo que le puede servir para realizar comprobaciones en una zona protegida. Al crear este tipo de proyecto, se puede especificar un repositorio incrustado para el proyecto. Además, es posible habilitar una opción de gestión del repositorio incrustado para reinicializarlo. El Identity Manager IDE ofrece una función de autopublicación que carga automáticamente el repositorio incrustado siempre que se ejecuta o depura el proyecto.
 - Un entorno de compilación de configuración (CBE) y un generador de archivos de importación de ejemplo.

Para obtener más información sobre el CBE, consulte el archivo `README.txt` suministrado con Identity Manager Project.
 - **Identity Manager Project (Remote):** Se utiliza para realizar pequeños cambios y depurar proyectos remotos en un servidor externo. Es un tipo de proyecto compacto y rápido de configurar que dispone de las mismas funciones de edición que Identity Manager Project, pero carece de entorno de compilación y no permite abrir el archivo `war`.

- El Identity Manager IDE ahora es independiente de la versión. (ID-14723)

La versión 7.1 del `.nbm` del Identity Manager IDE se ha desconectado de las clases de Identity Manager. El `.nbm` versión 7.1 es compatible con Identity Manager 7.0 y 7.1, y se prevé que también lo sea con Identity Manager 6.0 SP3.

Cada proyecto del Identity Manager IDE está ligado a una versión específica de Identity Manager, y el Identity Manager IDE ahora requiere un paquete de compatibilidad (`ide-bundle.zip`) que aporte los archivos `jar` de Identity Manager y algunos registros XML con información específica para cada versión de Identity Manager admitida. El paquete de compatibilidad se especifica al crear un proyecto:

- Para **Identity Manager Project**: El paquete de compatibilidad se incluye en el archivo `idm.war`, al que Identity Manager IDE accede automáticamente durante la configuración del proyecto.
- Para **Identity Manager Project (Remote)**: Dado que no se especifica la ubicación del archivo `war` para los proyectos remotos, hay que indicar dónde se encuentra el paquete de compatibilidad, que está en:

Identity Manager install root/sample/ide-bundle.zip

NOTA Identity Manager versión 7.0 no ofrecía paquete de compatibilidad para el IDE, pero el archivo se puede descargar del sitio de descargas de Identity Manager 7.0.

- Los objetos de la biblioteca, que disponen de hojas de propiedades, funciones de paleta y nodos de navegación, se han añadido a la lista de tipos de objetos que aparecen en la ventana del Explorador. (ID-14817)
- En la actualidad es necesario utilizar JDK 1.5 y Netbeans 5.5 con el plugin de Identity Manager IDE. (ID-14950)
- Ahora se puede comparar un solo objeto (diff) o una carpeta de objetos (de forma recursiva) de un directorio local con los del repositorio. Esta función permite apreciar las diferencias entre las copias locales y las del servidor. Además, sirve para transferir y recargar uno o varios objetos modificados. (ID-15151, 15206)
- Cuando se selecciona la vista de diseño de un objeto de regla, en la ventana del editor aparece un generador de expresiones que permite distinguir con facilidad la estructura lógica de la regla y modificar sus propiedades. (ID-15104)
- Los cuadros de diálogo del generador de expresiones del Identity Manager IDE incorporan nuevas funciones. Ahora es posible:

- Modificar tipos de datos simples (enteros y cadenas) directamente en la tabla del generador de expresiones. (ID-15528)
- Ver JavaDoc para métodos de API de Identity Manager al definir sentencias de invocación XPRESS (estáticas o de instancia) en los cuadros de diálogo del generador de expresiones. (ID-12961)

Cuando se seleccionan clases o métodos en los menús de nombre de clase y de nombre de método del generador de expresiones, el JavaDoc relacionado emerge junto al cuadro de diálogo. (ID-12960)

- Editar valores de propiedades que admiten expresiones y primitivas (como cadenas) directamente en una tabla de propiedades. (ID-13763)
 - Crear una expresión concreta en lugar de crear primero un BLOQUE para después convertirlo en la expresión deseada. (ID-15932)
 - Incluir o “envolver” un elemento de una expresión en otro elemento, lo que permite crear expresiones desde dentro hacia fuera.
 - Cambiar el tipo de expresión de un elemento con un nuevo botón y cuadro de diálogo de cambio. (ID-15933)
- El Identity Manager IDE ahora ofrece nodos distintos para los archivos, objetos persistentes y extensiones, con el fin de reflejar mejor el contenido XML subyacente. Además, es posible reordenar e insertar nodos en otras posiciones (antes, después o dentro de otros nodos en el árbol de proyecto). (ID-14689)
 - Los objetos del repositorio del Identity Manager IDE se pueden eliminar. (ID-14081, 15031)
 - Es posible transferir un objeto del Identity Manager IDE a un servidor de Identity Manager 7.0 y asignarle un ID de objeto manualmente. (ID-15474)
 - Para facilitarle el traslado de objetos entre repositorios, ahora puede configurar Identity Manager IDE de manera que elimine todos los ID de repositorio generados automáticamente antes de descargar objetos del repositorio. (ID-15307, 15347)

Identity Manager IDE busca y elimina todos los ID de objeto y de referencia de objeto que corresponden a una expresión especificada, sin suprimir los ID predefinidos en el código interno.

- Al editar formularios, ahora se pueden seguir las referencias a formularios y campos. Además, al editar flujos de trabajo, se pueden seguir los procesos externos. El Identity Manager IDE abre el archivo referenciado y busca la referencia. (ID-14428, 15406)
- Es posible especificar un contexto raíz dejando vacío el campo Contexto al crear el proyecto. (ID-15912)

Identity Manager SPE

- Identity Manager Identity Manager SPE admite reglas de correlación y confirmación de vínculo. (ID-10500) Para obtener más información, consulte la descripción del error de software 15760 en el Anexo a la documentación de estas Notas de la versión.
- Las respuestas de autenticación para usuarios de Service Provider se pueden modificar en la interfaz administrativa. (ID-12781)
- Los atributos LDAP borrados ahora se propagan una vez que vuelve a estar disponible un recurso inactivado. (ID-15471)

Informes

- Ahora se puede controlar globalmente la fuente utilizada al generar informes, para lo cual se editan los valores de la página Configurar > Informes. También se pueden reemplazar editando la configuración de cada informe. De manera predeterminada sólo se muestran las fuentes disponibles para todos los visores de PDF.

Para agregar otras fuentes al sistema, copie sus archivos de definición al directorio `WEB-INF/fonts` dentro del directorio donde está implementado IDM (por ejemplo, `/var/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm/WEBINF/fonts`). A continuación hay que reiniciar el servidor. Los formatos de definición de fuente aceptados incluyen `.ttf`, `.ttc`, `.otf` y `.afm`. Si se selecciona una de estas fuentes, la misma fuente deberá estar disponible en la máquina donde se visualice el informe o bien estar incluida en el informe.

Como el conjunto de fuentes predeterminado no admite todos los juegos de caracteres (por ejemplo, los asiáticos), es preciso instalar otra fuente en el directorio `fonts/` y seleccionarla en las páginas de configuración para generar informes capaces de mostrar otros juegos de caracteres. (ID-10641/14376)

NOTA Las licencias de las fuentes TrueType ofrecen distintos niveles de incrustación de fuentes. La licencia debe permitir incrustar para impresión y vista preliminar en el PDF la fuente elegida para generarlo. Si se carece de la licencia adecuada para incrustar la fuente en el PDF, éste se generará con una fuente estándar y, en consecuencia, el contenido del PDF quedará dañado. Actualmente, Identity Manager no registra un error para advertir de este problema.

Repositorio

- Ahora se ofrece información sobre el tamaño de los objetos del repositorio. Puede acceder a esta información a través de las páginas Web y desde la línea de comandos de la consola. (ID-9896)

NOTA Cuando se realicen actualizaciones, los objetos existentes presentarán un tamaño 0 hasta que se hayan actualizado.

Recursos

Adaptadores de recursos nuevos

Esta versión incorpora adaptadores nuevos:

- RACF LDAP
- SAP Governance, Risk, and Compliance (GRC) Access Enforcer

Para obtener información detallada sobre estos adaptadores de recursos, consulte *Identity Manager Resources Reference*.

Actualizaciones de adaptadores de recursos

- Los servidores que ejecutan ActiveSync ahora se tienen que configurar en la directiva de sincronización del recurso. El uso de `waveset.properties` se ha desaprobado, pero sigue disponible. Se recomienda migrar a la configuración en la directiva de sincronización. (ID-10167)
- La configuración del adaptador Flat File Active Sync se ha simplificado, sobre todo en el caso de los archivos delimitados. (ID-11678)
- Active Sync puede terminarse antes de que se hayan procesado todas las actualizaciones en el adaptador LDAP. (ID-13695)
- Identity Manager ahora es compatible con PeopleSoft HRMS 9.0. (ID-14195)
- El adaptador de Domino permite configurar el atributo de directiva explícita de los recursos de Domino 7.0. (ID-14315)
- El adaptador de recursos de Oracle ERP admite acciones antes y después. (ID-14659)

- 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)
- Se han añadido los atributos de recurso Grupo primario predeterminado y Shell de inicio de sesión a los adaptadores de recursos Solaris, AIX, HP-UX, Red Hat Linux y SuSE Linux: (ID-15034)
- El adaptador NDS ofrece mejor compatibilidad con GroupWise:
 - El adaptador ahora puede gestionar oficinas de correos en dominios secundarios. (ID-15122)
 - Los usuarios de GroupWise pueden suscribirse a cualquier lista de distribución conocida. (ID-15707)
 - El adaptador ya no utiliza el parámetro **Delete Pattern** como mecanismo para indicar que hay que eliminar una oficina de correos de un usuario de GroupWise. Con el nuevo método, no hay más que definir el campo de oficina de correos en "" (dos comillas). Si tiene formularios o flujos de trabajo anteriores programados para eliminar oficinas de correos, cámbielos para definir el campo en ". (ID-15970)
- El adaptador de recursos utilizado con los servidores Domino 7.0 admite usuarios móviles. (ID-15157)
- 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 ACF2 admite ACF2 8.0 SP2. (ID-15833)
- El formulario de ejemplo `NDSUserForm` incluye ejemplos válidos de las siete técnicas para obtener oficinas de correos y listas de distribución. (ID-15872)
- El adaptador de interfaz de componente de PeopleSoft permite especificar claves separadas para las operaciones GET, FIND y CREATE en la interfaz de componente. (ID-16055)
- El adaptador de interfaz de componente de PeopleSoft es compatible con PeopleTools 8.1 a 8.48. (ID-16128)
- El adaptador de recursos de Top Secret gestiona correctamente los comandos `ASUSPEND`, `PSUSPEND`, `VSUSPEND` y `XSUSPEND` al habilitar y deshabilitar usuarios. (ID-16295)

Roles

- Cuando se importan roles que contienen vínculos recíprocos con súper roles existentes, Identity Manager actualiza 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.

Para actualizar roles fuera del proceso de actualización puede importar el archivo `RoleUpdater.xml` nuevo que se encuentra disponible en `sample/forms/RoleUpdater.xml`. De forma predeterminada, Identity Manager añade vínculos de subrol durante la actualización o cuando se importa el archivo `RoleUpdater.xml`.

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

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

Consulte la información relacionada con la actualización automática de roles durante la importación en ID-15053, en la página [“Problemas detectados”](#).

- El modelo de delegación ha cambiado como se indica: (ID-15440)
 - Cuando se modifica un usuario que ha delegado en uno o varios usuarios o se cambia una regla eliminada después de la delegación original, el usuario o la regla aparecen entre paréntesis, lo que indica que se ha eliminado. Por ejemplo: `“(auser)”`.
 - Si la delegación del usuario cambia pero la lista todavía incluye el delegado eliminado, se genera una excepción y no se guarda la información. Cuando no cambia pero se modifican otros atributos del usuario, los datos se guardan debido a que la información delegada no ha variado.
 - Si intenta crear o actualizar un usuario y el aprobador ha delegado en un usuario que no existe, no podrá realizar la operación y aparecerá un mensaje para avisar que no se ha podido delegar el elemento de trabajo de aprobación tal como estaba configurado debido a que el delegado se ha eliminado.
 - El usuario que delega puede recuperar los elementos de trabajo que se delegaron en un usuario que después se eliminó. El usuario que delega puede entonces poner fin a la situación de delegación en el usuario eliminado.

Para obtener más información, consulte *Sun Java(TM) System Identity Manager Administration*.

Seguridad

- Identity Manager permite definir configuraciones de delegación diferentes para distintos tipos de elementos de trabajo (como autenticaciones, remediaciones, aprobaciones y demás). (ID-14152)
- Identity Manager incorpora un nuevo grupo de objetos/organización denominada Usuario final. (ID-14630)

Este nuevo grupo de objetos/organización forma parte de la organización superior. Al principio carece de objetos de afiliados. Además, no aparece en la tabla del árbol correspondiente a la ficha de cuentas de la interfaz de usuario del administrador y no puede tener organizaciones secundarias. A pesar de esto, cuando se modifican objetos (como roles, roles de administración, recursos, directivas o tareas) se puede utilizar la interfaz de usuario del administrador para poner objetos en el grupo/organización de usuario final.

Antes, a los usuarios que accedían a la interfaz de usuario final se les asignaban derechos sobre los tipos de objetos especificados en EndUser (como AdminRole, EndUserConfig o EndUserTask). En la actualidad, Identity Manager también les asigna automáticamente el control del nuevo grupo de objetos de usuario final y evalúa la regla de organización controlada de usuario final. Cuando se devuelven nombres de organización, Identity Manager también concede automáticamente a dichos usuarios el control de esas organizaciones. Identity Manager utiliza la vista de autenticación de usuario como argumento de entrada a la regla de organización controlada de usuario final. La regla puede devolver una organización (como cadena) o varias organizaciones (como lista) en las que el usuario cuenta con la capacidad EndUser cuando accede a la interfaz de usuario final.

Asimismo, se ha añadido una nueva función de administrador de usuario final para administrar los nuevos objetos. Los usuarios que disfrutan de esta posibilidad pueden ver y modificar los derechos sobre los tipos de objetos especificados en EndUser, así como el contenido de la regla de organización controlada de usuario final. Esta capacidad se asigna de forma predeterminada al usuario Configurator. Los usuarios que han iniciado la sesión no pueden ver de forma dinámica los cambios que se producen en la lista o en las organizaciones que se devuelven al evaluar la regla de organización controlada de usuario final. Para ver los cambios tienen que cerrar la sesión y volver a iniciarla.

El uso de este nuevo grupo de objetos/organización es la mejor forma de proporcionar acceso a los objetos de configuración de Identity Manager, como roles, recursos, tareas y demás.

En adelante debería utilizar este método en lugar de End User Tasks, End User Resources, System Configuration:EndUserAccess y End User authTypes, aunque estos métodos sigan admitiéndose para garantizar la compatibilidad con versiones anteriores.

- Cuando se crea un usuario, se pueden añadir contraseñas al historial de contraseñas del mismo. (ID-15179)
- Cuando las listas de objetos (como roles o recursos) contienen más de seis grupos `memberObjectGroups` de cualquiera de los objetos devueltos, Identity Manager no elimina de los resultados los `memberObjectGroups` truncados. (ID-15181)

NOTA Este comportamiento no es aplicable al tipo `USER` debido a que sólo puede ser miembro de un único grupo de objetos.

- 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 delegado, 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 seguimiento se puede configurar para rastrear un método y de todas sus subllamadas (tanto directas como indirectas). Esto puede ser útil a la hora de solucionar problemas que se sabe que se producen en algún nivel por debajo de un método de entrada específico. (ID-13436)

Para habilitar esta función, defina el nivel de seguimiento correspondiente a 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.

- Se han añadido los métodos siguientes al objeto `WSUser`. Consulte el JavaDoc suministrado en el kit de referencia para obtener más información sobre esta clase. (ID-15468/14152)

Métodos de objeto WSUser

Método	Descripción
<code>getWorkItemDelegates()</code>	Devuelve la serie actual de objetos delegados correspondientes al usuario especificado.
<code>getWorkItemDelegate(String workItemType)</code>	El comando <code>_delegates</code> devuelve un objeto delegado perteneciente al tipo de elemento de trabajo solicitado.
<code>addWorkItemDelegate(Delegate delegate)</code>	Añade al comando <code>_workItemDelegates</code> un objeto delegado perteneciente al tipo de elemento de trabajo especificado. Si uno de los tipos de elemento de trabajo especificados ya existe, se sustituye.
<code>removeWorkItemDelegate(String workItemType)</code>	Elimina el tipo de elemento de trabajo especificado de los elementos de trabajo delegados.
<code>setWorkItemDelegates(Map workItemDelegates)</code>	Define la serie de elementos de trabajo delegados correspondiente a este usuario.
<code>getWorkItemDelegateHistory()</code>	Devuelve la lista especificada por el usuario con el historial de objetos delegados.
<code>setWorkItemDelegateHistory(List workItemDelegateHistory)</code>	Configura la lista del historial de objetos delegados específica del usuario.

Elementos de trabajo

- Cuando se remite un elemento de trabajo (`WorkItem`) de autenticación, cualquier comentario suministrado por el autenticador que lo ha remitido se incluye en el elemento. Por tanto, cuando éste finalmente se autentica, también se incluyen los comentarios de otros autenticadores. (ID-14643)

Problemas corregidos en esta versión

En esta sección se describen los problemas que se han corregido en Identity Manager 7.1. La información se ha organizado como sigue:

- [Interfaces de administrador y usuario](#)
- [Auditoría](#)
- [Entorno de desarrollo integrado \(IDE\)](#)
- [Metavista](#)
- [Sincronización de contraseña](#)
- [Reconciliación](#)
- [Informes](#)
- [Repositorio](#)
- [Recursos](#)
- [Seguridad](#)
- [Servidor](#)
- [Flujo de trabajo](#)
- [Otros problemas corregidos](#)

Interfaces de administrador y usuario

- En las páginas de depuración, los grupos de objetos ya no aparecen dentro de la lista desplegable de tipos de objetos que pueden eliminarse en masa. (ID-13324)
- Ahora es posible desbloquear los objetos de organización que se bloquean cuando un usuario sin los derechos adecuados intenta eliminarlos. (ID-14942)
- Las tareas personalizadas de usuario final que requieren retirar la vista del usuario que ha iniciado la sesión no generan un error que indica que la cuenta no está disponible debido a que se encuentra bloqueada. (ID-15040)
- Ahora es posible buscar roles con muchas organizaciones en la página Buscar roles sin que aparezca un error de grupo de objeto. (ID-15303)

- El menú Buscar roles > Autenticadores de la ficha Roles puede mostrar los usuarios capacitados como aprobadores de rol. (ID-15373)
- Cuando se utiliza un formulario `customEdit.jsp` como formulario de modificación personalizado, ya no se obtienen una página sin barra de navegación ni dos copias del formulario personalizado. (ID-15460)
- Si utiliza Internet Explorer 6 o 7 con actualización de seguridad 912812, no necesita hacer doble clic en un cuadro de selección múltiple para resaltarlo ni en un elemento para moverlo. (ID-15824)
- Cuando se especifica `true` para `IAPI.cancel` (que cancela todas las actualizaciones pendientes que se detecten para el usuario procesado) en el formulario de entrada de ActiveSync, la vista del usuario deja de estar bloqueado una vez procesado. (ID-15912)
- La edición de usuarios pertenecientes a una organización de nivel superior, resultante de una búsqueda en la lista de usuarios, funciona correctamente y no genera errores. (ID-15977)
- Las reglas predeterminadas que permiten realizar exploraciones de acceso son miembro de la organización de nivel superior de forma predeterminada. Si quiere permitir que los administradores editen la exploración de acceso o las políticas de auditoría sin controlar la organización de nivel superior, tendrá que añadir las reglas siguientes a las demás organizaciones. (ID-15996)
 - Review Everyone (Revisar todos)
 - Review Changed Users (Revisar usuarios cambiados)
 - Reject Changed Users (Rechazar usuarios cambiados)
 - Default Remediator (Remediador predeterminado)
 - Default Attestor (Autenticador predeterminado)
 - Default Escalation (Escalación predeterminada)
 - AttestorAll (Autenticador todo)
 - Non-Administrators (No administradores)
 - All Administrators (Todos los administradores)
 - Users Without a Manager (Usuarios sin administrador)

Auditoría

- La nueva directiva de auditoría de comparación de roles de IDM permite comprobar si los atributos de recursos de los usuarios coinciden con los atributos de roles definidos en sus roles asignados. Si no hay coincidencias, se genera una infracción de cumplimiento cuando se explora un usuario infractor aplicando esta nueva directiva. (ID-11225)
- Ya no aparece un error cuando se edita un informe de datos de la revisión de accesos en el que el destino especificado para la revisión se ha borrado. (ID-14805)
- En Identity Manager 7.1, el informe de auditor predeterminado para todas las infracciones de incumplimiento utiliza el atributo de presentación `resourceNames` con el fin de que queden reflejados varios recursos. Con anterioridad se empleaba el atributo `resourceName`, que generaba un mensaje de advertencia. (ID-15915)

Nota sobre la actualización: Este problema se resuelve solamente cuando se instala Identity Manager 7.1. Al actualizar Identity Manager, es preciso solucionar el problema de forma manual mediante la introducción de `resourceNames`, en lugar de `resourceName`, en la tarea de informe predeterminada (y cualquier otro informe configurado en función de la definición de la tarea Informe resumido de violaciones).

- La interfaz gráfica de usuario del asistente de políticas de auditoría permite especificar 3 remediadores y un periodo de escalación entre ellos. Si define el periodo, tiene que especificar el remediador. De lo contrario, el remediador se elimina. (ID-14198)
- Es posible realizar una exploración de auditoría ni una revisión de los accesos cuando el ámbito del usuario corresponde a una organización dinámica. (ID-14886)
- Los informes de los registros de auditoría presentan detalles relacionados con los cambios de rol. (ID-15587)
- Las funciones de cumplimiento de Identity Manager ofrecen tareas, directivas y reglas listas para usarse. (ID-16127) Identity Manager crea inicialmente estos objetos en los grupos de la organización superior o de todas, según corresponda. En las implementaciones donde se usa administración delegada con administradores que no controlan el grupo de objetos superior, puede interesar añadir algunos o todos los objetos de Auditor a otros grupos de objetos. Identity Manager ofrece una secuencia de comandos que crea una lista de objetos de grupo y los añade o elimina de los objetos de Auditor. (Encontrará la lista completa de objetos de Auditor en `$WSHOME/sample/scripts/AuditorObjects.txt`)
 - Para ver la lista de objetos:

```
cd $WSHOME/sample/scripts
beanshell.sh objectGroupUpdate.bsh -action list -data AuditorObjects.txt
```

- Para agregar el grupo de objetos “All” a todos los objetos:

```
cd $WSHOME/sample/scripts
beanshell.sh objectGroupUpdate.bsh -action add -data AuditorObjects.txt -groups
```

- Para eliminar el grupo de objetos “All” de todos los objetos:

```
cd $WSHOME/sample/scripts beanshell.sh objectGroupUpdate.bsh -action remove
-data AuditorObjects.txt -groups All
```

- El componente de auditoría de Identity Manager ofrece flujos de trabajo listos para usar con potencial de ejecución a largo plazo. (ID-16173) Para poder actualizar de 7.0 a 7.1, hay que renombrar todas las instancias de tarea suspendidas de estos flujos.

Identity Manager incluye una secuencia de comandos que puede ejecutar antes de actualizar a la versión 7.1 para realizar automáticamente dicha operación de cambio de nombre. Estas secuencias se hallan en el directorio `util_scripts` de la imagen de instalación. Para ejecutar las secuencias de comandos hay que activar el directorio donde se hallan y el servidor de Identity Manager debe estar ejecutándose. Especifique la opción `-h idm-url`, incluso aunque ejecute la secuencia localmente en el servidor de Identity Manager. Se necesita la sintaxis prevista de `idm-url`. Puede omitirla si el servidor de Identity Manager está vinculado a la ruta URL predeterminada. Esta secuencia de comandos cambia el repositorio de Identity Manager de manera que sólo haya que ejecutarlo en un servidor de Identity Manager.

