CA Identity Manager

Notas de la versión

r12

Referencias a productos de CA

Este documento hace referencia a los siguientes productos de CA:

- CA Identity Manager
- Web Access Manager de CA SiteMinder®
- CA Security Command Center (SCC)
- CA Audit
- eTrust® Directory, también denominado CA Directory

Cómo ponerse en contacto con el servicio de asistencia al cliente

Si desea obtener asistencia técnica en línea y una lista completa de oficinas, horas principales de atención y números de teléfono, póngase en contacto con el servicio de asistencia al cliente en http://www.ca.com/worldwide.

Contenido

Capítulo 7: Documentación 71

Capítulo 1: Bienvenida

Este documento contiene consideraciones sobre la instalación del producto, la compatibilidad con sistemas operativos, problemas conocidos e información de contacto con el Soporte técnico de CA.

Capítulo 2: Nuevas funciones

Esta sección contiene los siguientes puntos:

Versiones y plataformas compatibles

En Identity Manager r12, se han realizado algunas adiciones a las versiones, directorios y bases de datos del servidor de aplicaciones compatibles.

Nota: Para obtener una lista completa de plataformas y versiones compatibles, consulte la matriz de soporte Identity Manager del sitio web de asistencia de Identity Manager http://ca.com/support.

Arquitectura de Identity Manager

La arquitectura de Identity Manager r12 incluye los siguientes cambios con respecto a las versiones anteriores:

- **Servidor de aprovisionamiento y Gestor de aprovisionamiento integrados**

  El servidor de aprovisionamiento es el servidor que gestiona las cuentas adicionales que se asignan a un usuario de Identity Manager. Al asignar una función de aprovisionamiento a un usuario de Identity Manager, el servidor de aprovisionamiento crea cuentas en extremos que cumplen los requisitos de la función. Por ejemplo, si se asigna una función de aprovisionamiento que incluya una plantilla de cuenta de Exchange, el servidor de aprovisionamiento asignará al usuario una cuenta de Exchange.

  El Gestor de aprovisionamiento es la interfaz de usuario utilizada para gestionar los tipos de extremos (como por ejemplo Exchange u Oracle) y los extremos (como por ejemplo el sistema concreto en el que está instalado Exchange). Anteriormente, esta interfaz se denominaba eTrust Admin Manager. El Gestor de aprovisionamiento incluye otras capacidades, tales como la exploración y la correlación de cuentas. Sin embargo, estas funciones están duplicadas en la consola de usuario de Identity Manager, desde la que se puede acceder a ellas más fácilmente.

  Las versiones anteriores de Identity Manager necesitaban eTrust Admin para el aprovisionamiento.

  Nota: El servidor de aprovisionamiento y el Gestor de aprovisionamiento son componentes opcionales.

- **Integración de Identity Manager con SiteMinder**

  SiteMinder ya no es un requisito para la instalación de Identity Manager. Ahora, la integración con SiteMinder es opcional y está dedicada a ofrecer funciones avanzadas, como la autenticación de SiteMinder y políticas de contraseñas avanzadas.

  Las versiones anteriores de Identity Manager necesitaban SiteMinder para las siguientes funciones:

  – Autenticación

  – Almacenamiento de la información de las funciones y tareas (en el almacén de políticas).

  – Conexión a un almacén de usuarios

  – Políticas de contraseñas

  En Identity Manager, esta función se proporciona de forma nativa.

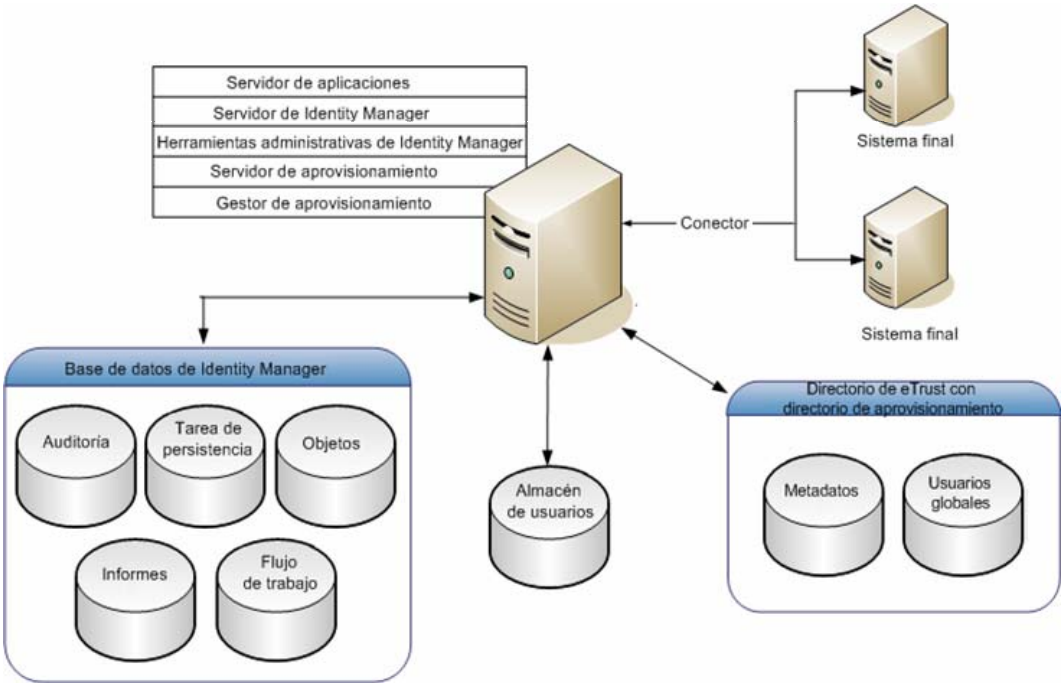
  Nota: Puede realizar la integración con SiteMinder para proporcionar funciones avanzadas, como la autenticación de SiteMinder y políticas de contraseñas avanzadas.