- Para crear la lista de tareas que deben renombrarse

```
./beanshell.sh taskUpdate.bsh -u Configurator -p configurator -h idm-url
-action list
```

- Para realizar la operación de cambio de nombre

```
./beanshell.sh taskUpdate.bsh -u Configurator -p configurator -h idm-url
-action rename
```

Los objetos de definición de tarea renombrados adoptarán la forma `nombre-antiguo-7.1-update[N]`

- Al terminar o eliminar una revisión de acceso, puede detectarse errores que impidan la realización de las tareas. En tal caso, la revisión de acceso adoptará el estado `TERMINATE ERROR` o `DELETE ERROR`. Para ver información específica del error, consulte los resultados de las tareas en Tareas del sistema -> Todas las tareas (ID-16211)

Entorno de desarrollo integrado (IDE)

- La mayoría de los nodos tienen una hoja de propiedades asociada en las ventanas Propiedades, y la mayoría de estos nodos tienen una propiedad Nombre para gestionar el valor del nombre. Si cambia el nombre de un objeto concreto mediante su nodo, ya sea haciendo clic con el botón secundario del ratón y seleccionando Renombrar o haciendo clic en el nodo y escribiendo texto sobre la etiqueta, la etiqueta del nodo se actualiza y cambia la información XML. Sin embargo, la hoja de propiedades no se actualiza. Si hace clic en otro nodo y vuelve a hacer clic en el nodo cuyo nombre ha cambiado, la hoja de propiedades se actualiza y muestra el nuevo nombre. También puede hacer clic en el título de la hoja de propiedades para que se actualicen los valores. (ID-13696)
- Las bibliotecas de reglas no se admiten salvo para realizar operaciones de edición y comprobación básicas de código XML en el comprobador de reglas. No se ha implementado el uso de la navegación y las propiedades. (ID-14093)
- Las propiedades de los formularios no pueden configurarse con el editor de propiedades si el tipo de datos es entero o booleano. (ID-14128)

Solución: Edite el valor de la propiedad directamente en XML.

- La carga, descarga o recarga de un objeto provoca el bloqueo del objeto en el repositorio. Por tanto, el acceso fracasará si un usuario que no sea el especificado en la configuración del proyecto intenta acceder al objeto antes de que expire el periodo de bloqueo. (ID-14132)
- Cuando se cambia el nombre de un objeto desde el menú contextual en NetBeans, es necesario guardar el cambio. Una vez que se realiza el cambio, el usuario puede guardarlo con la opción Archivo>Guardar sin abrir el archivo. Si el archivo está abierto, utilice Archivo>Guardar o cierre el archivo y elija guardar los cambios cuando aparezca el mensaje correspondiente. (ID-14420)
- Al configurar la clase displayClass de un campo con el valor InlineAlert, la propiedad del valor de InlineAlert no se visualiza si el campo tiene nombre. (ID-14456)
- La retirada de una vista de usuario en Identity Manager IDE bloquea el objeto. El registro o cierre de la vista no libera el bloqueo. Éste se libera automáticamente transcurridos 5 minutos. También puede liberar el bloqueo entrando en Identity Manager como el administrador que retiró la vista en el ID de IDM y viendo la información del usuario. (ID-14797)
- Es posible especificar un contexto raíz dejando vacío el campo **Contexto** al crear el proyecto. (ID-15925)

Identity Manager SPE

- Ahora se puede terminar la tarea de sincronización de SPE antes de procesar todas las actualizaciones. (ID-15077)
- También se puede configurar SPE para utilizar un directorio de usuario final habilitado para SSL. (ID-15773)
- La página de configuración de Identity Manager SPE ya no permite configurar directivas de cuentas que no pertenecen a SPE. (ID-14833)

Metavista

- El atributo `idmManager` se almacena correctamente en el atributo de usuario cuando se utiliza la metavista. (ID-14445)

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)
- Las contraseñas interceptadas con caracteres fuera del rango ASCII de 7 bits ahora se codifican 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)
- El uso de la opción `checkDynamicallyAssignedAdminRolesAtLoginTo` ya no causa errores del editor de directivas de reconciliación cuando se actualiza el programa de reconciliación. (ID-15338)

Informes

- Se admite el registro de auditoría para la creación, modificación y eliminación de roles de administración. (ID-12514)
- Los informes de usuario presentan el ID de todas las cuentas de recursos en una lista separada por punto y coma. En la lista también se incluyen las cuentas y los recursos que se asignan de forma indirecta a través de un rol o un grupo de recursos. Cuando sólo hay una cuenta de recursos, el ID de la cuenta únicamente se muestra si no coincide con el ID de la cuenta de Identity Manager. (ID-12820)
- Los cambios efectuados en las preguntas de autenticación de un usuario se registran en los registros de auditoría. (ID-13082)
- El **registro de violaciones de cumplimiento de los usuarios** no debería aparecer en el menú Informes del selector Informes de auditor. Se trata de la tarea **Default Compliance Audit Report** y debería permanecer oculta. (ID-14721)
- Si ha personalizado el formulario de datos de infracción de conflictos en una versión anterior, debería exportar el formulario antes de actualizar a la versión 7.0. Si lo prefiere, puede reimportar el formulario guardado después de la actualización. (ID-14772)
- 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)

Repositorio

- La opción `ObjectSource.OP_ALLOW_NOT_FOUND` (`allowNotFound`) está perfectamente representada en las llamadas a `getView` y `checkoutView` de `IDMXUserView`, y en las llamadas a `getObject` a través de `LighthouseContext` en Identity Manager. (ID-11900)
- El repositorio de Identity Manager cierra (para) una conexión de base de datos activa cuando se produce un error de Java (es decir, una instancia de `java.lang.Error`). En la versión anterior, el repositorio cerraba la conexión activa cuando se producía una excepción declarada o runtime (no un error). Este cambio evita dejar transacciones abiertas (sin confirmar) cuando Java Virtual Machine genera un error (como `OutOfMemoryError`). (ID-14411)
- La opción `-n` del comando `setRepo` impide correctamente que se compruebe la ubicación del repositorio actual. La opción `-n` permite que el comando `setRepo` tenga éxito cuando la ubicación del repositorio actual no es válida (o no está disponible la instancia de la base de datos en la ubicación actual). Con ello se resuelve una regresión introducida en Identity Manager 2005Q4M3 (Identity Manager 6.0). (ID-14809)

- El proceso de inicialización del repositorio de Identity Manager es más rápido debido a que RelationalDataStore genera una sentencia SQL que se ejecuta con más rapidez en tablas de bases de datos de mayor tamaño. (ID-14937)
- Los sistemas de base de datos lentos de Oracle ya no pueden provocar la ejecución de tareas suspendidas en más de un programador a la vez. (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

- Se ha incorporado el campo de parámetro de recursos **Servidores de conexión por fallo** para el adaptador de recursos LDAP. Este campo permite al usuario listar diversos servidores de conexión por fallo si falla el servidor preferido. El adaptador de recursos LDAP utiliza JNDI para mantener la conexión con el directorio de LDAP. Por tanto, JNDI intenta automáticamente la conexión con cada servidor por orden hasta que encuentra una. Una vez hallada una conexión, JNDI sigue usando ese servidor hasta que falla, en cuyo caso se repite el proceso. La repetición en todos los servidores de conexión por fallo es responsabilidad del cliente. (ID-10889)
- 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 adaptador de recursos de NDS permite fusionar grupos contenidos en la plantilla NDS con grupos no definidos en dicha plantilla. Esta acción se realiza en la interfaz de usuario con cambios en el formulario de usuario. Para obtener información detallada, consulte NDSUserForm.xml. (ID-12083)
- Los adaptadores Linux ahora pueden devolver un año con el último inicio de sesión. (ID-12182)

- Para poder usar una vista de otro usuario de Oracle, hay que establecer un alias con el fin de poder referirse a la vista sin asignarle un nombre de usuario. Identity Manager no lo detectaba y permitía especificar dicha vista en el adaptador de recursos. Identity Manager ahora detecta el error y emite un mensaje. (ID-12643)
- Cuando se ven usuarios en un recurso NIS de Solaris, la configuración del grupo principal aparece como nombre del grupo. (ID-12667)
- Las contraseñas se pueden configurar ahora como no caducadas al utilizar el modo CUA en un recurso de SAP. (ID-13355)
- El adaptador de recursos de VMS ahora tiene capacidades de reconciliación. (ID-13425)
- El aprovisionamiento reconoce la captura de un error de una secuencia de comandos `ResourceAction` durante las funciones de ejecución y actualización de usuario. (ID-13465)
- Identity Manager proporciona un parámetro de configuración de recursos denominado `enableEmptyString`. Este parámetro permite escribir cadenas vacías en lugar de valores nulos (NULL) en columnas basadas en caracteres definidas como no nulas en el esquema de tablas. El parámetro `enableEmptyString` no afecta a la manera en que se escriben las cadenas para tablas basadas en Oracle. (ID-13737)

El valor predeterminado de este parámetro es OFF o FALSE (comportamiento existente). Para escribir una cadena vacía, cambie el valor del parámetro a ON o TRUE.

- La actualización de una responsabilidad de una cuenta de Oracle ERP utilizando el adaptador de Oracle ERP ya no hace que se actualicen otras responsabilidades asociadas a la cuenta. (ID-13889)

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.

- 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. Ahora, el último valor modificado se calcula en función de la marca de tiempo `lastModifiedTimestamp` de los atributos de un usuario que se han definido en el esquema de Identity Manager. 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 envía a este usuario al servidor como modificado. (ID-13896)
- El adaptador de secuencias de comandos de shell admite ahora las funciones de cambio de nombre, de inhabilitación y de habilitación. (ID-14472)
- 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. Las conexiones aumentan al máximo y se abren conexiones que permanecen en el estado `CLOSED_WAIT`. Una vez que se alcanza el número máximo de conexiones y que todas se encuentran en el estado `CLOSED_WAIT`, Active Sync se detiene hasta que estas conexiones se limpian. (ID-14597)

- La asignación de atributos que el adaptador envía a la secuencia de comandos de actualización del cliente contiene una entrada para el atributo null-ed; el valor de la entrada de asignación será nulo. Esta condición (valor vacío en la asignación de atributo) indica que el atributo se está eliminando. (ID-14655)
- 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)
- 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)
- El adaptador de recursos LDAP vuelve a utilizar el control de VLV al listar y buscar cuentas de usuario si el servidor LDAP admite dicho control y el servidor está configurado correctamente. (ID-14526)
- El formulario de usuario de Oracle ERP incluye un campo Person Name. Este campo es de sólo lectura y muestra el nombre completo del usuario cuando una cuenta de Oracle ERP está vinculada al sistema Oracle HR mediante el número de empleado. (ID-14675)
- El adaptador de SAP informa ahora correctamente del estado de las cuentas inhabilitadas. (ID-14834)
- El método abreviado de activación nsaccountlock puede utilizar la lógica basada en la existencia o ausencia de valor al determinar si un usuario de LDAP está inhabilitado. (ID-14925)
- 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)
- 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)
- 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)
- 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)

- 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)
- El adaptador de recursos de ADSI cierra las conexiones cuando se consultan objetos de recurso. (ID-15098)
- Ahora se pueden especificar propiedades de conexión de ACF2 (como pantalla virtual más ancha y profunda). (ID-15158) Para implementar esta función debe importar su propia secuencia de comandos update.xml, que ha de contener:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <ImportCommand class='com.waveset.session.ResourceUpdater' >
    <Map>
      <MapEntry key='updateAttributes' value='true'/>
    </Map>
  </ImportCommand>
</Waveset>
```

Una vez ejecutado el adaptador, hay que detener y reiniciar el servidor de aplicación.

Para aumentar el tamaño de pantalla a un tipo de terminal de modelo 5, hay que agregar las siguientes propiedades:

```
Enable TN3270E: 1
Session Properties: SESSION_PS_SIZE <nueva línea> 5
```

Tenga presente que la <nueva línea> indica que SESSION_PS_SIZE y el parámetro 5 van en dos líneas distintas.

- Hay un nuevo atributo de recurso del esquema de Oracle ERP: person_fullname. La secuencia de comandos de ejemplo \$WSHOME/sample/other/CreateLHERPAdminUser.oracle se ha actualizado para incluir una tabla ICX* y para permitir la visualización de los sinónimos creados para usuarios que no usan APPS. (ID-15188)
- Las secuencias de comandos de ejemplo de JDBC no cerraban ResultSets y Statements cuando ya no eran necesarios. En una aplicación grande, ello puede provocar fugas de recursos. Se han modificado las secuencias de comandos para cerrar dichos objetos cuando ya no sean necesarios. (ID-15254)
- Identity Manager ahora intercepta y genera informes con las secuencias de comandos de eliminación que devuelven error abiertamente. (ID-15340)

- Se ha resuelto un problema de asignación de almacenamiento relacionado con la conversión de caracteres. (ID-15341)

Es preciso utilizar UTF-8 de manera uniforme en la puerta de enlace, así como configurar la puerta de enlace de Windows con una página de código ANSI predeterminada que sea compatible con los datos de la aplicación. Es decir, hay que utilizar una codificación de caracteres en Windows con la que se puedan representar todos los caracteres Unicode de los datos que se gestionan con Identity Manager.

- Con el fin de que no repitan al cabo del tiempo, se han cambiado los nombres de archivo temporales que se usan al ejecutar secuencias de comandos de shell para acciones de recursos. (ID-15348)
- Identity Manager ya no añade el destino `net.id` 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 error de software que hacía fallar la generación de ID de grupo o usuario NIS de Solaris al partir de un entorno sin usuarios o grupos, y los archivos de `passwd` y `group` de plantilla se hallan en directorios distintos 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 Solaris con NIS, para configurar el grupo principal predeterminado se utiliza `defgname` del archivo `/usr/sadm/defadduser`, en lugar de `defgroup`, como origen alternativo de los valores predeterminados de las cuentas recién creadas. (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)
- 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)
- El adaptador de interfaz de componente de PeopleSoft puede informar de los estados inhabilitados (ID-15674)
- Identity Manager ya no lee atributos de cuenta de sólo escritura del directorio de LDAP ni de Active Directory. (ID-15838)

- El adaptador de recursos de pasarela con secuencia de comandos ahora puede capturar correctamente los códigos de secuencia de comandos que devuelven valores distintos de cero e informar del error. (ID-15860)
- Al borrar un atributo de RACF en un formulario, Identity Manager no borraba el atributo para el usuario al enviar el formulario; ahora Identity Manager borra el atributo. (ID-15971)
- El atributo del recurso de plantilla NDS ahora muestra la ayuda emergente (i-Help) en lugar de la clave de mensaje NDS_TEMPLATE_HELP. (ID-15986)
- El adaptador de recursos de pasarela con secuencia de comandos ahora admite las acciones de recurso Habilitar y Deshabilitar. (ID-16066)
- El adaptador de recursos de pasarela con secuencia de comandos ahora pasa los atributos de recursos a las secuencias de comandos implementando las acciones getInfo y listAllObjects. (ID-16149)
- Se ha desaprobado el adaptador de recursos de GroupWise. Para gestionar usuarios de GroupWise debe utilizarse el adaptador NDS. (ID-16308)

Programador

- Se ha suprimido la salida de la entrada de syslog “EVNT00”, error LockedByAnother, ya que generaba una salida excesiva en sysLog dentro de entornos de clúster. (ID-15714)

Seguridad

- Los cambios de contraseña de usuario final iniciados por administradores (a través de SPML u otros medios) se añaden al historial de contraseñas cuando es posible. Esta corrección introduce una opción de configuración del sistema y otra de vista (formulario) que permiten al administrador cambiar al comportamiento deseado. (ID-13029)
 - Los administradores pueden alternar las opciones de configuración del sistema basándose en la aplicación de inicio de sesión. Esto proporciona una mayor flexibilidad, puesto que los administradores pueden no desear un comportamiento que afecte a todas las aplicaciones.
 - La opción de vista sustituirá siempre a los valores de configuración del sistema.
- Los administradores delegados que sólo posean capacidad de administrador no podrán eliminar de un informe las organizaciones fuera de ámbito (sobre las que se informa). (ID-14765)
- En el registro de auditoría de una organización se incluyen los aprobadores que se añaden a la organización o se eliminan de ésta. (ID-15232)

- Los administrador de roles de administración ahora gozan de bastantes privilegios para crear un rol de Admin. Cuando se crea un rol de administración o una capacidad nuevos, es posible que haya que seleccionar uno o varios usuarios que puedan asignar el rol o la capacidad a otros usuarios. Esta situación se produce cuando un creador no tiene autorización para asignar roles de administración o capacidades. La serie de usuarios entre los que puede elegir el creador no depende del ámbito de autorización de Identity Manager, ya que es posible que el creador necesite elegir los usuarios fuera de su ámbito de control. Los usuarios disponibles tienen garantizado el derecho "Assign Capability" (ID-15980)

Servidor

- El servidor de SPML devuelve ahora errores para solicitudes que contienen filtros que utilizan operadores no implementados aún. (ID-11343)
- Cuando se abandonaban atributos del objeto de configuración de atributos extendidos no se abandonaban también de los atributos de WSUser, sino que el XML conservaba los valores antiguos. Esto se ha corregido y ahora los valores se suprimen del XML. (ID-11721)
- Cuando se especifican comandos o usuarios para operaciones en masa mediante la GUI, la operación ya no genera un fallo "An object name must be specified" aunque se especifique un nombre de usuario. (ID-15112)
- Se han solucionado los problemas que causan errores del tipo OutOfMemory cuando los procesos acceden a un recurso de forma intensiva (como la reconciliación). (ID-16222)
- Para devolver una lista específica de elementos de trabajo de delegados, Identity Manager ahora ofrece los nuevos métodos públicos siguientes, que toman el argumento *workItemType*. (ID-15787/14152)

```
DelegateUtil#checkWorkItemDelegates()
```

```
DelegateUtil#getWorkItemDelegates()
```

Tareas

Cuando edite una tarea programada, tendrá que introducir otra vez la fecha de inicio en formato MM/DD/AAAA (ID-5675).

Flujo de trabajo

- La definición de la tarea de notificación de finalización de reconciliaciones de Identity Manager se completa y luego se envía una notificación por correo electrónico (ID-9259).

Otros problemas corregidos

8691, 8961, 9913, 10100, 10802, 11538, 12509, 12571, 12585, 12872, 13223, 13251, 13258, 13701, 13741, 13965, 14282, 14334, 14459, 14564, 14663, 14748, 14893, 15036, 15098, 15234, 15345, 15424, 15746, 15798, 15851, 15864, 16041, 16087, 16121, 16171, 16177, 16215, 16288,

Problemas detectados

En esta sección de las Notas de la versión de Identity Manager 7.1 se enumeran los problemas detectados y se ofrecen soluciones:

- [Identity Manager](#)
- [Service Provider Edition](#)

Identity Manager

En esta sección se describen los problemas detectados en Identity Manager y las soluciones a estos problemas. La información está organizada de la siguiente manera:

- [General](#)
- [Instalación y actualización](#)
- [Administración de cuentas](#)
- [Aprobaciones](#)
- [Auditoría](#)
- [Entorno de desarrollo integrado \(IDE\)](#)
- [Configuración de inicio de sesión](#)
- [Organizaciones](#)
- [Directivas y capacidades](#)
- [Reconciliación e importación de usuarios](#)
- [Informes](#)
- [Recursos](#)
- [Administración de objetos de recurso](#)
- [Grupos de recursos](#)
- [Seguridad](#)
- [Servidores](#)
- [Puerta de enlace de Sun Identity Manager](#)
- [Tareas](#)
- [Flujo de trabajo, formularios, reglas y XPRESS](#)

General

- Los campos necesarios definidos en el mapa del esquema de recursos sólo se comprueban cuando se crea una cuenta de usuario (ID-220). Cuando se vaya a necesitar un campo en las actualizaciones de usuario, el formulario de usuario tendrá que configurarse de manera que se requiera el campo.
- No se comprueba la existencia de caracteres no válidos en el nombre de organización, el nombre de administrador, el nombre de cuenta, el nombre de atributo de usuario (a la izquierda del mapa del esquema) o los nombres de tareas (ID-1145, 1206, 1679, 1734, 1767, 2413, 3331). El nombre de estos tipos de objetos no puede incluir los siguientes caracteres: símbolo de dólar (\$), coma (,), punto (.), apóstrofo ('), Y comercial (&), corchete izquierdo (⌈), corchete derecho (⌋) o dos puntos (:).
- En la página de cuentas aparece un mensaje de error engañoso si intenta realizar una acción una vez que la sesión ha terminado (ID-1223).
- El objeto de calendario no puede verse entero si el explorador utiliza fuentes de gran tamaño. (ID-2120)
- La casilla de verificación Select All de las páginas Find Results y List Task no se deselecciona si se anula la selección de uno de los elementos de la lista (ID-5090). La casilla de verificación selectAll no se tiene en cuenta en la acción resultante si no se han marcado las casillas de todos componentes de la lista.
- Si realiza un cambio en un catálogo de mensajes personalizados, tendrá que reiniciar el servidor para ver los cambios. (ID-6792)
- El mecanismo de detección actual de fallo del servidor asume que todos los sistemas de un clúster de Identity Manager están sincronizados en el tiempo. (ID-7064) Cuando se aplica el intervalo de error predeterminado de cinco minutos y un servidor presenta un desfase de sincronización de cinco minutos con otro, el servidor adelantado declara que el servidor atrasado está inactivo, lo que produce resultados inesperados.

Solución: Mejore la sincronización temporal o aumente el intervalo de reconexión de emergencia.

- Si inicia una sesión en Windows con un nombre de usuario que contiene caracteres de dos bytes y la codificación predeterminada del equipo sólo admite caracteres de un byte, debe configurar la variable de entorno USER_JPI_PROFILE en un directorio existente cuyo nombre sólo contenga caracteres de un byte. (ID-8540)
- Si un nodo expandido contiene menos de una página de datos y se inserta un nuevo nodo dependiente del otro (por ejemplo, cuando se crea un usuario de la organización) *delante* del primer registro de la página, Identity Manager introducirá una página con un elemento delante de la página actual cuando se actualice. (ID-12151)

Solución: Para *realinear* las páginas, haga clic en el botón First Page.

- 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 existente 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 suele afectar a roles creados fuera de Identity Manager que hacen referencia a roles (subroles o súper roles) existentes del 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 en “Roles” en la página 30.

- Es preciso actualizar a JDK 1.4.2_13 la versión que utiliza el servidor de aplicaciones para que se aplique la nueva hora de verano (DST) a partir de 2007. (ID-15475)

Para actualizarlo, realice este procedimiento:

- a. Actualice las funciones de tiempo del servidor de puerta de enlace desde

<http://www.microsoft.com/windows/timezone/dst2007.msp>

(Identity Manager obtiene del sistema operativo Windows las funciones de tiempo del servidor de puerta de enlace.)

- b. Instale una versión actualizada de Java que sea compatible en el servidor de aplicaciones.
Identity Manager Installation ofrece instrucciones para apagar, actualizar y volver a iniciar el servidor de aplicaciones.
- c. Revise la lista de tareas programadas para iniciarse durante el nuevo horario de verano ampliado (consulte la información relacionada con los efectos de estos periodos de tiempo a continuación).

Después de corregir la hora de verano es preciso volver a programar los elementos cuyo inicio debe producirse conforme a esta base de tiempo. Los elementos recurrentes que se ejecuten al menos una vez después de corregir la hora de verano y después del inicio de estos periodos de tiempo se ejecutarán en el momento previsto.

Consulte la información relacionada con la hora de verano en las actualizaciones de Java o utilice la herramienta `tzupdater` (<http://java.sun.com/developer/technicalArticles/Intl/USDST/>). Consulte también Alerta Sun para Java.

En Estados Unidos y Canadá ha cambiado la aplicación del horario de verano, de manera que ahora empieza antes y termina después que en años anteriores. El horario de verano empieza entre el segundo domingo de marzo y el primer domingo de abril y termina entre el último domingo de octubre y el primer domingo de noviembre. Para 2007 se ha previsto que su aplicación entre el 11 de marzo o el 1 de abril y el 28 de octubre o el 4 de noviembre. Los problemas ocasionados por el uso de software incompatible seguirán ocurriendo hasta que se utilice software compatible.

NOTA Si no se realiza el procedimiento anterior puede ocurrir lo siguiente:

- Algunas de las tareas programas (incluidas la reconciliación y Active Sync) pueden ejecutarse una hora antes o después de lo previsto, dependiendo de los parámetros de planificación.
 - Se puede incluir o excluir de los informes los eventos ocurridos una hora antes o después del intervalo de tiempo especificado.
 - Las modificaciones personalizadas que dependen de la fecha pueden generar resultados incorrectos.
-

- El menú de la interfaz de usuario final que permite remitir un elemento aprobado a otro aprobador de la lista de elementos de trabajo no presenta el contenido correcto. (ID-15935)

Solución: Inserte en el formulario el campo siguiente después del campo `userIds`, sustituyendo las cadenas "user*" por la lista adecuada de los ID de cuenta:

```
<Field name='forwardingUsers'>
  <Derivation>
    <list>
      <s>user1</s>
      <s>user2</s>
    </list>
  </Derivation>
</Field>
```

- Si modifica la configuración de un registro de cambios (por ejemplo, añadiendo atributos de columna), quizá no aparezcan esas modificaciones en un archivo CSV de registro de cambios que ya exista. (ID-15973)
- Las cadenas que aparecen en las fichas del componente de visualización `TabPanel` (usadas, por ejemplo, en el formulario de usuario con fichas) se ajustan si tienen espacios. Para alterar este comportamiento de modo que las cadenas no se ajusten, hay que añadir las dos líneas siguientes a `$/WSHOME/styles/customStyle.css`:

```
table.Tab2TblNew td
{background-image:url(../images/tabs/level2_deselect.jpg);background-repeat:repeat-x;b
ackground-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);backgroun
d-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}
```

- En sesiones de Identity Manager localizadas, las miniaplicaciones de diagrama de proceso pueden estar parcialmente localizadas (mezcla de inglés y el idioma seleccionado). (ID-16139)
- Al editar un rol, si se incluye un segundo rol como súper rol y subrol, se creará una referencia circular que probablemente producirá un error de desbordamiento de pila (StackOverflowError). (ID-16326)
- Para sincronizar contraseñas en modo directo hay que configurar SimpleRpcHandler en el archivo web.xml. De manera predeterminada, este gestor no se suministra como tal al servelt rpcrouter2. (ID-16469) Para usar sincronización de contraseñas en modo directo, defina como sigue el parámetro de inicialización del gestor:

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

Recuerde que se ha constatado que SimpleRpcHandler interfiere con determinadas llamadas de RemoteSession. Si prevé utilizar tanto RemoteSession como sincronización de contraseñas en modo directo, configure aparte un servlet para gestionar las llamadas de RemoteSession.

Instalación y actualización

NOTA Para obtener información sobre los problemas exclusivos esta versión, consulte [“Notas de instalación y actualización” en la página 73.](#)

- Cuando se actualiza la versión 6.x y se quiere empezar a utilizar las nuevas páginas de usuario final, es preciso cambiar manualmente la configuración del sistema `ui.web.user.showMenu` a `true` para que aparezca la barra de navegación horizontal. (ID-14900, 16401)

También es preciso cambiar a mano la asignación de formulario de usuario final de la configuración del sistema para que quede así:

```
<Attribute name='endUserMenu' value='End User Dashboard' />
```

- WebLogic 9.0 es incompatible porque un error de compilación afecta a varias páginas.

Solución: Utilice WebLogic 9.1 o 9.2. (ID-16002)

- No hay ninguna secuencia de comandos de actualización de la base de datos para el almacén de transacciones de Service Provider. Al actualizar desde Identity Manager 5.6 (Service Provider Edition 1.0) o Identity Manager 6.0 a 7.0 o 7.1, hay que añadir una columna nueva (“userId”) a la tabla existente. En esta versión, los ejemplos de secuencias de comandos de base de datos (create_spe_tables.*) muestran el tipo esperado y la longitud de valor máximo predeterminado de esta columna. (ID-16423)
- Al actualizar, en raros casos puede aparecer el error siguiente cuando se intenta ejecutar update.xml:

```
com.waveset.util.InternalError: Reserved item
```

```
'ComplianceViolation:LastModified' name is already in use by existing item
```

```
'ComplianceViolation:LastModified'.
```

Si esto sucede, elimine el elemento problemático del repositorio así en SQL:

```
delete from object where type='ComplianceViolation' and name='LASTMODIFIED'
```

Tras ello puede reanudar la actualización en el punto en que falló sin más que volver a importar update.xml. (ID-16437)

Administración de cuentas

- Es posible crear cuentas NT cuyo nombre tenga más de 20 caracteres y que las herramientas nativas de NT no puedan administrar (ID-710).
- El administrador no puede guardar recursos ni funciones que contengan organizaciones que él no administre (ID-839).
- Si ordena las columnas en la página de resultados de provisión, se añaden filas vacías adicionales a los resultados (ID-1105).
- La aprobación de varios cientos de cuentas de usuario requiere una cantidad de tiempo considerable (ID-1149).

Solución: Apruebe registros de cuentas de usuario en grupos más pequeños.

- No se pueden aprobar registros de aprobaciones de un administrador que ya no dispone de capacidad de aprobación (ID-1150).

Solución: Quite el administrador de los recursos, las funciones y las organizaciones en los que dispone de derechos de aprobación y, a continuación, apruebe los registros de aprobaciones importantes antes de quitar el administrador o su capacidad de aprobación.

- Cuando se actualiza un usuario sin realizar ninguna modificación no se muestra la página de resultados detallados (ID-2327).
- Cuando se crea un usuario nuevo o se añade un recurso a un usuario existente, si el nombre distinguido del usuario es incorrecto, el valor incorrecto se guarda en caché hasta que el administrador cierra la sesión (ID-2508). Los intentos de volver a crear el usuario una vez que se ha corregido el nombre distinguido no producen resultados hasta después de que el administrador haya cerrado la sesión.
- Windows Active Directory exige que la puerta de enlace actúe como un administrador que puede crear directorios (ID-2919). Identity Manager puede crear directorios iniciales en sistemas Windows 2000. El usuario que sirve de puerta de enlace es el que crea la cuenta del directorio inicial, y no el administrador especificado en la definición del recurso.

Solución: Pase al usuario que sirve de puerta de enlace del sistema local a una cuenta que disponga de permiso para crear recursos remotos compartidos, y configure permisos para utilizar esos recursos. Esta cuenta también necesitará los privilegios Bypass traverse checking (omitir comprobación de recorrido) y Act as operating system (actuar como sistema operativo).

- El recurso de Windows NT envía de forma incorrecta un mensaje de advertencia, en lugar de un mensaje de error, cuando se deshabilita una cuenta de usuario (ID-3222).
- Cuando se eliminan todos los recursos de un usuario mediante la página de edición de usuarios puede aparecer un mensaje java.lang.NullPointerException (ID-4811).

Solución: Utilice la página de eliminación de usuario para desenlazar o eliminar las cuentas de recursos del usuario.

- Si se crea un usuario de Identity Manager y se asigna a un recurso de Windows Active Directory donde ya existe la cuenta de usuario, el usuario no dispondrá del atributo GUID en la información del recurso (ID-5114). El atributo GUID sirve para detectar si ha cambiado la organización o el nombre del usuario en el directorio. La ejecución de la reconciliación desde el recurso puede solucionar este problema.
- Al crear un usuario se muestra una advertencia si se añade una función al usuario que contiene un recurso asignado directamente (ID-5385).
- No se puede especificar un administrador "Forward To" cuando se está creando un usuario. Esta opción sólo se puede configurar cuando se edita el usuario (ID-5695).

Aprobaciones

- Cuando se actualiza un usuario y se elige realizar la actualización en segundo plano, la actividad de aprobación aparece en la página de resultados de tareas (ID-3301). Esta aprobación se puede ignorar.
- Los registros de aprobaciones de un administrador no se muestran después de cambiar el nombre del usuario (ID-3386).

Solución: Resuelva las aprobaciones importantes antes de cambiar el nombre de usuario.

- Un administrador no puede ver los registros de aprobaciones autorizados o rechazados anteriormente si el usuario sometido a aprobación pertenece a una organización que el aprobador no controla (ID-3494).
- El recurso vuelve a intentar que las tareas aparezcan en la lista de aprobaciones pendientes del usuario Configurator (ID-3508).

Auditoría

- Durante una exploración no se admiten reintentos de exploración de cuentas de usuario que no se han podido capturar de los recursos o donde han ocurrido otros fallos. Estos fallos se notifican cuando la exploración termina, pero no existe ningún modo de explorar otra vez las cuentas forma automática. (ID-9112)
- Identity Auditor intenta hacer que los usuarios no infrinjan el cumplimiento entre exploraciones de directiva mediante la aplicación obligatoria de la directiva siempre que se edita el usuario. Si edita un usuario que tiene asignadas directivas de auditoría y además incumple una directiva, no podrá guardar los cambios, aunque se trate de un cambio tan simple como trasladar a un usuario a otra organización. (ID-9504)

Solución: Utilice la función de la miniaplicación de usuario que permite mover con un clic en el botón secundario del ratón (o la de búsqueda y desplazamiento) o deshabilite temporalmente las comprobaciones de la directiva de auditoría.

Para deshabilitar las comprobaciones de la directiva de auditoría, edite la configuración del sistema y elimine la propiedad `userViewValidators`. Esta propiedad, que tiene como valor una lista de cadenas, se añade durante la importación del archivo `init.xml` o `upgrade.xml`.

- En los historiales de infracciones de directivas de auditoría, recurso y organización, la implementación de una escala logarítmica para un tipo de gráfico STACK puede hacer que la presentación funcione de forma inusual. (ID-9522)

- En la actualidad, el administrador de informes de exploración de acceso de Auditor no puede programar la exploración de las directivas de auditoría. Se genera el error `Error message: Create access denied to Subject auditadmin on type TaskSchedule`. Para programar cualquier tarea, los administradores deben contar con privilegios `create` sobre `TaskSchedule` `authType`. (ID-14713)

Solución: Modifique el administrador para asignarle privilegios `create` sobre `TaskSchedule` o especifique un usuario que tenga las capacidades `Auditor Administrator` o `Wave set Adminsistrator` como mínimo.

- Los informes de exploración de las directivas de auditoría que haya creado en versiones anteriores de Identity Auditor no podrán verse cuando actualice a Identity Manager 7.0. Para solventar este inconveniente, cualquier administrador que ejerza de `Administrador de informes de Auditor` (o tenga otra capacidad superior) podrá editar estos informes y cambiar la visibilidad a **run**. (ID-14881)
- Cuando se realizan exploraciones de auditoría que dan lugar a varias infracciones, el Auditor puede crear un flujo de trabajo de remediación para gestionar el proceso de las infracciones. La configuración predeterminada de MySQL para `max_allowed_packet` (1M) es demasiado limitada para un flujo de trabajo con docenas de infracciones. Cuando se alcanza el límite, el Auditor no inicia el flujo de trabajo de remediación.

Solución: Este valor debe ser más alto cuando se utiliza con frecuencia el auditor. Para solucionar el problema, añada `max_allowed_packet = 32M` al archivo de configuración de MySQL (`my.cnf`) y reinicie el servidor de la base de datos. (ID-15830)

- Los nombres de directiva de auditoría no pueden contener los siguientes caracteres: ' (apóstrofo), . (punto), | (línea), [(corchete izquierdo),] (corchete derecho), , (coma), : (dos puntos), \$ (símbolo del dólar), " (comillas) y = (signo igual). (ID-16078)
- Puede resultar confuso cambiar los valores de gravedad y prioridad para las remediaciones de infracción de cumplimiento. Los valores iniciales del formulario *no son* los valores actuales de las infracciones de cumplimiento, sino los últimos valores definidos al realizar un cambio. Es importante saber qué valor de gravedad/prioridad interesa mientras aún está visible la vista de lista, ya que no es posible determinar los valores actuales en la página donde se pueden cambiar. (ID-16040)
- Las infracciones de cumplimiento producidas antes de actualizar a IdM 7.1 no permiten definir la gravedad ni la prioridad. El mensaje de error resultante indica que la infracción de cumplimiento ya no existe, pero esta afirmación es incorrecta. La infracción está ahí, pero IdM no es capaz de definir su gravedad o prioridad. (ID-16420)

Entorno de desarrollo integrado (IDE)

- Para cambiar el nombre de los objetos utilizando el Identity Manager IDE se debe usar el menú contextual del botón secundario del ratón en el explorador de proyectos, en lugar de editar en XML. (ID-13828)
- En el IDE de IDM se ha deshabilitado el navegador XML. Ventanas: >Se abre el panel del navegador y aparece <No view available>. (ID-13390)
- No se admite la función de eliminación de proyectos. (ID-14013)
- Cuando se cierra un proyecto, la opción Discard All no funciona correctamente. Para descartar los cambios efectuados en un objeto es preciso cerrar la ventana del editor y seleccionar Discard. Se trata de un problema relacionado con NetBeans (error 84236). (ID-14164)
- Cuando trabaje con un proyectos estándar de Identity Manager IDE, inicie la instancia de Tomcat incorporada para que se abra el cuadro de diálogo de Tomcat Manager. Normalmente se indica una de las condiciones siguientes: (ID-15546)
 - Se están ejecutando varias instancias de Tomcat.
 - Las credenciales no coinciden.

Se trata de un problema conocido de NetBeans.

Solución: Asegúrese de que hay una única instancia de Tomcat en ejecución en el host y que está configurada para conectarse al mismo puerto que la incorporada.

Las credenciales almacenadas como parte del servidor Tomcat incorporado deben coincidir con las almacenadas en los campos de nombre de usuario y contraseña del administrador de servidores. Para obtener más información sobre los valores de estos campos, consulte el siguiente sitio Web:

<http://wiki.netbeans.org/wiki/view/FaqInstallationDefaultTomcatPassword>

Para comprobar el número de puerto de la instancia de Tomcat incorporada y las credenciales almacenadas:

- a. Seleccione la ficha Runtime del Identity Manager IDE y abra los nodos de servidores e instancias de Tomcat incorporadas.
 - b. Haga clic con el botón secundario del ratón en el nodo de la instancia de Tomcat incorporada y seleccione Properties en el menú emergente.
 - c. Compruebe los valores incluidos en los campos Server Port, Username y Password en el cuadro de diálogo del administrador de servidores (Server Manager) que se abre.
- La clonación de documentos no funciona. (ID-15725)

- Si realiza una comparación (diff) en un documento pero no guarda los cambios, dicha acción no mostrará ningún resultado. En la actualidad no hay mensajes que adviertan de esta situación. El Identity Manager IDE sólo puede efectuar una acción de comparación (diff) con el contenido del archivo, pero no con el contenido de la ventana del editor. (ID-15952)
- Si realiza una comparación (diff) en un directorio que contiene archivos no guardados, no aparecerá ningún resultado en la ventana de resultados de la comparación. (ID-15955)
- Cuando se utiliza el generador de expresiones para crear una sentencia de invocación, se abre un ventana con el Javadoc correspondiente al método elegido. De momento no es posible usar las barras de desplazamiento para recorrer el documento. Esto significa que con algunos métodos la ventana no muestra el Javadoc completo. (ID-16093)

Soluciones:

- Una vez seleccionado un método, el Javadoc se transfiere temporalmente al final de la ventana de expresiones. Ahí puede recorrer todo el documento, pero sólo se trata de una copia temporal que no se restaurará si hace clic en otro elemento de la expresión o en otra expresión distinta.
- Utilice el Javadoc normal suministrado en el directorio *Image/REF/javadoc* del soporte de instalación.
- Se lanzará una excepción de puntero nulo cuando compruebe la validación en la vista de diseño. (ID-16168)

Solución: Realice la validación desde el XML (vista de origen).

Configuración de inicio de sesión

- El módulo de autenticación intermedia no funciona con el recurso de Domino (ID-1646).
- Los demás administradores que hayan iniciado una sesión no podrán ver los cambios efectuados en las páginas de configuración de inicio de sesión de administrador y de usuario (ID-3487). Para ver los cambios, esos administradores tendrán que cerrar la sesión de la interfaz del administrador y volver a iniciarla.
- Si un administrador inicia una sesión y selecciona “Cambiar mi contraseña” seguido de otra ficha, su cuenta se bloquea hasta que el intervalo de bloqueo termina. (ID-3705)

Cuando otro administrador intenta editar el administrador bloqueado, se muestra el siguiente mensaje:

```
com.waveset.util.WavesetException: Unable to access account #ID#Configurator at this time. Please try again later.
```

Si el administrador hace clic en el botón “Aceptar”, se muestra el diagrama del proceso de flujo de trabajo correspondiente a la última acción.

Organizaciones

- Cuando se eliminan varias organizaciones y falla la eliminación de una, las restantes tampoco se borran (ID-517).
- Si se cambia el nombre de una organización mientras hay pendientes solicitudes de provisión que afectan a usuarios de la organización, la solicitud falla (ID-564).

Solución: Asegúrese de que no hay solicitudes importantes antes de cambiar el nombre de la organización.

- Cuando se crea una organización nueva y se selecciona la opción User Member Rules antes de especificar un nombre de organización, en el campo de nombre de la organización aparece un ID al actualizar la página (ID-6302). El nombre se puede configurar antes de guardar la nueva organización.

() - Warning: Parenthesized values in field 'Approvers' do not match any of the allowed values.

Directivas y capacidades

- El atributo de directiva de cuenta Opción de notificación de reinicialización de Identity Manager tiene una opción “administrador” que no se aplica (ID-944). Las únicas opciones viables son “inmediata” y “usuario”.
- Cuando se eliminan varias funciones, la operación se detiene en lugar de continuar eliminando otras funciones si se detecta un error (ID-1168).
- El número mínimo de preguntas que un usuario debe responder se puede configurar en un valor mayor que el número de preguntas definidas (ID-1834). En este caso, el usuario no podrá iniciar una sesión utilizando la opción “Olvidó mi contraseña”.
- La directiva de cuenta de Lighthouse predeterminada no se puede clonar editando la directiva, cambiando el nombre y seleccionando crear un objeto nuevo (ID-5147).

Solución: Cree una directiva de cuenta nueva.

Reconciliación e importación de usuarios

- Al importar usuarios de un archivo CSV, los atributos del recurso no se actualizan si el usuario ya existe en Identity Manager (ID-2041).
- Los apóstrofes (') que presenta en los ID de cuenta el archivo en formato de valores separados por comas (CSV) que se ha cargado se transforman en signos de interrogación (?) (ID-2100).

- Las tareas programadas no aparecen al realizar una búsqueda en la página “Buscar tareas” cuando se utiliza la opción “Is Scheduled” (ID-5001).
- La reconciliación no se completa si se ejecuta en un recurso de la versión 8 de Red Hat (ID-6087).
- La reconciliación de un recurso de Oracle ERP termina con errores si la agrupación de conexiones del recurso está habilitada (ID-6386). Si quiere solucionar el problema, deshabilite la agrupación de conexiones durante la reconciliación.

Informes

- Los administradores de seguridad no pueden ejecutar ni crear informes (ID-1217).
Solución: Asigne funciones de administrador de informes a los administradores.
- Otros administradores, además de los administradores de informes, pueden ver los informes de análisis de riesgos (ID-1224).
- Los resultados de los informes que se envían por correo electrónico con la opción de texto normal no tienen formato (ID-2191).
Solución: Utilice la opción HTML para el correo electrónico.
- Las entradas del registro de auditoría pueden no registrarse si el volumen de resultados es grande (ID-5050).
- El panel no aparecerá aunque se seleccione si hay organizaciones en las que el nombre contiene apóstrofes (') (ID-5653).
- Si intenta ejecutar un informe de administrador y elige informar sólo a administradores que pertenecen a una organización específica, aparece un error java.lang.NullPointerException (ID-5722).

Recursos

- El botón de prueba de recursos no sirve para probar todos los campos (ID-51).
- Las asignaciones de puertos de recursos se pueden configurar en valores superiores a 65535 (ID-59).
- Cuando se configura un nombre de grupo de Active Directory incorrecto se muestra un mensaje de error (ID-393). Si intenta configurar el nombre del grupo de Active Directory en “groupname” en lugar de en “cn=groupname,cn=builtin,dc=waveset,dc=com”, aparece el mensaje de error “array index out of bounds”.

- A veces no se tienen en cuenta los atributos de cuenta necesarios si hay otro recurso con el mismo nombre de atributo de cuenta que no tiene configurado el indicador necesario (ID-1161).
- Si un administrador intenta añadir una organización a un recurso para el cual no dispone de derechos, aparece un error. Será preciso cancelar la edición del recurso y editar de nuevo el recurso para realizar otros cambios (ID-1274).
- El mensaje de error que aparece cuando una contraseña o un nombre de usuario de cuenta de recurso no es correcto en un recurso de PeopleSoft no es claro (ID-2235). El mensaje de error es el siguiente:

```
bea.jolt.ApplicationException: TPESVCFAIL - application level service failure
```

- Las acciones de recursos de Windows Active Directory que utilizan el estado de salida `%DISPLAY_INFO_CODE%` causan fallos con errores (ID-2827).
- Las acciones de recursos de Windows NT que devuelven un código de salida distinto de cero no causan fallos (ID-2828).
- No es posible configurar un ID de grupo principal de usuario en Active Directory cuando se crea el usuario (ID-3221).

Solución: Cree el usuario sin configurar el ID de grupo principal, y luego edite el usuario y configure el valor. El ID de grupo principal no lo establece el nombre distinguido (DN) del grupo, sino el número.

- Las direcciones IP de los recursos se almacenan en caché en JVM una vez que el nombre de host hace referencia a una dirección IP. Cuando se cambia la dirección IP de un recurso, es preciso reiniciar el servidor de aplicaciones para que Identity Manager detecte el cambio (ID-3635). Esto aparece configurado en Sun JDK (versión 1.3 o posterior) y se puede controlar con la propiedad `sun.net.inetaddr.ttl`, que normalmente se configura en `jre/lib/security/java.security`.
- En los recursos de Oracle no se pueden crear varias cuentas para un solo usuario (ID-3832).
- Los usuarios finales no pueden utilizar la función de autodescubrimiento en cuentas de recursos de Domino (ID-4775).
- Si se pasa un usuario desde o hasta un subcontenedor dentro de la organización de Active Directory, el adaptador de Active Sync detecta el cambio; sin embargo, cuando se visualiza el usuario en la página de edición (o se efectúa un cambio y se visualiza la página de confirmación), el ID de la cuenta del usuario sigue siendo el DN (nombre distinguido) original (ID-4950). La utilización de GUID para modificar el usuario no causa problemas de funcionamiento. La ejecución de la reconciliación contra el recurso puede solucionar este problema.

- Si el usuario se pasa de una organización (OU) a una suborganización, el adaptador del registro de cambios de LDAP no reconoce el cambio y asume que el usuario se ha eliminado. El objeto de usuario se bloquea en Identity Manager (si es la configuración actual) y no se crea una cuenta nueva para la que se ha movido (ID-4953).
- Las conexiones agrupadas que utilizan los adaptadores de recursos de UNIX se pueden dejar en un estado indeterminado si ocurre un error durante la ejecución de un comando o una secuencia de comandos (ID-5406).
- Sólo es posible crear organizaciones NDS en el nivel superior del árbol configurando el contexto de base del recurso en “[ROOT]” (ID-5509).
- Si en NDS edita un campo (como Grace Login Limit) de la provisión inicial y no introduce valores en los campos booleanos, todos los campos booleanos se configuran como falsos (ID-6770). Esto impide configurar otros campos de la ficha de restricción que requieren que los valores de ciertas casillas de verificación sean verdaderos. Para evitar esto, asegúrese de que todos los campos booleanos que necesite sean verdaderos para que se transmitan correctamente al editar otros campos.
- Si cambia la contraseña de un equipo UNIX mediante la función Manage Connection --> Change Resource Password, el nombre de tarea que aparece es:

```
_FM_PASSWORD_CHANGING_TASK null:null
```

Debería aparecer un nombre fácil. (ID-6947)

- No se puede utilizar la función de administración de conexión en recursos de UNIX que utilizan NIS (ID-6948). Esto genera un error debido a que la contraseña que se está intentando cambiar pertenece a la cuenta raíz, pero NIS no administra la cuenta raíz.
- Cuando se actualicen usuarios mediante una actualización desde una organización de Identity Manager, los usuarios que tengan un ID de cuenta de servidor Sun One recibirán un error si se crearon de forma nativa y se cargaron en Identity Manager (ID-7094). La solución consiste en actualizar los usuarios por separado.
- Identity Manager sigue incluyendo las clases desaprobadas que siguen:
 - com.waveset.object.IAPI
 - com.waveset.object.IAPIProcess
 - com.waveset.object.IAPIUser

Las clases de adaptador personalizado no deberían hacer referencia a estas clases, sino a las clases correspondientes del paquete com.waveset.adapter.iapi. (ID-8246)

- Se produce un error cuando se intenta eliminar un usuario que tiene una cuenta en el recurso de interfaz de componente de PeopleSoft. En la actualidad, este recurso no admite la eliminación de cuentas. (ID-9000)

- Si sale del asistente Nuevo objeto de recurso sin hacer clic en el botón **Guardar** o **Cancelar**, el formulario desechado quizá no se destruya e interfiera cuando después al crear objetos de recurso nuevos. (ID-11033) Esto produce un error que indica

No resource form id found in options or view.

Solución: Utilice siempre el botón Cancelar para salir del asistente Nuevo objeto de recurso.

- Los espacios de tablas temporales no respetan las configuraciones de cuota y, en caso de intento desde Oracle 10gR2, se produce una excepción de SQL. (ID-12843)

Hasta ahora, el adaptador de recursos definía una cuota en un espacio de tablas temporal, incluso aunque no estuviese asignado el atributo `oracleTempTSQuota`. Este comportamiento ha cambiado. Si asigna el atributo `oracleTempTSQuota`, se conserva el comportamiento anterior (no cambia), pero si suprime la asignación, no se define ninguna cuota en el espacio de tablas temporal.

Solución: En el caso de las instalaciones de Oracle 10gR2, elimine el atributo `oracleTempTSQuota` del adaptador de recursos.

- Se han detectado dos problemas en el editor de plantillas de integración de Remedy. (ID-14729)
 - El valor predeterminado de esquema de Remedy, "HPD:HelpDesk", no es adecuado para las últimas versiones de BMC Remedy, que no contienen ningún esquema "HPE:Help Desk".
 - La columna Opciones no aparece para algunos campos. Ello no afecta a la capacidad de usar plantillas de Remedy.
- Cuando determinados visores de la aplicación de consola 1 de NDS inspeccionan a los usuarios de NDS/Groupwise creados por Identity Manager que tienen los campos Access y AccountID (por ejemplo, al seleccionar primero las propiedades de usuario y después la ficha Groupwise) puede parecer que no se guardan sus valores correspondientes.

Sin embargo, los campos aparecen si se utiliza el visor de usuario de Groupwise Diagnostic -> Display Object. Este error de visor no parece afectar a las actualizaciones que Identity Manager realiza en los campos antes mencionados. (ID-16330)

- La regla IS_DELETE (usada para configurar el adaptador Active Sync de PeopleSoft) no aparece en el menú de reglas conocidas. (ID-16398)

Solución: Edite el archivo `$WSHOME/sample/rules/PeopleSoftRules.xml` y cambie al texto indicado a continuación. Después, vuelva a importar el archivo mediante Configuración->Importar archivo de intercambio.


```

<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <Rule name='IS_DELETE'>
    <Description>Should the active sync event delete the user?</Description>
    <O bien>
      <eq><ref>activeSync.Status</ref><s>T</s></eq>
      <eq><ref>activeSync.Status</ref><s>L</s></eq>
    </or>
  </Rule>
</Waveset>

```

- El adaptador Oracle ERP borra los valores anteriores de las responsabilidades al cargar un solo usuario. La descripción de responsabilidad del usuario y los valores start_date y end_date actuales no adoptan el formato correcto en el formulario con getUser(). En consecuencia, los datos de responsabilidad podrían resultar dañados. (ID-16414)

Solución: Edite el campo includeResponsibilities del formulario de usuario de ejemplo OracleERPUserForm.xml para incluir un valor predeterminado. Después, vuelva a importar el archivo mediante Configuración->Importar archivo de intercambio.

```

<Field name='includeResponsibilities'>
  <Display class='Checkbox' action='true'>
    <Property name='title' value='Add Direct Responsibilities' />
  </Display>
  <Default>
    <cond>
      <gt>
        <length>
          <ref>global.responsibilities</ref>
        </length>
        <i>0</i>
      </gt>
      <s>true</s>
    </cond>
  </Default>
  <Disable>
    <not>
      <ref>global.showOracleERPFields</ref>
    </not>
  </Disable>
</Field>

```

— O BIEN —

Seleccione el botón **Cargar** en la página de atributos para volver a cargar el usuario.

Administración de objetos de recurso

- No es posible cambiar el nombre de un objeto de Windows Active Directory (grupo, unidad organizativa o contenedor) en la página de lista de recursos (ID-3329).
- No se pueden crear grupos LDAP nuevos si hay usuarios que tienen CN con varios valores (ID-3848).

Solución: Utilice el valor DN, en lugar de CN, para administrar los miembros del grupo. Este valor se configura en el formulario de creación de grupo de LDAP.

Grupos de recursos

- Con la tecla de retorno de la página de creación o edición de grupos de recursos se borran los cambios efectuados en la página (ID-3430).
- Los informes de grupos de recursos no se pueden guardar en un archivo CSV. (ID-8001)

Seguridad

- Identity Manager ya no emite una excepción `java.lang.StackOverflowError` cuando se producen las siguientes condiciones: (ID-15035)

a. Hay definida al menos una organización dinámica (afiliados basados en reglas) en Identity Manager

b. El formulario de usuario incluye un <Campo> que llama a `getObject` en `Type.USER`

El error `StackOverflowError` se debe a un bucle infinito que resulta de evaluar el permiso de expansión.

Este problema se ha resuelto agregando dos nuevas opciones booleanas de vista de usuario:

- `NoFormDerivation` (valor predeterminado `true`)
- `NoFormExpansion` (valor predeterminado `true`)

Estas opciones siempre se pasan cuando se solicita la transferencia de una vista de usuario a una regla. Si estas opciones se definen en `true`, se impide la derivación y expansión del formulario.

NOTA Cuando estas opciones se definen en `true` y dentro de la regla se necesita derivación o expansión de campos de formulario, hay que incluirlas dentro de la lógica de la regla.

Consulte “Setting View Options in Forms” en *Identity Manager Workflows, Forms, and Views* para obtener más información sobre la configuración de opciones de vista.

Servidores

- Los usuarios de Identity Manager 4.x deben verificar que el servidor principal no utiliza una zona horaria ambigua. Por ejemplo, EST se puede utilizar en Australia o Estados Unidos. Sin embargo, GMT+10 o GMT-6 son ambiguos. (ID-8297)
 - La clase `com.waveset.rpm.SimpleRpcHandler` se ha desaprobadado en la versión 7.1 (ID-14756)
1. Añada la siguiente definición de servlet al descriptor de implementación:

```
<servlet>
  <servlet-name>rpcrouter3</servlet-name>
  <display-name>OpenSPML SOAP Router</display-name>
  <description>no description</description>
  <servlet-class>
    org.openspml.server.SOAPRouter
  </servlet-class>

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

  <init-param>
    <param-name>spmlHandler</param-name>
    <param-value>com.waveset.rpc.SpmlHandler</param-value>
  </init-param>

  <init-param>
    <param-name>rpcHandler</param-name>
    <param-value>com.waveset.rpc.RemoteSessionHandler</param-value>
  </init-param>
</servlet>
```

2. Añada la siguiente asignación de servlet al descriptor de implementación:

```
<servlet-mapping>
  <servlet-name>rpcrouter3</servlet-name>
  <url-pattern>/servlet/rpcrouter3</url-pattern>
</servlet-mapping>
```

Para utilizar `createView` con `RemoteSession`, necesita usar el servlet `rpcrouter3`. Para acceder a `rpcrouter3`, tiene que utilizar el constructor `RemoteSession` (`URL`, `String`, `EncryptedData`).

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

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

Se ha probado el funcionamiento de Microsoft SQLServer 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 SQLServer 2000.

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

```
ALTER DATABASE dbname SET READ_COMMITTED_SNAPSHOT ON
```

</quote>

- Si implementa Identity Manager en Sun Application Server y transfiere la opción `--precompile`, la precompilación de JSP falla, porque Identity Manager utiliza fragmentos de JSP, pero no los nombra como `.jspf`. (ID-16373)

Solución: Renombre estos archivos con la extensión `.jspf`.

Sun Application Server 8.2 y 9.0 ahora ofrecen una opción para ignorar los errores de precompilación debidos a fragmentos de `.jsp`. Para obtener más información, consulte

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6393940

Puerta de enlace de Sun Identity Manager

- La Puerta de enlace de Sun Identity Manager a veces no se detiene cuando se pulsa el botón Stop en la pantalla NT Services. (ID-590)

Solución: Cancele la solicitud del servicio (si todavía está bloqueado) y detenga de nuevo del servicio, o salga del cuadro de diálogo NT services, vuelva a entrar e intente realizar la operación de parada otra vez.

- No se pueden añadir usuarios a grupos de un dominio NT si la puerta de enlace se encuentra en un dominio de confianza remoto (ID-711).
- En ocasiones la puerta de enlace no se detiene cuando se utiliza "net stop "Puerta de enlace de Sun Identity Manager"" (ID-2337).

Tareas

- Los administradores con privilegios de administrador de Identity Manager no pueden visualizar la página de administración de tareas si la lista de tareas contiene un análisis de riesgos (ID-1225).
- Los administradores que no disponen de control de nivel superior no pueden crear tareas programadas Discovery o ResourceScanner (ID-1414).
- La página de búsqueda de tareas no muestra el número de tareas que satisfacen los criterios de búsqueda (ID-5152).
- Los administradores delegados que no disponen de control de nivel superior pueden programar tareas y ver los resultados, pero no pueden visualizar la tarea una vez creada (ID-6659). La tarea programada se ha incluido en el nivel superior y el administrador delegado no tiene los derechos adecuados para visualizar el objeto.
- Se ha añadido un campo denominado Deferred Tasks a la biblioteca. Este campo ofrece una lista de tareas aplazadas de un usuario. Para implementar este campo, es preciso añadir la línea siguiente al formulario de usuario con fichas y al formulario de vista de usuario con fichas (ID-7660).

```
<FieldRef name='Deferred Tasks' />
```

Fujo de trabajo, formularios, reglas y XPRESS

- Puede utilizar la función XPRESS `<eq>` para comparar valores booleanos con las cadenas TRUE or FALSE o con los enteros 1 o 2 (ID-3904).

Solución: Utilice lo siguiente:

```
<cond>
  <isTrue><ref>Boolean_variable</ref></isTrue>
  <s>True action</s>
  <s>False action</s>
</cond>
```

- Las expresiones de ruta no funcionan cuando se repite una lista de objetos genéricos mediante dolist (ID-4920).

```
<dolist name='genericObj'>
  <ref>listOfGenericObjects</ref>
  <ref>genericObj.name</ref>
</dolist>
```

Solución: Utilice `<get>` / `<set>` como se indica:

```
<dolist name='genericObj'>
  <ref>listOfGenericObjects</ref>
  <get><ref>genericObject</ref><s>name</s>
</dolist>
```

- Si utiliza variables `global.attrname` para los campos del formulario de usuario y varios recursos comparten el mismo atributo, también debería definir una regla de derivación (ID-5074). De lo contrario, cuando se efectúe un cambio nativo en el atributo en uno de los recursos, cabrá la posibilidad de que el atributo se capte y propague, o no, a otros recursos.
- No se pueden utilizar cadenas especiales que empiezan con `&` en los componentes HTML de los formularios. Por ejemplo, ` `; ya no aparece como un espacio. Este problema surgió debido a un cambio relacionado con los caracteres especiales (`&\<>`) admitidos en las listas de selección (ID-5548).
- Los comentarios relacionados con formularios, flujo de trabajo y reglas que aparecen en las fichas `<Comment>` llevan cadenas `
` que representan el carácter de avance de línea (ID-6243). Estos caracteres sólo pueden verse en la versión XML de estos objetos; el servidor de Identity Manager y el editor de procesos de negocio procesan estos caracteres correctamente.
- Si utiliza las plantillas eliminadas con acciones globales, anularán el comportamiento de acción global sin avisar. (ID-10320)
- Si utiliza el formulario de tabla de recursos de usuario para editar usuarios, al editar un recurso de usuario no se obtendrán los atributos del recurso la primera vez que aparezca el formulario.

Solución: Haga clic en el botón Actualizar para que se capturen los datos del atributo. (ID-10551)

Service Provider Edition

En esta sección se describen los problemas detectados en Identity Manager SPE y las soluciones a estos problemas.

- Identity Manager SPE y Sun Java System Portal Server pueden ser incompatibles debido a un problema relacionado con las bibliotecas cifradas. (ID-10744)

Este problema se puede solucionar configurando los valores siguientes en el archivo `/etc/opt/SUNWam/config/AMConfig.properties` de Portal Server y reiniciando el contenedor Web:

```
com.ipanet.security.encryptor=com.ipanet.services.util.JCEEncryption
com.ipanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.
    JSSESocketFactory
com.ipanet.security.SecureRandomFactoryImpl=com.ipanet.am.util.
    SecureRandomFactoryImpl
```

- Cuando se trabaja con paneles de control SPE: si un gráfico tarda varios minutos en cargarse por primera vez, deber verificar que el explorador no se ha configurado para utilizar Microsoft Java Virtual Machine (MSJVM). Identity Manager SPE no permite utilizar MSJVM para ejecutar miniaplicaciones de explorador. (ID-10837)
 - 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 recurso: regla de exclusión de cuentas, aprobadores y organizaciones asociados con el recurso.
 - Atributos de función
 - De forma predeterminada, la auditoría no se realiza cuando se utilizan las llamadas `checkinObject` y `deleteObject` `IDMXContext` de API. La auditoría se debe solicitar de forma explícita configurando la clave `IDMXContext.OP_AUDIT` como verdadero en la asignación de opciones transferida a estos métodos. El método `createAndLinkUser()` de la clase `ApiUsage` muestra cómo solicitar la auditoría. (ID-11261)
 - Los cambios de nombre de gráfico del panel de control no funcionan bien. Aunque el nombre nuevo aparece al editar el gráfico, éste no se referencia con dicho nombre en ninguna otra página. (ID-11690)
 - El grupo de módulos de inicio de sesión predeterminado asume que el nombre asignado al recurso de Service Provider es "Directorio de usuarios SPE". La página de inicio de sesión de usuario de Service Provider no funciona correctamente cuando se usa otro nombre. La página no mostrará los campos relacionados con el inicio de sesión. (ID-14891)
- Solución:** Actualice el objeto `UI_LOGIN_MOD_GRP_DEFAULT_SPE_PWD LoginModGroup` con el nombre de recurso correcto.
- La tarea de sincronización de SPE está programada, de modo que la sincronización no se detiene al detener dicha tarea en la página Tareas. Para lograrlo puede deshabilitar la programación en sí. (ID-16000)

Solución: El método preferible para iniciarla y detenerla es utilizar la interfaz del producto en la página Recurso o programar (por ejemplo, desde un flujo de trabajo) los métodos `SessionUtil` para que inicien y detengan la sincronización de SPE. Para impedir que la sincronización de SPE empiece automáticamente cada vez que se inicie una instancia del servidor de Identity Manager, hay que deshabilitarla en la directiva de sincronización para el recurso. Al detener la sincronización de SPE con la interfaz de usuario o con el método `SessionUtil`, sólo se detiene la sincronización hasta que se inicia otra instancia del servidor de Identity Manager.

- Cuando se utiliza la página de inicio de sesión de usuario final de Identity Manager SPE en WebSphere y aparece un error 404 en el explorador, se genera una excepción `javax.servlet.UnavailableException`. (ID-16001)

Solución: Utilice las propiedades siguientes en IBM 1.5 JDK:

- a. En el directorio `was-install/java/jre/lib`, cambie `jaxb.properties.sample` a `jax.properties` y quite los comentarios de estas dos líneas:

```
javax.xml.parsers.SAXParserFactory=  
    org.apache.xerces.jaxp.SAXParserFactoryImpl  
javax.xml.parsers.DocumentBuilderFactory=  
    org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
```

- b. Guarde el archivo y reinicie el servidor de aplicaciones.

Notas de instalación y actualización

En esta sección se proporciona información relacionada con la instalación y la actualización. La información se ha organizado como sigue:

- [Notas de instalación](#)
- [Notas de actualización](#)

Con la mayoría de las versiones principales de Identity Manager se produce un cambio de esquema. Antes de actualizar a una nueva versión de Identity Manager es preciso actualizar el esquema. Para cambiar a Identity Manager 7.1, ejecute una de las secuencias de comandos de actualización de esquema siguientes, según la versión que tenga instalada. (ID-15392 y ID-15722)

- Desde Identity Manager 6.0, ejecute la secuencia de comandos `upgradeto71from60` adecuada.
- Desde Identity Manager 7.0, ejecute la secuencia de comandos `upgradeto71from70` adecuada.

NOTAS

- Cuando actualice Identity Manager, asegúrese de revisar la sección de instalación correspondiente a su servidor de aplicaciones en el documento *Sun Java(TM) System Identity Manager Installation*.
 - Para obtener información detallada e instrucciones de actualización, consulte *Sun Java(TM) System Identity Manager Upgrade*.
 - Si la instalación actual 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.
-

Notas de instalación

La información siguiente se refiere al proceso de instalación del producto:

- Debe instalar Identity Manager de forma manual en HP-UX.
- La utilidad de instalación de Identity Manager ahora puede realizar la instalación o actualización con cualquier nombre de directorio de instalación. Es preciso crear ese directorio antes de iniciar el proceso de instalación o seleccionar la creación del directorio desde el panel de configuración.
- Para ejecutar la Puerta de enlace de Sun Identity Manager en Windows NT es preciso instalar la extensión de cliente de Microsoft Active Directory (DSClient), que está disponible en:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358>

NOTA Consulte las instrucciones detalladas de instalación del producto en *Sun Java(TM) System Identity Manager Installation*.

- En Unix/Linux existen dos requisitos de instalación adicionales (ID-8403):
 - Para 5.0 - 5.0 SP1:
 - El directorio `/var/tmp` existe.
 - El usuario que realiza la instalación puede escribir en el directorio `/var/tmp`.
 - Para 5.0 SP2 y posterior:
 - El directorio `/var/opt/sun/install` existe.
 - El usuario que realiza la instalación puede escribir en el directorio `/var/opt/sun/install`.

Notas de actualización

Esta sección contiene un resumen de las tareas que es preciso realizar para actualizar Identity Manager de la versión 6.0 o 7.0 a la versión 7.1. (Consulte [“Itinerarios de actualización de Identity Manager” en la página 13](#) para obtener información sobre las versiones que pueden actualizarse a Identity Manager 7.1.)

La información se ha organizado como sigue:

- [Cuestiones relativas a la actualización](#)
- [Uso del programa de actualización de Identity Manager](#)
- [Actualización manual](#)

Cuestiones relativas a la actualización

- Tras la actualización, `changedFileList` y `notRestoredFileLists` incluirán los archivos que aparecen abajo. Estos archivos no deberían mostrarse, pero no es necesario realizar ninguna acción. (ID9228)

`bin/winnt/nspr4.dll`

`bin/winnt/jdic.dll`

```

bin/winnt/MozEmbed.exe
bin/winnt/IeEmbed.exe
bin/winnt/AceApi.dll
bin/winnt/DominoAPIWrapper.dll
bin/winnt/DotNetWrapper.dll
bin/winnt/gateway.exe
bin/winnt/lhpwic.dll
bin/winnt/msems.inf
bin/winnt/pwicsvc.exe
bin/winnt/remedy.dll
bin/solaris/libjdic.so
bin/solaris/mozembed-solaris-gtk2
bin/linux/librfccm.so
bin/linux/libsapjcorfc.so
bin/linux/libjdic.so
bin/linux/mozembed-linux-gtk2

```

- Cuando se actualiza de la versión 6.x a la versión 7.0 o 7.1 y se quiere empezar a utilizar las nuevas páginas de usuario final de Identity Manager, es preciso cambiar manualmente la configuración del sistema `ui.web.user.showMenu` a verdadero para que aparezca la barra de navegación horizontal. (ID-14901)

Asimismo, si quiere que el nuevo panel de control de usuario final aparezca en la página inicial del usuario final, debe cambiar a mano la asignación de formulario de usuario final para el tipo de formulario “endUserMenu”. Acceda a Configurar -> Asignaciones de formularios y procesos -> y, en el tipo de formulario “endUserMenu”, cambie Nombre de formulario asignado a “Panel de control de usuario final”.

También debe actualizar la asignación del tipo de formulario “endUserWorkItemListExt”. Cambie Nombre de formulario asignado a “End User Approvals List”.

- Si actualiza la versión 6.0 o 7.0 a la versión 7.1 y está utilizando `LocalFiles`, tiene que exportar todos los datos antes de la actualización para luego importarlos de nuevo una vez que se instala correctamente la versión 7.1. (ID-15366)
- Cuando se actualiza a Identity Manager 7.1, el archivo `WEB-INF/speConfiguration.xml` no se elimina durante el proceso. Como la función Service Provider deja de usar este archivo, puede eliminarse sin problema. Algo parecido ocurre con la propiedad `spe.enableServer`, que puede seguir apareciendo en el archivo `Waveset.properties`. En Identity Manager 7.0 y 7.1 no se utiliza esta propiedad. (ID-15765)

Uso del programa de actualización de Identity Manager

En esta sección se describen los pasos necesarios para actualizar Identity Manager con el programa de instalación y actualización de Identity Manager.

-
- NOTAS**
- Con la mayoría de las versiones principales de Identity Manager se produce un cambio de esquema. Antes de actualizar a una nueva versión de Identity Manager es preciso actualizar el esquema. Para cambiar a Identity Manager 7.1, ejecute una de las secuencias de comandos de actualización de esquema siguientes, según la versión que tenga instalada. (ID-15722)
 - Desde Identity Manager 6.0, ejecute la secuencia de comandos `upgradeto71from60` adecuada.
 - Desde Identity Manager 7.0, ejecute la secuencia de comandos `upgradeto71from70` adecuada.

Para obtener más información, consulte *Sun Java(TM) System Identity Manager Upgrade*.
 - En algunos entornos, incluido HP-UX, puede que necesite o prefiera seguir los procedimientos de actualización manual alternativos. Si es así, pase directamente a la sección [“Actualización manual” en la página 79](#).
 - En entornos UNIX, asegúrese de que existe el directorio `install` en las ubicaciones siguientes, y de que puede escribir en él:
 - **Para Linux/HP-UX:** `/var/opt/sun/install`
 - **Para Solaris:** `/var/sadm/install`
 - Durante la actualización, necesitará conocer la ubicación en la que se encuentra instalado su servidor de aplicaciones.
 - Cualquier parche instalado con anterioridad se archivará en el directorio siguiente:
`$WSHOME/patches/HotfixName`
 - 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 va a cambiar a Identity Manager 6.0 o Identity Manager 7.0, debe actualizar el esquema de la base de datos del repositorio de la manera siguiente:
 - **Identity Manager 6.0** introduce un cambio de esquema que proporciona la tabla de syslog y nuevas tablas para tareas, grupos y organizaciones. Debe crear estas nuevas estructuras de tablas y trasladar a ellas los datos existentes.
 - Identity Manager 6.0 almacena los objetos de usuario en dos tablas. Puede utilizar las secuencias de comandos de ejemplo proporcionadas en el directorio `db_scripts` para hacer cambios en el esquema. Consulte la secuencia de comandos `db_scripts/upgradeto2005Q4M3.DatabaseName` para actualizar las tablas del repositorio.

NOTAS

- Antes de actualizar el esquema del repositorio, haga una copia de seguridad completa de las tablas que contiene.
 - La actualización de las bases de datos de MySQL tiene que ver bastante con este proceso. Consulte `db_scripts/upgradeto2005Q4M3.mysql` para obtener más información.
-

- **Identity Manager 7.0** introduce nuevas tablas para derechos de los usuarios. Debe crear estas nuevas estructuras de tablas y trasladar a ellas los datos existentes. Puede utilizar las secuencias de comandos de ejemplo proporcionadas en el directorio `db_scripts` para hacer cambios en el esquema.

NOTAS

- Antes de actualizar el esquema del repositorio, haga una copia de seguridad completa de las tablas que contiene.
 - Consulte la secuencia de comandos `db_scripts/upgrade7.0.DBMSName` para obtener más información.
-

3. Si está ejecutando la Puerta de enlace de Sun Identity Manager en el servidor de Identity Manager, utilice el siguiente comando para detener el servicio de la puerta de enlace:

```
net stop "Puerta de enlace de Sun Identity Manager"
```

4. Utilice uno de estos métodos para iniciar el programa de instalación:
 - Para usar el programa de instalación con la interfaz gráfica, ejecute el archivo `install.bat` (para Windows) o `install` (para UNIX).

El instalador muestra el panel de bienvenida.

- Para activar el instalador en modo `nodisplay`, cambie al directorio en el que se encuentra situado el software e introduzca el siguiente comando:

```
install -nodisplay
```

El instalador presenta el texto de bienvenida y luego una lista de preguntas para obtener la información de instalación en el mismo orden que la versión gráfica.

-
- | | |
|--------------|--|
| NOTAS | <ul style="list-style-type: none">• Si no hay ninguna pantalla presente, el instalador utiliza la opción <code>nodisplay</code> de forma predeterminada.• El programa no instala versiones antiguas del software sobre versiones nuevas. Si intenta hacerlo, aparece un mensaje de error y el instalador se cierra. |
|--------------|--|
-

5. En el panel de bienvenida, haga clic en el botón Siguiente.
6. En el panel Install or Upgrade?, seleccione Upgrade (actualizar) y haga clic en Siguiente.
7. En el panel Select Installation Directory (seleccionar el directorio de instalación), elija el directorio en el que estaba instalada la anterior versión de Identity Manager y haga clic en Siguiente.

El instalador muestra barras de progreso para los procesos previos y posteriores a la actualización y luego presenta el panel de resumen de la instalación.

8. Para obtener información detallada sobre la instalación, haga clic en Details (detalles) y luego en Cerrar para salir del instalador.
9. Suprima todos los archivos compilados de Identity Manager del directorio de trabajo del servidor de aplicaciones.
10. Si está ejecutando la puerta de enlace en un sistema remoto, actualícela con el siguiente procedimiento.
 - a. Inicie la sesión en el sistema Windows y cambie al directorio en el que se encuentra instalada la puerta de enlace.
 - b. Detenga el servicio de la puerta de enlace ejecutando el comando:

```
gateway -k
```
 - c. Si utiliza Windows 2000 o una versión posterior, cierre todas las instancias del plugin Services MMC.
 - d. Utilice el comando siguiente para suprimir el servicio de puerta de enlace:

```
gateway -r
```

- e. Haga la copia de seguridad y borre los archivos de la puerta de enlace.
- f. Descomprima los nuevos archivos de la puerta de enlace.
Si va a instalar la puerta de enlace actualizada en un sistema distinto del servidor de Identity Manager, copie el archivo `gateway.zip` del CD de instalación de Identity Manager.
- g. Descomprima el archivo `gateway.zip` en el directorio donde está instalada la puerta de enlace.
- h. Utilice el comando siguiente para instalar el servicio de puerta de enlace:
`gateway -i`
- i. Utilice el comando siguiente para iniciar el servicio de puerta de enlace:
`gateway -s`

Actualización manual

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

-
- NOTAS**
- No olvide configurar 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`.
-

En plataformas Windows

Utilice los pasos siguientes para actualizar Identity Manager de forma manual en las plataformas Windows compatibles:

1. Detenga el servidor de aplicaciones y la Puerta de enlace de Sun Identity Manager.
2. Actualice la base de datos de Identity Manager. (Consulte [Paso 2 en la página 77](#) para obtener instrucciones detalladas.)
3. Introduzca los comandos siguientes para configurar el entorno:

```
set ISPATH=Ruta de acceso al software de instalación
set WSHOME=Ruta de acceso al directorio de montaje O instalación de Identity Manager
set TEMP=Ruta de acceso al directorio temporal
```

4. Ejecute el proceso previo:

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

5. Instale el software:

```
cd %WSHOME%
jar -xvf %ISPATH%\IDM.WAR
```

6. Ejecute el proceso posterior:

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

NOTA El programa de instalación permite actualizar instalaciones en las que se haya borrado, deshabilitado o cambiado el nombre de la cuenta predeterminada de Configurator.

El instalador solicita el nombre de usuario y la contraseña para importar el archivo `update.xml` durante el proceso posterior a la actualización. Si el nombre de usuario o la contraseña se introducen de forma incorrecta, el sistema solicita su correcta introducción (hasta tres veces). El error se muestra en el cuadro de texto situado detrás.

Para realizar la instalación manual, es necesario suministrar los indicadores `-U username -P password` para pasar las credenciales al procedimiento `UpgradePostProcess`.

7. Si ha realizado la instalación en un directorio de montaje, cree un archivo `.war` para la implantación en el servidor de aplicaciones.
8. Suprima los archivos de Identity Manager del directorio de trabajo del servidor de aplicaciones.
9. Si el proceso de actualización no lo ha hecho aún, traslade cualquier archivo de clase de parches del directorio `WEB-INF\classes` al directorio `$WSHOME\patches\HotfixName`.

10. Inicie el servidor de aplicaciones.
11. Actualice y, a continuación, reinicie la Puerta de enlace de Sun Identity Manager.
(Consulte [Paso 10 en la página 78](#) para obtener instrucciones detalladas.)

En plataformas UNIX

Utilice los pasos siguientes para actualizar Identity Manager de forma manual en las plataformas UNIX compatibles:

1. Detenga el servidor de aplicaciones y la Puerta de enlace de Sun Identity Manager.
2. Actualice la base de datos de Identity Manager. (Consulte [Paso 2 en la página 77](#) para obtener instrucciones.)
3. Introduzca los comandos siguientes para configurar el entorno:

```
export ISPATH=Ruta de acceso al software de instalación
export WSHOME=Ruta de acceso al directorio de montaje O instalación de Identity Manager
export TEMP=Ruta de acceso al directorio temporal
```

4. Ejecute el proceso previo:

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

5. Instale el software:

```
cd $WSHOME
jar -xvf $ISPATH/idm.war
```

6. Ejecute el proceso posterior:

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

NOTA El programa de instalación permite actualizar instalaciones en las que se haya borrado, deshabilitado o cambiado el nombre de la cuenta predeterminada de Configurator.

El instalador solicita el nombre de usuario y la contraseña para importar el archivo `update.xml` durante el proceso posterior a la actualización. Si el nombre de usuario o la contraseña se introducen de forma incorrecta, el sistema solicita su correcta introducción (hasta tres veces). El error se muestra en el cuadro de texto situado detrás.

Para realizar la instalación manual, es necesario suministrar los indicadores `-U username -P password` para pasar las credenciales al procedimiento `UpgradePostProcess`.

7. Cambie al directorio `$WSHOME/bin/solaris` o `$WSHOME/bin/linux` y configure los permisos sobre los archivos del directorio para que sean ejecutables.
8. Si ha realizado la instalación en un directorio de montaje, cree un archivo `.war` para la implantación en el servidor de aplicaciones.
9. Suprima los archivos de Identity Manager del directorio de trabajo del servidor de aplicaciones.
10. Si el proceso de actualización no lo ha hecho aún, traslade cualquier archivo de clase de parches del directorio `WEB-INF/classes` al directorio `$WSHOME/patches/HotfixName`.
11. Inicie el servidor de aplicaciones.
12. Actualice y, a continuación, reinicie la Puerta de enlace de Sun Identity Manager. (Consulte [Paso 10 en la página 78](#) para obtener instrucciones.)

API desaprobada

En esta sección se enumeran todas las Identity Manager interfaces de programación de aplicaciones (API) que se han desaprobado a partir de Identity Manager 6.0 2005Q4M3, y las alternativas (si existen). Esta información se ha dividido como sigue:

- [Constructores y clases desaprobados](#)
- [Métodos y campos desaprobados](#)

Constructores y clases desaprobados

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

Desaprobado	Alternativa
com.sun.idm.idmx.IDMXContext	com.waveset.object.LighthouseContext
com.sun.idm.idmx.IDMXContextFactory	com.waveset.session.SessionFactory
com.waveset.adapter.ActiveDirectoryActiveSyncAdapter	com.waveset.adapter.ADSIResourceAdapter
com.waveset.adapter.AIXResourceAdapter.BlockAcctIter	Las referencias a esta clase deben sustituirse por un iterador de cuentas basado en el modelo del proveedor. Por ejemplo, BufferedAccountQueue(new AIXAccountSupplier).
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.AttrParse	com.waveset.object.AttrParse
com.waveset.adapter.ConfirmedSync	Las referencias a esta clase deben sustituirse por un iterador de cuentas basado en el modelo del proveedor. Por ejemplo, BufferedAccountQueue(new LinuxAccountSupplier).
com.waveset.adapter.DbiBufIterator	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.LinuxResourceAdapter.BlockAcctIter	
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter

Desaprobado	Alternativa
<code>com.waveset.adapter.ResourceAdapterBase.SimpleAccountIterator</code>	Los usuarios de esta clase deben pasar a usar el modelo del proveedor para la iteración de cuentas. Un sustituto directo de esta clase sería: <code>new BufferedAccountQueue(new SimpleAccountSupplier(accounts));</code>
<code>com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter</code>	Las referencias a esta clase deben sustituirse por un iterador de cuentas basado en el modelo del proveedor. Por ejemplo, <code>BufferedAccountQueue(new SVIDAccountSupplier)</code> .
<code>com.waveset.adapter.TopSecretActiveSyncAdapter</code>	<code>com.waveset.adapter.TopSecretResourceAdapter</code>
<code>com.waveset.exception.ConfigurationError</code>	<code>com.waveset.util.ConfigurationError</code>
<code>com.waveset.exception.IOException</code>	<code>com.waveset.util.IOException</code>
<code>com.waveset.exception.XmlParseException</code>	<code>com.waveset.util.XmlParseException</code>
<code>com.waveset.object.IAPI</code>	<code>com.waveset.adapter.iapi.IAPI</code>
<code>com.waveset.object.IAPIProcess</code>	<code>com.waveset.adapter.iapi.IAPIFactory</code>
<code>com.waveset.object.IAPIUser</code>	<code>com.waveset.adapter.iapi.IAPIUser</code>
<code>com.waveset.object.RemedyTemplate</code>	
<code>com.waveset.object.ReportCounter</code>	
<code>com.waveset.object.SourceManager</code>	<code>com.waveset.view.SourceAdapterManagerView</code>
<code>com.waveset.object.ViewMaster()</code>	
<code>com.waveset.object.ViewMaster.ViewMaster(String,String)</code>	
<code>com.waveset.object.ViewMaster.ViewMaster(Subject,String)</code>	
<code>com.waveset.security.authn.LoginInfo</code>	<code>com.waveset.object.LoginInfo</code>
<code>com.waveset.security.authn.SignedString</code>	<code>com.waveset.util.SignedString</code>
<code>com.waveset.security.authn.Subject</code>	<code>com.waveset.object.Subject</code>
<code>com.waveset.security.authz.Permission</code>	<code>com.waveset.object.Permission</code>
<code>com.waveset.security.authz.Right</code>	<code>com.waveset.object.Right</code>
<code>com.waveset.util.CSVParser</code>	<code>com.waveset.util.ConfigurableDelimitedFileParser</code>
<code>com.waveset.util.Debug</code>	<code>com.sun.idm.logging.Trace</code>
<code>com.waveset.util.HtmlUtil</code>	<code>com.waveset.ui.util.html.HtmlUtil</code>
<code>com.waveset.util.ITrace</code>	<code>com.sun.idm.logging.Trace</code>
<code>com.waveset.util.PipeDelimitedParser</code>	<code>com.waveset.util.ConfigurableDelimitedFileParser</code>

Métodos y campos desaprobados

En las tablas de esta sección se recogen todos los métodos y campos que se han desaprobado 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 o campo desaprobado	Alternativa
<code>handlePDEException(Exception)</code>	<code>handlePDEException(PDEException)</code>

`com.waveset.adapter.ACF2ResourceAdapter`

Método o campo desaprobado	Alternativa
<code>getAccountAttributes(String)</code>	

com.waveset.adapter.ActiveSync

Método o campo desaprobadado	Alternativa
RA_UPDATE_IF_DELETE	

com.waveset.adapter.ActiveSyncUtil

Método o campo desaprobadado	Alternativa
getLogFileFullPath()	

com.waveset.adapter.ADSIResourceAdapter

Método o campo desaprobadado	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 o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.AuthSSOResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.ClearTrustResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.DatabaseTableResourceAdapter

Método o campo desaprobadado	Alternativa
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.DB2ResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.DominoResourceAdapter

Método o campo desaprobadado	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 o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.ExampleTableResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.GenericScriptResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.GetAccessResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.HostConnectionPool

Método o campo desaprobadado	Alternativa
getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool#getAffinityConnection(HostAccessLogin)
releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(HostAccess)
releaseConnection(IHostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(IHostAccess)

com.waveset.adapter.HostConnPool

Método o campo desaprobadado	Alternativa
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	
putFree(IHostAccess)	putAffinityFree

com.waveset.adapter.iapi.IAPIFactory

Método o campo desaprobado	Alternativa
getAPIProcess(Map,Map,String,Resource)	getAPI(Map,Map,String,ResourceAdapterBase)
getAPIProcess(Element)	
getAPIUser(Element)	
getAPIUser(Map,Map,String,Map)	getAPI(Map,Map,String,ResourceAdapterBase)
getAPIUser(Map,Map,String,Resource)	getAPI(Map,Map,String,ResourceAdapterBase)

com.waveset.adapter.IDMResourceAdapter

Método o campo desaprobado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.INISafeNexessResourceAdapter

Método o campo desaprobado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.LDAPResourceAdapterBase

Método o campo desaprobadado	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 o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.NaturalResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.NDSResourceAdapter

Método o campo desaprobado	Alternativa
buildEvent(UpdateRow)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.ONTDirectorySmartResourceAdapter

Método o campo desaprobado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.OS400ResourceAdapter

Método o campo desaprobado	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 o campo desaprobado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.RASecureConnection

Método o campo desaprobadado	Alternativa
ExchangeAuth(boolean)	ExchangeAuth(boolean,byte[])

com.waveset.adapter.RequestResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.ResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceAdapterBase

Método o campo desaprobadado	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 o campo desaprobadado	Alternativa
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceManager

Método o campo desaprobadado	Alternativa
getResourceTypes()	getResourcePrototypes() getResourcePrototypes(ObjectCache,boolean)
getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

com.waveset.adapter.SAPHRActiveSyncAdapter

Método o campo desaprobadado	Alternativa
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.SAPResourceAdapter

Método o campo desaprobadado	Alternativa
reverseMapMultiAttr(String, Object, WSUser)	
setUserField(JCO.Function, String)	Function#setUserField(String)
unexpirePassword(String,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)

com.waveset.adapter.ScriptedConnection

Subclase	Método o campo desaprobadado	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 o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SkeletonResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SMEResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SQLServerResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.SunAccessManagerResourceAdapter

Método o campo desaprobado	Alternativa
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.SybaseResourceAdapter

Método o campo desaprobado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.TestResourceAdapter

Método o campo desaprobado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.TopSecretResourceAdapter

Método o campo desaprobado	Alternativa
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)
login(IHostAccess hostAccess)	#login(IHostAccess hostAccess, ServerAffinity affinity)

com.waveset.adapter.VerityResourceAdapter

Método o campo desaprobado	Alternativa
getAccountAttributes(String)	

com.waveset.adapter.XMLResourceAdapter

Método o campo desaprobadado	Alternativa
getAccountAttributes(String)	

com.waveset.msgcat.Catalog

Método o campo desaprobadado	Alternativa
getMessage(String, Object[], Locale)	format (Locale, String, Object[])
getMessage(Locale, String, Object[])	format (Locale, String, Object[])
getMessage(Locale, String)	format (Locale, String)
getMessage(String, Locale)	format (Locale, String)
getMessage(String, Object[])	format (Locale, String, Object[])

com.waveset.object.Account

Método o campo desaprobadado	Alternativa
getUnowned()	hasOwner()
setUnowned(boolean)	setOwner(WSUser)

com.waveset.object.AccountAttributeType

Método o campo desaprobadado	Alternativa
getAttrType()	getSyntax()
setAttrType(String)	setSyntax(String)
	setSyntax(Syntax)

com.waveset.object.Attribute

Método o campo desaprobadado	Alternativa
BLOCK_SIZE	BLOCK_ROWS_GET BLOCK_ROWS_LIST
EVENTDATE	EVENT_DATETIME
EVENTTIME	EVENT_DATETIME
getDbColumnLength()	
getDbColumnName()	
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 o campo desaprobadado	Alternativa
AttributeDefinition(String,String)	AttributeDefinition(String,Syntax)
setAttrType(String)	setSyntax(Syntax)

com.waveset.object.AuditEvent

Método o campo desaprobadado	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 o campo desaprobadado	Alternativa
getAllObjects(Type,AttributeCondition[])	listObjects(Type,AttributeCondition[])
getAllObjects(Type,WSAttributes)	listObjects(Type,WSAttributes)
getAllObjects(Type)	listObjects(Type)

com.waveset.object.Constants

Método o campo desaprobadado	Alternativa
MAX_SUMMARY_STRING_LENGTH	

com.waveset.object.EmailTemplate

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

com.waveset.object.GenericObject

Método o campo desaprobado	Alternativa
toMap(boolean)	toMap(String,int)
toMap(String,boolean)	

com.waveset.object.LoginConfig

Método o campo desaprobado	Alternativa
getApp(String)	getLoginApp(String)

com.waveset.object.MessageUtil

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

com.waveset.object.RepositoryResult

Método o campo desaprobado	Alternativa
get(int)	
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	
seek(int)	hasNext() next()
sort()	

com.waveset.object.RepositoryResult.Row

Método o campo desaprobadado	Alternativa
getSummaryAttributes()	getAttributes()

com.waveset.object.ResourceAttribute

Método o campo desaprobadado	Alternativa
setType(String)	setSyntax(Syntax)

com.waveset.object.TaskInstance

Método o campo desaprobadado	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 o campo desaprobadado	Alternativa
setMode(String)	setExecMode(String)
setMode(TaskDefinition.ExecMode)	setExecMode(TaskDefinition,ExecMode)

com.waveset.object.Type

Método o campo desaprobadado	Alternativa
AUDIT_CONFIG	
AUDIT_PRUNER_TASK	
AUDIT_QUERY	
DISCOVERY	
getSubtypes()	getLegacyTypes()
NOTIFY_CONFIG	
REPORT_COUNTER	
SUMMARY_REPORT_TASK	
USAGE_REPORT	
USAGE_REPORT_TASK	

com.waveset.object.UserUIConfig

Método o campo desaprobadado	Alternativa
getCapabilityGroups()	
getAppletColumns()	getAppletColumnDefs()
getCapabilityGroup(String)	
getCapabilityGroupNames()	
getFindMatchOperatorDisplayNameKeys()	
getFindMatchOperators()	
getFindResultsColumns()	
getFindResultsSortColumn()	
getFindUserDefaultSearchAttribute()	
getFindUserSearchAttributes()	
getFindUserShowAttribute(int)	
getFindUserShowCapabilitiesSearch(int)	
getFindUserShowDisabled(int)	
getFindUserShowOrganizationSearch(int)	

Método o campo desaprobadado	Alternativa
getFindUserShowProvisioningSearch(int)	
getFindUserShowResourcesSearch(int)	
getFindUserShowRoleSearch(int)	

com.waveset.object.WSUser

Método o campo desaprobadado	Alternativa
getApproverDelegate()	getWorkItemDelegate(String workItemType)
getDelegateHistory()	getWorkItemDelegateHistory()
setApproverDelegate(WsUser.Delegate)	addWorkItemDelegate(Delegate workItemDelegate)
setDelegateHistory(List)	etWorkItemDelegateHistory(List workItemDelegateHistory)

com.waveset.session

Subclase	Método o campo desaprobadado	Alternativa
LocalSession	getAdministrators(Map)	com.waveset.view.WorkItemUtil#getAdministrators
Sesión	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 o campo desaprobadado	Alternativa
getAccessPolicy()	
getRepository()	

com.waveset.ui.util.FormUtil

Método o campo desaprobado	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)
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)

Método o campo desaprobadado	Alternativa
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)
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)
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 o campo desaprobado	Alternativa
installIfAvailable()	

com.waveset.util.PdfReportRenderer

Método o campo desaprobado	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 o campo desaprobado	Alternativa
getQuota()	

com.waveset.util.ReportRenderer

Método o campo desaprobadado	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 o campo desaprobadado	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)
level4(Object,String)	com.sun.idm.logging.trace.Trace#level4(String)

Método o campo desaprobadado	Alternativa
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 desaprobadado	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)
getLocalHostName()	#getServerId() (para obtener un identificador de servidor único)

com.waveset.workflow.WorkflowContext

Método o campo desaprobadado	Alternativa
VAR_CASE_TERMINATED	com.waveset.object.WFProcess#VAR_CASE_TERMINATED

Método o campo desaprobadado	Alternativa
getApproverDelegate()	
setApproverDelegate()	
getDelegateHistory()	
setDelegateHistory()	

Anexos a la documentación y correcciones

Esta sección contiene información nueva y corregida que ha sido necesaria tras publicar la documentación de Identity Manager 7.1. Esta información se ha dividido como sigue:

- [Identity Manager Installation](#)
- [Actualización de Identity Manager](#)
- [Identity Manager Administration Guide](#)
- [Identity Manager Resources Reference](#)
- [Identity Manager Technical Deployment Overview](#)
- [Identity Manager Workflows, Forms, and Views](#)
- [Identity Manager Deployment Tools](#)
- [Ajuste, solución de problemas y mensajes de error en Identity Manager](#)
- [Implementación de Identity Manager Service Provider Edition](#)
- [Utilización de helpTool](#)

Identity Manager Installation

Esta sección contiene información nueva y corregida relacionada con *Sun Java(TM) System Identity Manager Installation*.

- El adaptador de recursos de Exchange 5.5 no es compatible. Ignore toda referencia a dicho adaptador.

Actualización de Identity Manager

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager Upgrade*.

- Antes de actualizar, es importante realizar copia de seguridad del directorio donde está instalado Identity Manager y de la base de datos que utiliza Identity Manager. Para hacer copia de seguridad del sistema de archivos de Identity Manager puede utilizar software de terceros o una utilidad de copia de seguridad incluida en su sistema. Para hacer copia de seguridad de la base de datos, consulte en la documentación de ésta cuáles son los procedimientos aconsejados. (ID-2810)

Antes de crear las copias de seguridad debe cerrar o dejar inactivo Identity Manager. A continuación, ejecute las utilidades correspondientes para hacer copia de seguridad de la base de datos y del sistema de archivos donde está instalado Identity Manager.

- El recurso AD Active Sync se ha desaprobadado, y ha sido reemplazado por AD. Realice los pasos siguientes para migrar AD Active Sync a versiones más recientes: (ID-11363)
 - Exporte el recurso AD Active Sync existente a un archivo xml (desde la línea de comandos o las páginas de depuración).
 - Elimine el recurso existente (esto no afecta a usuarios de Identity Manager ni a usuarios de cuentas de recursos).
 - Cree un recurso AD nuevo que sea Active Sync.
 - Exporte el nuevo objeto de recurso a un archivo XML.
 - Edite este archivo y cambie el valor de los atributos de ID y de nombre para que coincidan con los valores del objeto de recurso OLD que se ha guardado en el paso 1. Estos atributos se encuentran en la ficha `<Resource id='idnumber' name='AD' ...>`.
 - Guarde los cambios realizados en el archivo.
 - Importe el objeto modificado en Identity Manager mediante la página Configure>Import Exchange File o la línea de comandos.
- La sección Otros objetos de repositorio personalizados se ha actualizado con instrucciones sobre el uso de la función de instantáneas de Identity Manager para crear una instantánea o imagen de referencia de los objetos de repositorio personalizados en una implementación. (ID-14840)

Otros objetos de repositorio personalizados

Anote los nombres de todos los objetos de repositorio personalizados que haya creado o actualizado. Quizá tenga que exportar dichos objetos desde la instalación actual y luego reimportarlos a la nueva versión de Identity Manager tras actualizar.

- Grupo Admin
- Rol de Admin
- Configuración
- Directiva
- Tarea de abastecimiento
- Configuración de Remedy
- Formulario de recurso
- Formulario de recurso
- Rol
- Regla
- Definición de tarea
- Plantilla de tarea
- Formulario de usuario

Puede usar la función de instantáneas de Identity Manager para crear una instantánea o imagen de referencia de los objetos de repositorio personalizados en su implementación, que le resultará muy útil en caso de actualización.

Cree copias instantáneas de los siguientes tipos de objetos específicos del sistema como elementos de comparación:

- AdminGroup
- AdminRole
- Configuración
- EmailTemplate
- Directiva
- ProvisionTask
- RemedyConfig
- ResourceAction

- Resourceform
- Rol
- Regla
- TaskDefinition
- TaskTemplate
- UserForm

Ello le permitirá comparar dos instantáneas para averiguar los cambios aplicados a determinados objetos del sistema antes y después de actualizar.

NOTA Esta función no está ideada para realizar comparativas detalladas continuas de XML (diff), es una herramienta básica para efectuar comparaciones preliminares.

Para crear una instantánea:

1. En la página Depurar de Identity Manager ([Figura 1](#)), pulse el botón SnapShot para acceder a la página Administración de instantáneas.

Figura 1 Página Administración de instantáneas

Administración de instantáneas

En esta página se pueden administrar instantáneas de la configuración del sistema. Básicamente, copia tipos específicos del sistema para comparar. A partir de esta comparación, se pueden determinar las modificaciones realizadas antes y después de la instantánea. Ello puede ayudar a disponer de un inventario de las modificaciones de objeto para usarlo al planificar una actualización.

The image shows a control panel for managing snapshots. It includes a 'Crear' button followed by a text input field. Below that is an 'Eliminar' button with a dropdown arrow. The 'Comparar' button is followed by two dropdown arrows. Below these is the 'Exportar' label. At the bottom is a 'Cancelar' button.

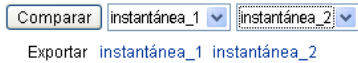
2. Introduzca un nombre para la instantánea en el cuadro de texto Crear y pulse el botón Crear.

Cuando Identity Manager añade la instantánea, su nombre aparece en la lista del menú Comparar y a la derecha de la etiqueta Exportar.

Para comparar dos instantáneas:

1. Seleccione las instantáneas en cada uno de los dos menús Comparar ([Figura 2](#)).

Figura 2 Página Administración de instantáneas



2. Pulse el botón Comparar.
 - Si no se ha cambiado ningún objeto, la página indicará que no se han encontrado diferencias.
 - Si por el contrario se han encontrado cambios de objetos, la página mostrará el tipo y nombre del objeto, así como si el objeto es distinto, está ausente o está presente.

Por ejemplo, si un objeto está presente en la instantánea 1, pero no en la instantánea 2, la columna de la instantánea 1 indicará **Presente** y la columna de la instantánea 2 indicará **Ausente**.

Puede exportar instantáneas en formato XML. Haga clic en el nombre de la instantánea para exportar el archivo de la misma.

Para eliminar una instantánea, selecciónela en el menú Eliminar y haga clic en el botón Eliminar.

- Se ha agregado el párrafo siguiente a la sección de JSP modificados para incluir información sobre el uso del comando `inventory -m` para identificar JSP modificados en una implementación: (ID-14840)

Puede utilizar el comando `inventory -m` (descrito en la página anterior) para identificar las modificaciones de JSP realizadas en la implementación.
- Si actualiza de la versión 6.x a la versión 7.0 o 7.1 y quiere empezar a utilizar las nuevas páginas de usuario final de Identity Manager, deberá cambiar manualmente la configuración del sistema `ui.web.user.showMenu` a **true** para que aparezca la barra de navegación horizontal. (ID-14901)
- Si actualiza la versión 6.0 o 7.0 a la versión 7.1 y está utilizando `LocalFiles`, tiene que exportar todos los datos antes de la actualización para luego importarlos de nuevo una vez que se instala correctamente la versión 7.1. (ID-15366)
- Para actualizar de la versión 6.0 o 7.0 a la 7.1 hay que actualizar el esquema de la base de datos. (ID-15392)
 - En caso de actualizar de 6.0 a 7.1, debe utilizar la secuencia de comandos `upgradeto71.*` correspondiente al tipo de RDBMS que use.
 - En caso de actualizar de 7.0 a 7.1, debe utilizar la secuencia de comandos `upgradeto71from70.*` correspondiente al tipo de RDBMS que use.

- Durante el proceso de actualización, Identity Manager analiza todos los roles del sistema y actualiza todos los vínculos de subroles y súper roles ausentes mediante la clase RoleUpdater. (ID-15734)

Para verificar y actualizar roles fuera del proceso de actualización, importe el nuevo objeto de configuración RoleUpdater, suministrado en `sample/forms/RoleUpdater.xml`. Por ejemplo:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <ImportCommand class='com.waveset.session.RoleUpdater' >
    <Map>
      <MapEntry key='verbose' value='true' />
      <MapEntry key='noupdate' value='false' />
      <MapEntry key='nofixsubrolelinks' value='false' />
    v</Map>
  </ImportCommand>
</Waveset>
```

Donde:

- **verbose:** Proporciona salida detallada al actualizar los roles. Especifique **false** para permitir una actualización silenciosa de los roles.
 - **noupdate:** Determina si se actualizan los roles. Especifique **false** para obtener un informe que incluya únicamente los roles que se van a actualizar.
 - **nofixsubrolelinks:** Determina si los súper roles se actualizan con vínculos de subrol ausentes. El valor predeterminado es "false", que repara los vínculos.
- Si hay espacio en la ruta al directorio de instalación de Identity Manager, debe especificar la variable de entorno WSHOME sin comillas ("), como indica el ejemplo siguiente (ID-15470):

NOTA Las barras diagonales finales (\) no se deben utilizar al especificar la ruta, aunque no contenga espacios.

```
set WSHOME=c:\Program Files\Apache Group\Tomcat 4.1\idm
```

O bien

```
set WSHOME=c:\Progra~1\Apache~1\Tomcat~1\idm
```

La ruta siguiente no funciona:

```
set WSHOME="c:\Program Files\Apache Group\Tomcat 4.1\idm"
```

Identity Manager Administration Guide

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager Administration*.

Capítulo 3, User and Account Management (Administración de usuarios y de cuentas)

- En la sección “Disable Users (User Actions, Organization Actions)” se ha corregido la nota:

NOTA	Si un recurso asignado carece de soporte nativo para deshabilitar cuentas, pero sí permite cambiar contraseñas, es posible configurar Identity Manager para deshabilitar cuentas de usuario en dicho recurso asignando nuevas contraseñas generadas aleatoriamente. Esta configuración requiere que se habiliten las características de cuenta Deshabilitar y Contraseña en la página Parámetros de Identity System del Asistente de recursos. Para obtener más información, consulte el capítulo 4, dedicado a la configuración.
-------------	---

- En la sección “Enable Users (User Actions, Organization Actions)” se ha añadido la nota:

NOTA	Si un recurso asignado carece de soporte nativo para habilitar cuentas, pero sí permite cambiar contraseñas, es posible configurar Identity Manager para habilitar cuentas de usuario en dicho recurso reiniciando las contraseñas. Esta configuración requiere que se deshabiliten las características de cuenta Deshabilitar y Contraseña en la página Parámetros de Identity System del Asistente de recursos. Para obtener más información, consulte el capítulo 4, dedicado a la configuración.
-------------	--

Capítulo 5, Administration (Administración)

- En la sección “Delegating Work Items” se ha añadido la nota siguiente.

NOTA	Una vez configurada la delegación, todos los elementos de trabajo que se creen durante el periodo efectivo de delegación se añadirán a la lista del usuario y a la del delegado. Si termina la delegación, se recuperarán los elementos de trabajo delegados, lo que podría dar lugar a elementos duplicados. Cuando se aprueba o rechaza un elemento, el duplicado se suprime automáticamente de la lista.
-------------	---

- En la sección “Managing Work Items” se ha añadido la información siguiente.

Delegaciones a usuarios eliminados

Si ha delegado un elemento de trabajo a un usuario que después se elimina de Identity Manager, el usuario eliminado se indica entre paréntesis en la lista Delegaciones actuales. Si posteriormente edita o crea una delegación que incluya el usuario eliminado, fallará la acción. También fallará la creación o actualización de elementos de trabajo de cualquier usuario que se hayan delegado en un usuario eliminado.

Para recuperar los elementos de trabajo que se han delegado en un usuario eliminado, termine la delegación.

- Se ha agregado la capacidad Administrador de usuario final a la tabla “Identity Manager Capabilities Descriptions”. Cualquier usuario que tenga asignada esta capacidad puede ver y modificar los derechos sobre los tipos de objetos especificados en la capacidad de usuario final, así como el contenido de la regla de organizaciones controladas por el usuario final. Esta capacidad se asigna de forma predeterminada al usuario Configurator.

Capítulo 11, Identity Auditing (Auditoría de Identity)

Se ha añadido la información siguiente a este capítulo.

Solución de limitaciones de las capacidades de auditor

Las capacidades predeterminadas que se necesitan para realizar tareas de auditoría se hallan en la organización (grupo de objetos) de nivel superior o Top. En consecuencia, sólo los administradores que controlan Top pueden asignar estas capacidades a otros administradores.

Esta limitación se puede solucionar agregando las capacidades a otra organización. Identity Manager facilita esta tarea con dos utilidades incluidas en el directorio `sample/scripts`.

1. Para ver una lista de todas las capacidades (grupos Admin) y sus organizaciones asociadas (grupos de objetos), ejecute el comando:

```
beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
```

Este comando almacena la salida en un archivo de valores separados por comas (CSV).

2. Edite el archivo CSV para ajustar como convenga las asignaciones de capacidades a las organizaciones.
3. Ejecute este comando para actualizar Identity Manager.

```
beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
```

Capítulo 13, Service Provider Administrator (Administrador de Service Provider)

En la sección “Configure Synchronization” debe indicarse que el intervalo de sincronización predeterminado para las tareas de sincronización de Service Provider es 1 minuto.

Identity Manager Resources Reference

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager Resources Reference*:

- El adaptador de recursos de Exchange 5.5 no es compatible. Ignore toda referencia a dicho adaptador.
- En la documentación del adaptador de tabla de base de datos, no es válido el ejemplo del último predicado obtenido. Debe definirse así:

```
lastMod > '$(lastmod)'
```

- El adaptador Flat File Active Sync dificulta la configuración de la propiedad `sources.hosts` en el archivo `Waveset.properties`. Esta configuración debería efectuarse ahora mediante una directiva de sincronización.
- El adaptador NDS ofrece mejor compatibilidad con GroupWise:
 - El adaptador ahora puede gestionar oficinas de correos en dominios secundarios.
 - Los usuarios de GroupWise pueden suscribirse a cualquier lista de distribución conocida.
 - Es posible eliminar una oficina de correos sin especificar un patrón de eliminación.
- El procedimiento “Managing ACL List” indica: (ID-16476)

3. Edite el usuario en Identity Manager y en el formulario Editar usuario.

La instrucción correcta es:

3. Edite el usuario en Identity Manager con el formulario Editar usuario.

Identity Manager Technical Deployment Overview

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager Technical Deployment Overview*:

- Puede utilizar hojas de estilo en cascada para establecer el ancho de las columnas de las tablas de listas de usuarios y recursos en un valor porcentual o en un valor fijo expresado en píxeles. Para hacerlo, añada las siguientes clases de estilos (inhabilitadas de forma predeterminada) a `customStyle.css`. A continuación, puede editar los valores para que se cumplan los requisitos del usuario.

```
th#UserListTreeContent_Col0 {
    width: 1px;
}

th#UserListTreeContent_Col1 {
    width: 1px;
}

th#UserListTreeContent_Col2 {
    width: 50%;
}

th#UserListTreeContent_Col3 {
    width: 50%;
}

th#ResourceListTreeContent_Col0 {
    width: 1px;
}

th#ResourceListTreeContent_Col1 {
    width: 1px;
}

th#ResourceListTreeContent_Col2 {
    width: 33%;
}

th#ResourceListTreeContent_Col3 {
    width: 33%;
}

th#ResourceListTreeContent_Col4 {
    width: 33%;
}
```

También puede cambiar el tamaño de las columnas haciendo clic sobre el borde derecho del encabezado de la columna y arrastrándolo. Si pasa el ratón por el borde derecho del encabezado, el cursor se transformará en una flecha de redimensionamiento horizontal. Haga clic con el botón izquierdo del ratón y arrastre el cursor para cambiar el tamaño de la columna (la acción finaliza cuando se suelta el botón del ratón).

- El objeto de configuración del sistema (System Configuration) ahora contiene el atributo `security.delegation.historyLength`, que controla el número de delegaciones registradas con anterioridad.
- El panel de control Revisión de accesos y el informe de detalles de revisión de los accesos muestran instancias de revisiones que se han guardado en los registros de auditoría. Si no se realizan funciones de mantenimiento de la base de datos, el tamaño de los registros de auditoría nunca se reduce y la lista de revisiones crece. Identity Manager ofrece la posibilidad de limitar las revisiones mostradas siguiendo criterios de antigüedad. Para cambiar este límite, debe personalizar `compliance/dashboard.jsp` (panel de control) y `sample/auditortasks.xml` (informe de detalles). (El valor predeterminado establece que sólo se muestren las revisiones con menos de 2 años de antigüedad.)

Para restringir las revisiones incluidas en el panel de control Revisión de accesos, personalice `compliance/dashboard.jsp` de la manera siguiente:

- a. Abra `compliance/dashboard.jsp` en el Identity Manager IDE o en un editor de su elección:
- b. Cambie la línea `form.setOption("maxAge", "2y");` a `form.setOption("maxAge", "6M");` para limitar la lista de revisiones a las ejecutadas en los últimos 6 meses. Estos son los calificadores:
 - m: minuto
 - h: hora
 - d: día
 - w: semana
 - m: mes
 - y: año

Para ver todas las revisiones que sigan existiendo en los registros de auditoría, inhabilite esta línea.

Para limitar las revisiones incluidas en el informe de detalles de revisión de los accesos:

- a. Abra `sample/auditortasks.xml` en el IDE o un editor de su elección.

b. Cambie la línea siguiente según se indica:

```
<s>maxAge</s>
<s>2y</s>
```

a

```
<s>maxAge</s>
<s>6M</s>
```

para limitar las revisiones a los últimos 6 meses. Se utilizan los calificadores citados anteriormente.

Cada revisión periódica de los accesos incluye un conjunto de registros UserEntitlement que se crearon en el momento de ejecutar la revisión. Estos registros, que se acumulan con el tiempo, proporcionan información histórica de interés sobre las cuentas. No obstante, para conservar espacio en la base de datos, considere la posibilidad de borrar algunos registros. Puede borrar un registro ejecutando **Tareas del servidor > Ejecutar tareas > Eliminar revisión de acceso**. Cuando se suprime una revisión, se añaden entradas al registro de auditoría que dejan constancia de la eliminación y se borran todos los registros UserEntitlement asociados, con lo que se libera espacio en la base de datos.

- En la sección “ Changing Background Image on the Login Page”, la tercera línea de código debería indicar:

```
url(../images/other/login-backimage2.jpg)
```

- El Ejemplo de código 5.5 contiene información que debería aparecer en el Ejemplo de código 5.4.
El Ejemplo de código 5.4 debería aparecer como sigue:

Ejemplo de código 5-4 Personalización de las fichas de navegación

```
/* LEVEL 1 TABS */
.TabLvl1Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#333366;
    padding:6px 10px 0px;
}
a.TabLvl1Lnk:link, a.TabLvl1Lnk:visited {
    display:block;
    padding:4px 10px 3px;
    font: bold 0.95em sans-serif;
    color:#FFF;
    text-decoration:none;
    text-align:center;
}
table.TabLvl1Tbl td {
    background-image:url(../images/other/dot.gif);
```


Ejemplo de código 5-4 Personalización de las fichas de navegación (*Continuación*)

```

        background-repeat:repeat-x;
        background-position:left top;
        background-color:#666699;
        border:solid 1px #abab5;
    }
    table.TabLvl1Tbl td.TabLvl1TblSelTd {
        background-color:#9999CC;
        background-image:url(../images/other/dot.gif);
        background-repeat:repeat-x;
        background-position:left bottom;
        border-bottom:none;
    }
}

/* LEVEL 2 TABS */
.TabLvl2Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#9999CC;
    padding:6px 0px 0px 10px
}
a.TabLvl2Lnk:link, a.TabLvl2Lnk:visited{
    display:block;
    padding:3px 6px 2px;
    font: 0.8em sans-serif;
    color:#333;
    text-decoration:none;
    text-align:center;
}
table.TabLvl2Tbl div.TabLvl2SelTxt {
    display:block;
    padding:3px 6px 2px;
    font: 0.8em sans-serif;
    color:#333;
    font-weight:normal;
    text-align:center;
}
table.TabLvl2Tbl td {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left top;
    background-color:#CCCCFF;
    border:solid 1px #abab5;
}
table.TabLvl2Tbl td.TabLvl2TblSelTd {
    border-bottom:none;
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#FFF;
    border-left:solid 1px #abab5;
    border-right:solid 1px #abab5;
    border-top:solid 1px #abab5;
}

```

El Ejemplo de código 5.5 debería aparecer como sigue:

Ejemplo de código 5-5 Cambio de fichas del panel de fichas

```
table.Tab2TblNew td
{background-image:url(../images/other/dot.gif);background-repeat:repeat-x;background-positi
on:left top;background-color:#CCCCFF;border:solid 1px #8f989f}
table.Tab2TblNew td.Tab2TblSelTd
{border-bottom:none;background-image:url(../images/other/dot.gif);background-repeat:repeat-
x;background-position:left bottom;background-color:#FFF;border-left:solid 1px
#8f989f;border-right:solid 1px #8f989f;border-top:solid 1px #8f989f}
```

- En la interfaz de usuario final de Identity Manager, la barra de navegación horizontal se habilita mediante el formulario de usuario final de navegación del archivo `enduser.xml`. (ID-12415)

El archivo `userHeader.jsp`, que está incluido en todas las páginas de usuario final, incorpora otro JSP denominado `menuStart.jsp`. Este JSP proporciona acceso a dos objetos de configuración del sistema:

- `ui.web.user.showMenu`: Habilita y deshabilita la presentación del menú de navegación (predeterminado: `true`).
- `ui.web.user.menuLayout`: Determina si el menú se va a representar como una barra de navegación horizontal con fichas (predeterminado: `horizontal`) o un árbol vertical (`vertical`).

Las clases de estilo en cascada que determinan cómo se va a aparecer el menú se encuentran en `style.css`.

- Identity Manager ahora ha cambiado la cuenta **Lighthouse** por la cuenta **Identity Manager**. Este cambio de nombre se puede anular mediante el uso de un catálogo personalizado. (ID-14918) Para obtener información sobre los catálogos personalizados, consulte *Habilitación de internacionalización en Identity Manager Technical Deployment Overview*.

La presentación del nombre del producto se controla con las siguientes entradas del catálogo:

`PRODUCT_NAME=Identity Manager`

`LIGHTHOUSE_DISPLAY_NAME=[PRODUCT_NAME]`

`LIGHTHOUSE_TYPE_DISPLAY_NAME=[PRODUCT_NAME]`

`LIGHTHOUSE_DEFAULT_POLICY=Predeterminado [PRODUCT_NAME]` Directiva de cuentas

- Identity Manager proporciona un nuevo objeto de configuración (`WorkItemTypes`) que permite especificar todos los nombres, las extensiones y los nombres para mostrar de los tipos de elementos de trabajo admitidos. (ID-15468) Este objeto de configuración se define en `sample/workItemTypes.xml`, y se importa mediante `init.xml` y `update.xml`.

Gracias al atributo extendido existe una jerarquía de tipos de elementos de trabajo (`workItemTypes`). El elemento de trabajo que crea Identity Manager se delega a los usuarios especificados cuando es del tipo:

- delegado
- subordinado al tipo delegado

Tipo de elemento de trabajo	Descripción	Nombre para mostrar
Aprobación	WorkItem extendido	Aprobación
OrganizationApproval	Aprobación extendida	Aprobación de organización
ResourceApproval	Aprobación extendida	Aprobación de recurso
RoleApproval	Aprobación extendida	Aprobación de rol
Autenticación	WorkItem	Autenticación de revisión de acceso
revisión	WorkItem	Remediación
accessReviewRemediation	WorkItem	Acceso

- De forma predeterminada, el proceso de registro anónimo de Identity Manager genera valores de ID de cuenta y dirección de correo electrónico a partir de los nombres (`firstName`), apellidos (`lastName`) e ID de empleado que proporciona el usuario. (ID-16131)

Como el proceso de registro anónimo puede incluir caracteres no ASCII en la dirección de correo electrónico y el ID de las cuentas, es recomendable que los usuarios internacionales modifiquen las reglas de la biblioteca de reglas de usuario final (`EndUserRuleLibrary`) para que Identity Manager mantenga el uso de caracteres ASCII en ambos casos.

Para que los ID de las cuentas y las direcciones se generen en ASCII durante el proceso de registro anónimo, realice los pasos siguientes:

1. Modifique las tres reglas siguientes de la biblioteca de reglas de usuario final como se indica a continuación.

Modifique esta regla	Para realizar este cambio...
getAccountId	Para utilizar sólo employeeId (y eliminar firstName y lastName)
getEmailAddress	Para utilizar el ID de empleado solamente (eliminar el nombre, el apellido y ".")
verifyFirstname	Para cambiar la longitud de 2 a 1 y permitir el uso de nombres asiático de un solo carácter

2. Modifique el formulario End User Anon Enrollment Completion para eliminar los argumentos firstName (nombre) y lastName (apellido) de las llamadas a las normas AccountId y getEmailAddress.

Identity Manager Workflows, Forms, and Views

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager Workflows, Forms, and Views*.

- Puede desactivar la comprobación de las directivas en su formulario de usuario añadiendo a éste el campo siguiente:

```
<Field name='viewOptions.CallViewValidators'>
  <Display class='Hidden' />
  <Expansion>
    <s>false</s>
  </Expansion>
</Field>
```

Este campo sustituye al valor del campo OP_CALL_VIEW_VALIDATORS de modify.jsp.

- Las páginas de Interfaz de usuario de Identity Manager incluyen un segundo formulario de XPRESS que implementa la barra de navegación. Como resultado, la página representada contiene dos etiquetas <FORM>, cada una de ellas con un atributo de nombre (name) diferente:

```
<form name="endUserNavigation"> y <form name="mainform">
```

Para evitar posibles confusiones entre estos dos elementos <FORM>, asegúrese de utilizar el atributo `name` de la forma siguiente para indicar a qué etiqueta <FORM> hace referencia: `document.mainform` o `document.endUserNavigation`.

Capítulo 2, Identity Manager Workflow (Flujo de trabajo de Identity Manager)

- Identity Manager proporciona el nuevo flujo de trabajo de revisión de acceso de ejemplo en `/sample/workflows`. (ID-15393)

Comprobación automática de autenticación

Se utiliza para probar las nuevas reglas de determinación de revisión sin crear elementos de trabajo de autenticación. Este flujo de trabajo no crea elementos de trabajo y simplemente termina poco después de iniciarse. Deja todos los objetos de derecho a usuario en el mismo estado en que se crearon durante la exploración de acceso. Utilice las opciones Terminar y Eliminar para limpiar los resultados de las exploraciones de acceso que se ejecutan con este flujo de trabajo.

Este flujo de trabajo se puede importar cuando resulta necesario. (Identity Manager no lo importa automáticamente.)

- En Identity Manager, el Cumplimiento utiliza los flujos de trabajo como puntos de integración y personalización de la aplicación. A continuación se describen los flujos de trabajo predeterminados que están relacionados con el cumplimiento. (ID-15447)

Nombre del flujo de trabajo	Función
Remediación	Remediación para un único remediador que trabaja con una sola infracción del cumplimiento
Remediación de revisión de acceso	Remediación para un único remediador que trabaja con un solo registro de derecho a usuario (UserEntitlement)
Autenticación	Autenticación para un único autenticador que trabaja con un solo registro de derecho a usuario (UserEntitlement)
Multirremediación	Remediación para una sola infracción del cumplimiento y varios remediadores
Actualizar infracción del cumplimiento	Mitigar una infracción del cumplimiento
Iniciar exploración de acceso	Iniciar una tarea de exploración de acceso desde otra de revisión de acceso
Iniciar reexploración de derecho	Iniciar una nueva exploración de los derechos de acceso de un usuario
Iniciar reexploración de infracción	Iniciar una nueva exploración de las directivas de auditoría asociadas a un usuario

- La descripción de la propiedad `maxSteps` se ha revisado. (ID-15618)
Especifica el número máximo de pasos permitido en cualquier proceso o subproceso del flujo de trabajo. Cuando se supera este nivel, Identity Manager termina el flujo de trabajo. Este parámetro se utiliza como medida de seguridad para detectar el momento en el que el flujo de trabajo se bloquea y entra en un bucle infinito. El valor predeterminado configurado en el flujo de trabajo mismo es 0, lo que indica que Identity Manager debería obtener el valor real de la configuración global almacenada en el atributo `workflow.maxSteps` del objeto de configuración del sistema. El valor de configuración global es 5000.
- Este capítulo contiene la descripción de la tarea `Scripted Task Executor` siguiente. (ID-15258)
Ejecuta `BeanShell` o `Javascript` en función de la secuencia de comandos proporcionada. Como se trata de una tarea, se puede programar para que se ejecute periódicamente. Por ejemplo, se puede utilizar para exportar datos del repositorio a una base de datos de generación de informes y análisis. Entre las ventajas que ofrece se encuentra la posibilidad de introducir una tarea personalizada sin escribir código Java personalizado. (Aunque el código Java personalizado requiere una recompilación con cada actualización y debe implementarse en todos los servidores, no es necesario recompilarlo ni implementarlo debido a que la secuencia de comandos está incrustada en la tarea.)

Capítulo 3, Identity Manager Forms (Formularios de Identity Manager)

- Este capítulo contiene la siguiente descripción de los formularios utilizados en los procedimientos de auditoría y cumplimiento. (ID-15447, 16240)

Los formularios de auditoría y cumplimiento de Identity Manager aportan una funcionalidad exclusiva dentro de los formularios de Identity Manager: es posible asignar un formulario en función del usuario y en función de la organización. Los formularios asignados en función del usuario pueden multiplicar la eficacia en los procesos de autenticación y remediación.

Por ejemplo, se puede especificar el formulario de usuario que presenta Identity Manager para editar un usuario en el contexto de una revisión de acceso, una remediación o una remediación de una infracción del cumplimiento. Dicho formulario se puede especificar en el nivel de usuario o de organización. Cuando Identity Manager reexplora un usuario en el contexto de una reexploración o una remediación de revisión de acceso, la reexploración respeta las directivas de auditoría definidas en la exploración de acceso. Se puede definir de modo que incluya las directivas de auditoría de cumplimiento continuo.

NOTA	Para configurar componentes de auditoría, se necesita ser administrador de Identity Manager con las capacidades Configurar auditorías y Administrador de Auditor.
-------------	---

Información relacionada

- Consulte *Identity Manager Administration* para conocer los conceptos en que se basan las funciones de auditoría y cumplimiento de Identity Manager, así como los procedimientos básicos para implementarlas con sus parámetros predeterminados.
- Consulte las reglas de Identity Manager en *Identity Manager Deployment Tools* para conocer tanto información general al respecto como detalles específicos sobre las reglas de remediación.

Acerca del procesamiento de formularios relacionados con auditoría

De forma muy similar a `userForm` y `viewUserForm`, es posible definir un formulario para un determinado usuario u organización y ese usuario (o todos los de la organización) empleará dicho formulario. Si define un formulario tanto para un usuario como para la organización, tendrá prioridad el formulario del usuario. (Al buscar el formulario, Identity Manager indaga en las organizaciones hacia arriba.)

Los formularios relativos a auditoría funcionan del mismo modo que el de usuario y el de vista de usuarios: cada usuario puede designar un formulario determinado para utilizarlo, y la organización decidirá qué formulario debe emplear un usuario específico.

Especificación de formularios de usuario

Los formularios de lista de directivas de auditoría y de lista de exploraciones de acceso admiten una propiedad `fullView` que permite mostrar en el formulario un número considerable de datos sobre los elementos de la lista. Si esta directiva se configura como `false`, aumenta el rendimiento del visualizador de listas.

El formulario de lista de aprobación de acceso posee una propiedad análoga, denominada `includeUE`, mientras que el de lista de remediación utiliza la propiedad `includeCV`.

Formularios relacionados con auditoría

En la tabla siguiente se indican los formularios predeterminados relacionados con auditoría que se incluyen con Identity Manager.

Nombre del formulario	Nombre asignado	Control por el usuario	Función general
Lista de aprobación de acceso	<code>accessApprovalList</code>		Mostrar la lista de elementos de trabajo de autenticación.
Confirmación de eliminación de revisión de acceso	<code>accessReviewDeleteConfirmation</code>		Confirmar la eliminación de una revisión de acceso.
Confirmación de anulación de revisión de acceso	<code>accessReviewAbortConfirmation</code>		Confirmar la anulación de una revisión de acceso.

Nombre del formulario	Nombre asignado	Control por el usuario	Función general
Panel de control Revisión de accesos	accessReviewDashboard		Mostrar la lista completa de revisiones de acceso.
Formulario de remediación de revisión de acceso	accessReviewRemediationWorkItem	Sí	Representa cada elemento de trabajo de remediación basado en DU
Resumen de revisión de acceso	accessReviewSummary		Mostrar los detalles de una revisión de acceso específica.
Formulario de exploración de acceso	accessScanForm		Mostrar o modificar una exploración de acceso.
Lista de exploraciones de acceso	accessScanList		Mostrar la lista completa de exploraciones de acceso.
Confirmación de eliminación de exploración de acceso	accessScanDeleteConfirmation		Confirmar la eliminación de una exploración de acceso.
Lista de aprobación de acceso	attestationList	Sí	Mostrar la lista completa de exploraciones de acceso.
Formulario de autenticación	attestationWorkItem	Sí	Representa cada elemento de trabajo de autenticación
Derecho a usuario	userEntitlementForm		Mostrar el contenido de un registro de derecho a usuario.
Resumen de derecho a usuario	userEntitlementSummaryForm		
Dato de infracción	violationDetailForm		Mostrar los detalles de una infracción del cumplimiento.
Lista de remediación	remediationList	Sí	Mostrar una lista de elementos de trabajo de remediación.
Lista de directivas de auditoría	auditPolicyList		Mostrar una lista de las directivas de auditoría.
Confirmación de eliminación de directiva de auditoría	auditPolicyDeleteConfirmation		Confirmar la eliminación de una directiva de auditoría.
Datos de infracción por conflicto	conflictViolationDetailsForm		Mostrar la matriz de infracciones SOD.
Resumen de infracciones de cumplimiento	complianceViolationSummaryForm		
Formulario de remediación	reviewWorkItem	Sí	Representa una infracción de cumplimiento.

¿Por qué personalizar estos formularios?

Los autenticadores y remediadores pueden especificar formularios que muestren exactamente los detalles necesarios para aumentar la eficacia al autenticar y remediar. Por ejemplo, un autenticador de recursos puede mostrar atributos específicos de recurso en el formulario de lista para poder autenticarlos sin consultar cada elemento de trabajo. Como este formulario varía según el tipo de recurso (y, por tanto, los atributos), tiene sentido personalizar el formulario en función del autenticador.

Durante la autenticación, cada autenticador puede contemplar los derechos desde una perspectiva exclusiva. Por ejemplo, el autenticador de `idmManager` puede observar el derecho de usuario de forma genérica, mientras que a un autenticador de recursos sólo le interesan los datos específicos del recurso. Si se permite que cada autenticador adapte tanto el formulario de lista de autenticación como el de elementos de trabajo de autenticación (`AttestationWorkItem`) para recuperar y mostrar sólo la información que necesita, la interfaz del producto puede multiplicar su eficacia.

Variables de la tarea de exploración

En la definición de las tareas de exploración de directiva de auditoría y de exploración de acceso se especifica los formularios que se utilizan al iniciar la tarea. Estos formularios incluyen campos que permiten controlar la mayoría de las variables de la tarea de exploración, pero no todas.

Nombre de la variable	Valor predeterminado	Función
<code>maxThreads</code>	5	Indica el número de usuarios que pueden explorarse a la vez en una sola operación. El aumento de este valor ofrece la posibilidad de mejorar el resultado cuando se exploran usuarios con cuentas de muy bajos recursos.
<code>userLock</code>	5000	Indica el tiempo (en ms) que se tarda intentando bloquear al usuario que se va explorar. Cuando se realizan varias operaciones de exploración simultáneas en el mismo usuario y los recursos del usuario son lentos, el aumento de este valor puede reducir el número de errores de bloqueo, pero también puede ralentizar la exploración.
<code>scanDelay</code>	0	Indica el tiempo de demora (en ms) entre nuevos subprocesos de exploración. Se puede definir en un número positivo para que se utilicen menos recursos de la CPU durante la exploración.

- La descripción del elemento Disable se ha revisado. (ID-14920)

Calcula un valor booleano. Si es verdadero, el campo y todos sus campos anidados se ignoran durante el procesamiento del formulario.

No cree actividades que puedan tardar en ejecutarse en los elementos Disable. Estas expresiones se ejecutan cada vez que se recalcula el formulario. Realice el cálculo en otro elemento de formulario que no se ejecute con tanta frecuencia.

- En la sección “Inserting Javascript into a Form” se afirma por error que es posible incluir código JavaScript en los formularios con una etiqueta <JavaScript> (ID-15741). También se puede realizar como sigue:

```
<Field>
  <Expansion>
    <script>
    .....
```

NOTA Las variables `display.session` y `display.subject` no están disponibles para deshabilitar los elementos de formulario.

- Ahora es posible introducir mensajes de advertencia (WARNING), error (ERROR) o informativos (OK) en un formulario XPRESS. (ID-14540, ID-14953)

NOTA Aunque en este ejemplo se ilustra la forma de introducir un objeto `ErrorMessage` en un formulario, se le puede asignar un nivel de seguridad diferente.

1. Utilice el Identity Manager IDE para abrir el formulario al que quiera añadir la advertencia.
2. Añada `<Property name='messages' >` a la clase de presentación `EditForm` o `HtmlPage` principal.
3. Añada el bloque de código `<defvar name='msgList' >` del siguiente código de ejemplo.
4. En la cadena, sustituya la clave de mensaje que identifica el texto del mensaje que se va a mostrar en el cuadro de alerta:

```
<message name='UI_USER_REQUESTS_ACCOUNTID_NOT_FOUND_ALERT_VALUE >
```

5. Guarde y cierre el archivo.

Ejemplo de código

```
<Display class='EditForm'>
  <Property name='componentTableWidth' value='100%' />
  <Property name='secret' value='false'>
  <Property name='requiredMarkerLocation' value='left' />
  <Property name='messages'>
    <ref>msgList</ref>
  </Property>
</Display>
<defvar name='msgList'>
  <cond>
    <y 433>
      <nonnull>
        <ref>username</ref>
      </nonnull>
      <isnull>
        <ref>userview</ref>
      </isnull>
    </y>
    <list>
      <new class='com.waveset.msgcat.ErrorMessage'>
        <invoke class='com.waveset.msgcat.Severity' name='fromString'>
          <s>warning</s>
        </invoke>
        <message name='UI_USER_REQUESTS_ACCOUNTID_NOT_FOUND_ALERT_VALUE'>
          <ref>username</ref>
        </message>
      </new>
    </list>
  </cond>
</defvar>
```

Para que aparezca un nivel de seguridad distinto del de advertencia, sustituya `<s>warning</s>` en el ejemplo anterior por uno de estos dos valores:

- `error`: Hace que Identity Manager represente el componente `InlineAlert` con un icono de “error” de color rojo.
- `ok`: Se muestra un componente `InlineAlert` con un icono informativo de color azul en el caso de los mensajes satisfactorios o que no sean críticos.

Identity Manager representa esto como un componente `InlineAlert` con un icono de advertencia

```
<invoke class='com.waveset.msgcat.Severity' name='fromString'>
  <s>warning</s>
</invoke>
```

donde `warning` también puede ser `error` u `ok`.

Capítulo 4, Identity Manager Views (Vistas de Identity Manager)

- La descripción de la vista organizativa se ha actualizado así: (ID-13584)

Se utiliza para especificar el tipo de organización que se crea y las opciones con que se procesa.

Atributos comunes

La tabla siguiente muestra los atributos de nivel superior de la vista organizativa.

Nombre	¿Editable?	Tipo de datos	¿Requerido?
orgName	Leer	Cadena	Generado por sistema
orgDisplayName	Leer/Escribir	Cadena	Sí
orgType	Leer/Escribir	Cadena	No
orgId	Leer	Cadena	Generado por sistema
orgAction	Escribir	Cadena	No
orgNewDisplayName	Escribir	Cadena	No
orgParentName	Leer/Escribir	Cadena	No
orgChildOrgNames	Leer	Lista	Generado por sistema
orgApprovers	Leer/Escribir	Lista	No
allowsOrgApprovers	Leer	Lista	Generado por sistema
allowedOrgApproverIds	Leer	Lista	Generado por sistema
orgUserForm	Leer/Escribir	Cadena	No
orgViewUserForm	Leer/Escribir	Cadena	No
orgPolicies	Leer/Escribir	Lista	No
orgAuditPolicies	Leer/Escribir	Lista	No
renameCreate	Leer/Escribir	Cadena	No
renameSaveAs	Leer/Escribir	Cadena	No

orgName

Identifica el UID de la organización. Este valor se diferencia de la mayoría de los nombres de objeto de vista porque el nombre de las organizaciones puede adoptar la misma forma abreviada, pero sus organizaciones precursoras pueden ser distintas.

orgDisplayName

Especifica el nombre abreviado de la organización. Este valor sólo se utiliza en visualización y no tiene por qué ser único.

orgType

Define el tipo de organización, cuyos valores admitidos son `junction` o `virtual`. Las organizaciones que no son de tipo `junction` o `virtual` carecen de valor.

orgId

Especifica el ID que identifica a la organización en exclusiva dentro de Identity Manager.

orgAction

Sólo se admite con empalmes de directorios, organizaciones virtuales y organizaciones dinámicas. El valor permitido es `refresh`. Cuando una organización es virtual o un empalme de directorios, el comportamiento de la operación de regeneración depende del valor de `orgRefreshAllOrgsUserMembers`.

orgNewDisplayName

Especifica el nuevo nombre abreviado al renombrar la organización.

orgParentName

Identifica la ruta de acceso completa a la organización precursora.

orgChildOrgNames

Muestra una lista con los nombres de interfaz de Identity Manager de todas las organizaciones derivadas directas e indirectas.

orgApprovers

Muestra una lista con los administradores de Identity Manager necesarios para aprobar usuarios añadidos o modificados en esta organización.

allowedOrgApprovers

Muestra una lista con los posibles nombres de usuario que podrían actuar como aprobadores de los usuarios añadidos o modificados en esta organización.

allowedOrgApproverIds

Muestra una lista con los posibles ID de usuario que podrían actuar como aprobadores de los usuarios añadidos o modificados en esta organización.

orgUserForm

Especifica el formulario de usuario (`userForm`) que los afiliados de esta organización utilizan para crear o editar usuarios.

orgViewUserForm

Especifica el formulario de vista de usuario que los afiliados de esta organización utilizan para ver usuarios.

orgPolicies

Identifica las directivas que se aplican a todos los afiliados de esta organización. Se trata de una lista de objetos que se introducen mediante cadenas de tipo: Cada objeto de directiva contiene los siguientes atributos de vista, que llevan el prefijo `orgPolicies[<type>]`. `<type>` representa el tipo de directiva (por ejemplo, cuenta de Lighthouse).

- `policyName` -- Especifica el nombre
- `id` -- Indica el ID
- `implementation` -- Identifica la clase que implementa esta directiva.

orgAuditPolicies

Especifica las directivas de auditoría que se aplican a todos los afiliados de esta organización.

renameCreate

Cuando se define en `true`, clona esta organización en otra utilizando el valor de `orgNewDisplayName`.

renameSaveAs

Cuando se define en `true`, renombra esta organización utilizando el valor de `orgNewDisplayName`.

Atributos de empalme de directorios y organización virtual

Nombre	¿Editable?	Tipo de datos	¿Requerido?
<code>orgContainerId</code>	Leer	Cadena	Generado por sistema
<code>orgContainerTypes</code>	Leer	Lista	Generado por sistema
<code>orgContainers</code>	Leer	Lista	Generado por sistema
<code>orgParentContainerId</code>	Leer	Cadena	Generado por sistema
<code>orgResource</code>	Leer/Escribir	Cadena	Sí, en caso de empalme de directorios u organización virtual
<code>orgResourceType</code>	Leer	Cadena	Generado por sistema
<code>orgResourceId</code>	Leer	Cadena	Generado por sistema
<code>orgRefreshAllOrgsUserMembers</code>	Escribir	Cadena	No

orgContainerId

Especifica el dn del contenedor de directorio LDAP asociado (por ejemplo, cn=foo,ou=bar,o=foobar.com).

orgContainerTypes

Muestra una lista con todos los tipos de objetos de recurso permitidos que pueden contener otros objetos de recurso.

orgContainers

Muestra una lista con los contenedores básicos del recurso que la interfaz de Identity Manager utiliza para presentar una lista donde elegir.

orgParentContainerId

Especifica el dn del contenedor de directorio LDAP principal asociado (por ejemplo, cn=foo,ou=bar,o=foobar.com).

orgResource

Especifica el nombre del recurso de Identity Manager utilizado para sincronizar empalmes de directorios y organizaciones virtuales (por ejemplo, West Directory Server).

orgResourceType

Especifica el tipo de recurso de Identity Manager desde el que se sincronizan empalmes de directorios y organizaciones virtuales (por ejemplo, LDAP).

orgResourceId

Especifica el ID del recurso de Identity Manager utilizado para sincronizar empalmes de directorios y organizaciones virtuales.

orgRefreshAllOrgsUserMembers

Si se define en `true` y si el valor de `orgAction` es `refresh`, sincroniza la afiliación del usuario de la organización de Identity con la afiliación del contenedor de recursos para la organización seleccionada y todas las organizaciones derivadas. Si se define en `false`, no se sincronizará la afiliación del contenedor de recursos, sino únicamente los contenedores de recursos con las organizaciones de Identity para la organización seleccionada y todas las derivadas.

Atributos de organización dinámica

Nombre	¿Editable?	Tipo de datos	¿Requerido?
orgUserMembersRule	Leer/Escribir	Cadena	No
orgUserMembersRuleCacheTimeout	Leer/Escribir	Cadena	No

orgUserMembersRule

Identifica (por nombre o UID) la regla cuyo tipo de autorización (`authType`) es `UserMembersRule`, que se evalúa en tiempo de ejecución para determinar la afiliación del usuario.

orgUserMembersCacheTimeout

Especifica el tiempo transcurrido (en milésimas de segundo) antes de que se agote el tiempo de espera en caché si los afiliados devueltos por la regla `orgUserMembersRule` van a incluirse en caché. Un valor de 0 indica que no se incluye en caché.

En la actualidad, el análisis de la vista de usuario también está relacionado con los atributos `accounts[Lighthouse].delegates: (ID-15468)`

accounts[Lighthouse].delegates

Ofrece una lista de objetos delegados, clasificados por `workItemType`, en la que cada objeto incluye información concreta sobre un tipo de elemento de trabajo específico.

- Cuando el valor de `delegateApproversTo` es `delegatedApproversRule`, identifica la regla seleccionada.
- Este atributo no tiene valor cuando `manager` es el valor de `delegateApproversTo`.

accounts[Lighthouse].delegatesHistory

Ofrece una lista de objetos delegados, clasificados entre 0 y n , donde n corresponde al nivel máximo actual de historiales.

Este atributo sólo tiene un atributo, `selected`, que es un valor booleano que indica el objeto de historial actualmente seleccionado.

accounts[Lighthouse].delegatesOriginal

Después de una operación `get` o `checkout view`, ofrece la lista original de objetos delegados, clasificados por `workItemType`.

Todos los atributos `accounts[Lighthouse].delegates*` reciben los siguientes atributos:

Atributos de <code>accounts[Lighthouse].delegate*</code>	Descripción
<code>workItemType</code>	Identifica el tipo de elemento de trabajo que se delega. Para obtener una lista de tipos de elementos de trabajo válidos, consulte la descripción del modelo de objeto delegado en la sección <i>Identity Manager Technical Deployment Overview</i> de este anexo.

Atributos de <code>accounts[Lighthouse].delegate*</code>	Descripción
<code>workItemTypeObjects</code>	<p>Presenta una lista con los nombres concretos de los roles, los recursos o las organizaciones cuya solicitud futura de aprobación de elemento de trabajo piensa delegar el usuario. Este atributo es válido cuando el valor de <code>workItemType</code> es <code>roleApproval</code>, <code>resourceApproval</code> o <code>organizationApproval</code>.</p> <p>Si no se especifica, este atributo establece de forma predeterminada la delegación de solicitudes futuras de aprobación de elemento de trabajo relacionadas con roles, recursos u organizaciones de los que el usuario es aprobador.</p>
<code>toType</code>	<p>Tipo al que se va a delegar. Los valores válidos son:</p> <ul style="list-style-type: none"> <code>manager</code> <code>delegateWorkItemsRule</code> <code>selectedUsers</code>
<code>toUsers</code>	<p>Lista de los nombres de los usuarios en los que se delega (si <code>toType</code> es <code>selectedUsers</code>).</p>
<code>toRule</code>	<p>Especifica el nombre de la regla de evaluación que se empleará para determinar el conjunto de usuarios en el que se va a delegar (si <code>toType</code> es <code>delegateWorkItemsRule</code>).</p>
<code>startDate</code>	<p>Especifica la fecha de inicio de la delegación.</p>
<code>endDate</code>	<p>Especifica la fecha en la que termina la delegación.</p>

Referencia de un objeto `DelegateWorkItems` View de un formulario

En el siguiente ejemplo de código se ilustra la forma de hacer referencia a un objeto delegado `DelegateWorkItems` View desde un formulario.

```
<Field name='delegates[*].workItemType' >
<Field name='delegates[*].workItemTypeObjects' >
<Field name='delegates[*].toType' >
<Field name='delegates[*].toUsers' >
<Field name='delegates[*].toRule' >
<Field name='delegates[*].startDate' >
<Field name='delegates[*].endDate' >
```

donde los valores de índice (*) admitidos son valores `workItemType`.

- Este capítulo contiene la descripción de la vista de derechos de usuario siguiente:
Se usa para crear y modificar objetos de derecho de usuario.

Esta vista tiene los siguientes atributos de nivel superior:

Nombre	¿Editable?	Tipo	¿Requerido?
name		Cadena	Sí
status		Cadena	Sí
user		Cadena	Sí
userId		Cadena	Sí
attestorHint		Cadena	No
userView		GenericObject	Sí
reviewInstanceId		Cadena	Sí
reviewStartDate		Cadena	Sí
scanId		Cadena	Sí
scanInstanceId		Cadena	Sí
approvalWorkflowName		Cadena	Sí
organizationId		Cadena	Sí
attestorComments.name		Cadena	No
attestorComments.attestor		Cadena	No
attestorComments.time		Cadena	No
attestorComments.timestamp		Cadena	No
attestorComments.status			No

name

Identifica el derecho de usuario mediante un identificador exclusivo.

status

Especifica el estado del objeto de derecho de usuario. Los estados válidos incluyen PENDING (pendiente), ACCEPTED (aceptado), REJECTED (denegado), REMEDIATING (remediando) y CANCELLED (cancelado).

user

Identifica el nombre del WSUser asociado a este derecho.

userId

Especifica el ID del WSUser asociado.

attestorHint

Muestra al autenticador el truco (cadena) que ofrece la regla de determinación de revisión. Este truco sirve como consejo de la regla al autenticador.

userView

Contiene la vista de usuario que captura la operación de exploración de derechos de usuario. Esta vista contiene cero o más cuentas de recurso según la configuración del objeto de exploración de acceso.

reviewInstanceId

Especifica el ID de la instancia de la tarea PAR.

reviewStartDate

Indica la fecha de inicio (cadena) de la tarea PAR (en formato canónico).

scanId

Especifica el ID de la definición de tarea de exploración de acceso.

scanInstanceId

Especifica el ID de la instancia de tarea de exploración de acceso.

approvalWorkflowName

Identifica el nombre del flujo de trabajo que se debe ejecutar para aprobación. Este valor procede de la definición de tarea de exploración de acceso.

organizationId

Especifica el ID de la organización de WSUser en el momento de la exploración.

attestorComments

Muestra los registros de autenticación del derecho. Cada registro de autenticación indica una acción o instrucción efectuadas acerca del derecho, incluidas aprobación, denegación y reexploración.

attestorComments[timestamp].name

Indicación de tiempo utilizada para identificar este elemento en la lista.

attestorComments[timestamp].attestor

Identifica el nombre de WSUser del autenticador que comenta el derecho.

attestorComments[timestamp].time

Especifica la hora en que el autenticador autenticó este registro. Puede ser distinta a la indicación de tiempo.

attestorComments[timestamp].status

Indica el estado asignado por el autenticador. Puede ser cualquier cadena, pero suele indicar la acción realizada por el autenticador; por ejemplo, aprobar, denegar, reexplorar o remediar.

attestorComments[name].comment

Contiene comentarios introducidos por el autenticador.

- Se han desaprobado los siguientes atributos de vista de usuario. (ID-15468)
- `accounts[Lighthouse].delegateApproversTo`
- `accounts[Lighthouse].delegateApproversSelected`
- `accounts[Lighthouse].delegateApproversStartDate`
- `accounts[Lighthouse].delegateApproversEndDate`
- Aunque se ha desaprobado la vista de aprobadores delegados, sigue sirviendo para editar objetos delegados cuyo tipo de elemento (`workItemType`) es `approval`.

Los atributos `accounts[Lighthouse].delegate*` anteriores de vista de usuario se han desaprobado y ya no están disponibles con dicha vista. Utilice la nueva vista `accounts[Lighthouse].delegates`.

Capítulo 6, XPRESS Language (Lenguaje XPRESS)

Este capítulo se ha actualizado sustancialmente. Consulte el archivo `XPRESS.pdf`, incluido en el mismo directorio que estas Notas de la versión.

Capítulo 8, HTML Display Components (Componentes de visualización HTML)

- Este capítulo incorpora un análisis relacionado con una alternativa al componente `MultiSelect`:

Con el componente `MultiSelect` puede ser difícil mostrar varios roles de administración (ya se utilice la miniaplicación o la versión HTML). Identity Manager ofrece una forma más gradual de mostrar y administrar los roles de administración: la plantilla de campo `objectSelector`. (ID-15433)

La biblioteca de selección escalable (`sample/formlib.xml`) incluye un ejemplo de cómo utilizar la plantilla `objectSelector` para buscar nombres de roles de administración que el usuario pueda utilizar.

Ejemplo de código**Ejemplo de objectSelector**

```

<Field name='scalableWaveset.adminRoles'>
  <FieldRef name='objectSelector'>
    <Property name='selectorTitle' value=' FM_ADMIN_ROLES'/>
    <Property name='selectorFieldName' value='waveset.adminRoles'/>
    <Property name='selectorObjectType' value='AdminRole'/>
    <Property name='selectorMultiValued' value='true'/>
    <Property name='selectorAllowManualEntry' value='true'/>
    <Property name='selectorFixedConditions'>
      <appendAll>
        <new class='com.waveset.object.AttributeCondition'>
          <s>hidden</s>
          <s>notEquals</s>
          <s>true</s>
        </new>
        <map>
          <s>onlyAssignedToCurrentSubject</s>
          <Boolean>true</Boolean>
        </map>
      </appendAll>
    </Property>
    <Property name='selectorFixedInclusions'>
      <appendAll>
        <ref>waveset.original.adminRoles</ref>
      </appendAll>
    </Property>
  </FieldRef>
</Field>

```

Cómo utilizar el código de ejemplo de objectSelector

1. En el Identity Manager IDE, abra el objeto de formulario de usuario de la biblioteca del administrador.
2. Añada el código siguiente a este formulario:

```

<Include>
  <ObjectRef type='UserForm' name='Scalable Selection Library'/>
</Include>

```

3. Seleccione el campo `accounts [Lighthouse] .adminRoles` en el campo `AdministratorFields`.
4. Sustituya `accounts [Lighthouse] .adminRoles` por la referencia siguiente:

```

<FieldRef name='scalableWaveset.adminRoles'/>

```

5. Guarde el objeto.

Cuando después modifique un usuario y seleccione la ficha de seguridad, Identity Manager presentará el formulario personalizado. Cuando haga clic en ... se abrirá el componente Selector y aparecerá un campo de búsqueda. Utilice este campo para buscar roles de administración que empiecen con una cadena de texto y defina el campo en uno o varios valores.

Para restaurar el formulario, importe el archivo `$WSHOME/sample/formlib.xml` mediante el uso del menú **Configurar > Importar fichero de intercambio**.

Consulte la biblioteca de selección escalable del archivo `sample/formlib.xml` para ver otros ejemplos de cómo utilizar la plantilla `objectSelector` para administrar recursos y roles en entornos con muchos objetos.

- La sección relacionada con el componente `TabPanel` incluye la siguiente descripción de la propiedad `validatePerTab`: (ID-15501)

`validatePerTab`: Cuando se define como `true`, Identity Manager ejecuta expresiones de validación en cuanto el usuario cambia a una ficha diferente.

- La sección dedicada al componente `MultiSelect` incluye esta descripción de la propiedad `displayCase`: (ID-14854)

`displayCase`: Asigna los valores admitidos a sus equivalentes en mayúscula o minúscula y adopta uno de ellos (mayúscula o minúscula).

- A este capítulo se ha añadido la información sobre el componente `Menu` que se expone a continuación: (ID-13043)

Consta de tres clases: `Menu`, `MenuBar` y `MenuItem`.

- `Menu` hace referencia a todo el componente.
- `MenuItem` es una página, o nodo, que corresponde a una ficha del primer o segundo nivel.
- `MenuBar` corresponde a una ficha que contiene varios `MenuBar` o `MenuItems`.

`Menu` contiene las siguientes propiedades:

- `layout`: Cadena con valor `horizontal` o `vertical`. El valor `horizontal` genera una barra de navegación horizontal con fichas. El valor `vertical` hace que el menú se represente como un árbol vertical con la típica estructura nodal.
- `stylePrefix`: Prefijo de cadena correspondiente al nombre de clase de las hojas de estilo en cascada. El valor es `User` para las páginas de usuario final de Identity Manager.

MenuBar contiene las siguientes propiedades:

- default: Ruta URL que corresponde a una de las propiedades MenuItem URL de MenuBar. Controla la subficha que se muestra de forma predeterminada como seleccionado cuando se hace clic en la ficha MenuBar.

MenuItem contiene las siguientes propiedades:

- containedUrls: Lista de rutas URL de acceso a JSP que están “relacionadas” con MenuItem. El elemento MenuItem actual aparecerá como “seleccionado” si se representa alguna de las páginas de Java Server (JSP) de containedUrls. Un ejemplo es la página de resultados de petición de inicio que aparece después de iniciar un flujo de trabajo desde la página de petición de inicio.

Estas propiedades se pueden definir en MenuBar o MenuItem:

- title: Especifica la cadena de texto que aparece como hipervínculo en la ficha o estructura de árbol.
- URL: Especifica la ruta URL correspondiente al hipervínculo del título.

En el siguiente ejemplo de la función XPRESS se crea un menú con dos fichas. La segunda ficha contiene a su vez dos subfichas:

Ejemplo de código 5-4 Implementación de los componentes Menu, MenuItem y MenuBar

```
<Display class='Menu' />
<Field>
  <Display class='MenuItem'>
    <Property name='URL' value='user/main.jsp' />
    <Property name='title' value='Home' />
  </Display>
</Field>
<Field>
  <Display class='MenuBar' >
    <Property name='title' value='Work Items' />
    <Property name='URL' value='user/workItemListExt.jsp' />
  </Display>
  <Field>
    <Display class='MenuItem'>
      <Property name='URL' value='user/workItemListExt.jsp' />
      <Property name='title' value='Approvals' />
    </Display>
  </Field>
  <Field>
    <Display class='MenuItem'>
      <Property name='URL' value='user/otherWorkItems/listOtherWorkItems.jsp' />
      <Property name='title' value='Other' />
    </Display>
  </Field>
</Field>
```

Apéndice A, Form and Process Mappings (Asignaciones de formularios y procesos)

- Hay una versión actualizada de este apéndice (Form and Process Mappings) en el mismo directorio que estas Notas de la versión.
- A través de los nombres asignados es posible acceder a tareas específicamente relacionadas con el cumplimiento. (ID-15447)

Nombre del proceso	Nombre asignado	Descripción
Revisión de acceso 220	accessReview	Realiza una revisión de acceso.
Exploración de acceso	accessReviewScan	Realiza una exploración de acceso.
Reexploración de revisión de acceso	accessReviewRescan	Realiza una reexploración de acceso.
Reexploración de directiva de auditoría	auditPolicyRescan	Realiza una reexploración de directiva de auditoría.
Anular revisión de acceso	abortAccessReview	Termina una revisión de acceso.
Eliminar revisión de acceso	deleteAccessReview	Elimina una revisión de acceso.
Recuperar revisión de acceso	recoverAccessReview	Recupera los objetos de estado de revisión de acceso que faltan de los registros de auditoría.

Identity Manager Deployment Tools

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager Deployment Tools*:

Novedades

El manual *Identity Manager Deployment Tools* contiene importante información nueva en los capítulos siguientes:

- El capítulo 1, “Using the Identity Manager IDE”, se ha actualizado para ofrecer información sobre las siguientes funciones y características nuevas:
 - El proceso para crear proyectos de Identity Manager IDE y trabajar con ellos se ha actualizado con el fin de proporcionar dos tipos de proyectos (ID-14587):
 - En Identity Manager, el proyecto es un entorno de desarrollo básico para desarrolladores que dispone de todas las funciones.
 - En Identity Manager, el proyecto (remoto) sirve para realizar pequeñas modificaciones y para efectuar depuraciones en un servidor externo.

- Los proyectos del Identity Manager IDE se integran en un entorno de compilación de configuración (CBE) (ID-14980).
- En la actualidad hay un menú IdM en la barra de menús de nivel superior de NetBean, desde donde se pueden seleccionar acciones apropiadas para los nodos de objetos seleccionados. (ID-14787)
- Los objetos de la biblioteca, que disponen de hojas de propiedades, funciones de paleta y nodos de navegación, se han añadido a la lista de tipos de objetos que aparecen en la ventana del Explorador. (ID-14817)
- Cuando se selecciona la vista de diseño de un objeto de regla, en la ventana del editor aparece un generador de expresiones que permite distinguir con facilidad la estructura lógica de la regla y modificar sus propiedades. (ID-15104)
- Ahora se pueden comparar objetos (diff) de un directorio local con los del repositorio. (ID-15206)
- El proceso para probar los formularios y las reglas ha cambiado. La opción *Form Previewer* ha cambiado de nombre y ahora se denomina *Form Tester*. (ID-15325)
- Los cuadros de diálogo del generador de expresiones del Identity Manager IDE incorporan nuevas funciones:
 - Es posible modificar tipos de datos simples (enteros y cadenas) directamente en la tabla del generador de expresiones. (ID-15528)
 - En lugar de crear primero un BLOQUE para después convertirlo en la expresión deseada, se puede crear una expresión concreta. (ID-15932)
 - Se ha creado un nuevo botón *Change To* con cuadro de diálogo asociado para cambiar el tipo de expresión de un elemento. (ID-15933)
 - Ahora es posible editar valores de propiedades que admiten expresiones y primitivas (como cadenas) directamente en una tabla de propiedades. (ID-15528)
 - Al definir sentencias de invocación de XPRESS estáticas o de instancia en el generador de expresiones, es posible ver la información de JavaDoc relacionada para los métodos de API de Identity Manager. Para acceder a este JavaDoc, pase el cursor sobre los métodos incluidos en los menús de nombre de método; aparecerá una ventana con la información.
- En la actualidad es necesario utilizar JDK 1.5 y Netbeans 5.5 con el plugin de Identity Manager IDE. (ID-14950)
- Los objetos del repositorio del Identity Manager IDE se pueden eliminar. (ID-15031)
- Es posible transferir un objeto del IDE a un servidor de Identity Manager 7.0 y asignarle un ID de objeto manualmente. (ID-15474)

- Se puede hacer clic con el botón secundario en un árbol de proyecto y abrir objetos a los que hacen referencia ciertas referencias (como ObjectRefs, FormRefs, FieldRefs y Workflow Subprocesses). (ID-15406)
- También se han realizado otros cambios menores en la interfaz de usuario y en los procesos.
- La sección “*Auditor Rules*” (Reglas de auditor) del capítulo 2, “*Working with Rules*”, se ha actualizado para proporcionar información más detallada sobre las reglas de Identity Auditor. (ID-15367, 15496, 15609, 15934, 16166, 16263 y 16292)
- El capítulo 7, “*Using SPML 1.0 with Identity Manager Web Services*”, se ha actualizado para que incluya información sobre la interfaz SPML de SPE. (ID-14458)
- La sección “*Using Trace in SPML*” (Seguimiento en SPML) del capítulo 7, “*Using SPML 1.0 with Identity Manager Web Services*,” se ha actualizado con el fin de ofrecer información adicional sobre la forma de habilitar la salida de seguimiento para que sea posible registrar el tráfico SPML de Identity Manager y diagnosticar problemas. (ID-15346)
- La sección “*Using Trace in SPML*” (Seguimiento en SPML) del capítulo 8, “*Using SPML 2.0 with Identity Manager Web Services*,” se ha actualizado con el fin de ofrecer información adicional sobre la forma de habilitar la salida de seguimiento para que sea posible registrar el tráfico SPML de Identity Manager y diagnosticar problemas. (ID-15346)

Actualizaciones

Esta sección contiene las correcciones y los anexos a la documentación *Identity Manager Deployment Tools*:

- Las secciones “*Palette Window*” (Ventana de paleta) y “*Properties Window*” (Ventana de propiedades) del capítulo 1, “*Using the Identity Manager IDE*” deberían incluir *GenericObjects* en la lista de elementos suministrados en el primer párrafo de ambas secciones, como sigue: (ID-14817)
 - La ventana de paleta (como en la figura 1-11) permite arrastrar y soltar elementos en objetos de plantilla de correo electrónico, formulario, *GenericObjects*, biblioteca, proceso de flujo de trabajo o subproceso de flujo de trabajo mostrados en las ventanas de Editor, sin necesidad de escribir XML.
 - La ventana de propiedades de Identity Manager IDE está formada por una hoja de propiedades para elementos XML asociados a objetos de plantilla de correo electrónico, formulario, *GenericObjects*, biblioteca, proceso de flujo de trabajo o subproceso de flujo de trabajo. Esta hoja de propiedades puede servirle para ver y editar las propiedades de un objeto seleccionado, incluido su nombre, tamaños de archivo, tiempos de modificación, información resultante, etc.

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

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager Tuning, Troubleshooting, and Error Messages*.

- Ahora se ofrece información sobre el tamaño de los objetos del repositorio (en número de caracteres). Esta información permite detectar objetos con problemas de exceso de tamaño que podrían afectar al sistema. (ID-9896, ID-15239)

A esta información se accede desde la página Web debug/Show_Sizes.jsp o introduciendo lo siguiente en la línea de comando:

```
showSizes [<type> [<limit>]]
```

NOTA Cuando se realicen actualizaciones, los objetos existentes presentarán un tamaño 0 hasta que se hayan actualizado.

- Algunas tareas se han trasladado desde el adaptador hasta el paquete de tareas. Estas rutas se tienen que actualizar cuando se habilita el seguimiento de cualquiera de las tareas siguientes o cuando existen definiciones de tareas personalizadas que hacen referencia a estos paquetes.

Nombre de paquete anterior	Nombre de paquete nuevo
com.waveset.adapter.ADSyncFailoverTask	com.waveset.task.ADSyncFailoverTask
com.waveset.adapter.ADSyncRecoveryCollectorTask	com.waveset.task.ADSyncRecoveryCollectorTask
com.waveset.adapter.SARunner	com.waveset.task.SARunner
com.waveset.adapter.SourceAdapterTask	com.waveset.task.SourceAdapterTask

Implementación de Identity Manager Service Provider Edition

Esta sección contiene información nueva y corregida relacionada con el documento *Sun Java(TM) System Identity Manager SPE Deployment*.

Capítulo 5, Other Objects in Identity Manager SPE (Otros objetos en Identity Manager SPE)

Identity Manager Identity Manager SPE admite reglas de correlación y confirmación de vínculo.

Regla de correlación de vínculo

La opción `linkTargets` de la vista de `IDMXUser` permite al llamador especificar la lista de recursos que deberían ser objeto de la vinculación. Cuando se utilizan formularios, la lista puede presentarse como una propiedad de formulario con el mismo nombre. Las propiedades de formulario se incorporan a las opciones de la vista cuando se registra la vista de `IDMXUser`.

Una regla de correlación de vínculo selecciona las cuentas de recurso que puede tener el usuario. Para la vista de usuario, la regla de correlación devuelve una identidad, una lista de identidades o una asignación de opciones.

Si la regla devuelve una asignación de opciones, el controlador de la vista utiliza dicha asignación para buscar las cuentas de recurso y obtiene una lista de las identidades que cumplen esas opciones. Por ejemplo, la opción `searchFilter` del método `getResourceObjects` `FormUtil` sirve para transferir un filtro de búsqueda al adaptador de recursos LDAP.

En la regla de correlación de vínculo, el atributo `authType` debe estar configurado en `SPERule` y `subtype` en `SUBTYPE_SPE_LINK_CORRELATION_RULE`.

Regla de confirmación de vínculo

Una regla de confirmación de vínculo elimina todas las cuentas de recurso de la lista de posibles cuentas seleccionadas por la regla de correlación de vínculo. Para la vista de usuario y la lista de cuentas de recursos posibles, a regla de vínculo selecciona como máximo una cuenta de la lista. A la vista del usuario se accede mediante la ruta "view", mientras que la lista de posibles cuentas se encuentra disponible en "candidates".

Si la regla de correlación de vínculo selecciona una sola cuenta de recurso, no es necesaria la regla de confirmación de vínculo.

NOTA A diferencia de las reglas de confirmación de Identity Manager, sólo se llama a las reglas de confirmación de vínculo durante el proceso de vinculación.

En la regla de confirmación de vínculo, el atributo `authType` debe estar configurado en `SPERule` y `subtype` en `SUBTYPE_SPE_LINK_CONFIRMATION_RULE`.

API de LighthouseContext

A la clase `SessionFactory` se han añadido varios métodos útiles. La tabla de la página 16 debería actualizarse como sigue.

Tipo de conexión	Método	Descripción
Local anónima	<code>getServerInternalContext()</code>	Devuelve un contexto completamente autorizado sin autenticación.
Local autenticada	<code>getSPESession(String user, EncryptedData password)</code>	Crea una sesión para la interfaz de usuario de Service Provider.
Local autenticada	<code>getSPESession(Map credentials)</code>	Crea una sesión para la interfaz de usuario de Service Provider. La asignación especifica las credenciales del usuario, incluidas las claves y contraseñas de usuario.
Local preautenticada	<code>getSPEPreAuthenticatedSession(String user)</code>	Crea una sesión preautenticada para la interfaz de usuario de Service Provider.
Remota anónima	No aplicable	Este tipo de conexión sólo está disponible en SPML.
Remota autenticada	<code>getSession(URL url, String user, EncryptedData pass)</code>	Devuelve una sesión autenticada.

Ámbito de localización

Históricamente, en Identity Manager no se localizan las funciones y los objetos de recurso, porque son principalmente ejemplos que se cargan (mediante `init.xml`) durante la inicialización de Identity Manager y porque los atributos de tipo de objeto pueden variar de una a otra implementación de cliente según el nivel de personalización. A continuación se indican áreas que pueden aparecer en inglés: (ID-16349)

- Formularios de usuario y asignaciones de procesos predeterminados
 - **Ejemplo:** Menús desplegables Editar usuario > Seguridad > Formulario de usuario
 - **Ejemplo:** Configurar > Asignaciones de formularios y procesos
- Nombres de atributo de objetos de configuración

Ejemplo: Configurar > Interfaz de usuario, nombres concatenados como `displayPasswordExpirationWarning`
- Tareas predeterminadas
 - Plantillas de tarea

Ejemplo: Tareas del servidor > Configurar tareas > nombres de plantillas de tarea disponibles en la tabla
 - Etiquetas de tipo de tarea

Ejemplo: Tareas del servidor > Ejecutar tareas > elementos de la segunda columna de la tabla Tareas disponibles
 - Definiciones de tareas

Ejemplo: Tareas de servidor > Buscar tareas > segundo menú desplegable para seleccionar Definición de tarea
- Nombres de informe predeterminado

Ejemplo: Nombres de informe en Informes > Ejecutar informes > Tabla de informe
- Nombres de directiva predeterminados

Ejemplo: Cumplimiento > Administrar directivas > nombres y descripciones de directivas de auditoría
- Nombres de capacidad predeterminados

Ejemplo: Editar usuario > Seguridad > Capacidades disponibles
- Nombres de informes y gráficos predeterminados
- Miniaplicaciones diagramas de procesos/ flujos de trabajo

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.

- **Archivo 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:

- o **Directorio de destino:** `html/docs`
- o **Archivos de entrada:** `../doc/HTML/en_US`

NOTA La herramienta copiará el directorio `en_US/` y los subdirectorios en el destino.

- o **Directorio de índice Nova:** `index/docs`
- o **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.

- o **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/2005:13:24:25] PM Making meta file: index/docs/MF: 0
[15/Dec/2005:13:24:25] PM Created active file: index/docs/AL
[15/Dec/2005:13:24:28] MP Partition: 1, 192 documents, 38488 terms.
[15/Dec/2005:13:24:29] MP Finished dumping: 1 index/docs 0.617
[15/Dec/2005:13:24:29] IS 192 documents, 14.70 MB, 3.81 s, 13900.78 MB/h
[15/Dec/2005:13:24:29] PM Waiting for housekeeper to finish
[15/Dec/2005:13:24:30] PM Shutdown index/docs AWord 1252155067
```