- **Almacén de objetos**

  Ahora, Identity Manager r12 almacena información de tareas y funciones en un nuevo almacén de objetos. El almacén de objetos es una base de datos relacional que Identity Manager configura automáticamente en tiempo de ejecución.

La siguiente ilustración muestra una implementación de Identity Manager que incluye aprovisionamiento.

Nota: El directorio de aprovisionamiento, que almacena la información necesaria para utilizar el aprovisionamiento e información sobre los usuarios globales, se debe instalar en eTrust Directory. Este es un requisito para la instalación de Identity Manager con aprovisionamiento.



Mejoras del instalador

Ahora, todos los componentes necesarios para la instalación del servidor de Identity Manager se instalan con un instalador. Este instalador incluye componentes para el aprovisionamiento y extensiones para el servidor de políticas de SiteMinder.

El instalador de Identity Manager proporciona el servidor de aprovisionamiento de Identity Manager, el directorio de aprovisionamiento y el Gestor de aprovisionamiento. También configura las conexiones con las bases de datos que almacenan datos de objeto y datos para el flujo de trabajo, persistencia de tareas, informes y auditoria.

Estos son algunos de los cambios realizados en la instalación de Identity Manager:

- Identity Manager ya no necesita SiteMinder para la autenticación.
- La persistencia de tareas ya no es opcional y se activa tras la instalación.
- El esquema de base de datos se amplía automáticamente para todas las bases de datos que utiliza Identity Manager.
- Las herramientas administrativas ahora se instalan en las siguientes ubicaciones:
  - **Windows:** C:\Archivos de programa\CA\IAM Suite\Identity Manager\tools
  - **UNIX:** *HOME*/CA/IAM_Suite/Identity_Manager/tools
- Ya no se necesitan secuencias de comandos posteriores a la instalación.

Mejoras de los informes

Los informes de Identity Manager le permiten ver el estado actual de un entorno de Identity Manager. Puede utilizar esta información para garantizar la conformidad con las políticas del negocio internas o las normativas externas.

Identity Manager r12 incluye las siguientes mejoras para los informes:

- **Integración con el servidor de informes de IAM**

  Identity Manager r12 utiliza Business Objects Enterprise XI para diseñar, gestionar y ver los informes de la base de datos de informes. Identity Manager proporciona una versión en tiempo de ejecución de Business Objects, de modo que no se necesita una licencia independiente.

- **Nuevas tareas de administración para exportar datos a la base de datos de informes**

  Identity Manager incluye nuevas tareas predeterminadas, que permiten exportar datos desde Identity Manager a la base de datos de informes. Cada vez que se exportan datos a la base de datos de informes, se crea una *instantánea*, es decir, una representación del estado actual de los objetos especificados por el usuario en un entorno Identity Manager.

  Mediante las nuevas tareas predeterminadas, se pueden crear definiciones de instantáneas y capturar una instantánea a partir la cual se puede generar un informe.

- **Otros Informes predefinidos**

  Identity Manager incluye los siguientes informes predefinidos, que se pueden utilizar tal y como se instalan o que se pueden personalizar para adaptarlos a las necesidades del negocio:

  - **Cuentas de extremos**

    Lista de las cuentas por nombre de cuenta, propietario y hora de creación para cada extremo, ordenadas por tipo de extremo.

  - **Cuentas no estándar**

    Lista de las cuentas no estándar, tales como cuentas huérfanas y cuentas del sistema.

  - **Tendencias de las cuentas no estándar**

    Tendencias de las cuentas no estándar por tipo de cuenta no estándar mostradas como gráficos.

  - **Cuentas huérfanas**

    Lista de las cuentas que no están asociadas con un usuario. Las cuentas huérfanas se enumeran por nombre de cuenta, propietario y hora de creación para cada extremo y se ordenan por tipo de extremo.

  - **Políticas**

    Lista de las políticas, incluyendo las condiciones de las políticas y las acciones Acción al aplicar y Acción al eliminar.

  - **Administradores de funciones**

    Lista de los administradores de las funciones.

  - **Miembros de funciones**

    Lista de los miembros de las funciones.

  - **Propietarios de funciones**

    Lista de los propietarios de las funciones.

  - **Funciones**

    Lista de las funciones y sus descripciones.

  - **Instantáneas**

    Lista de todas las instantáneas disponibles en la base de datos de informes.

  - **Funciones de tareas**

    Lista de las tareas por descripción, categoría y tipo. Para cada tarea, se especifican todas las funciones asociadas.

- **Cuentas de usuario**

  Lista de las cuentas por usuario. Las cuentas de usuario se enumeran por nombre de la cuenta, atributos de la cuenta y extremo, ordenadas por tipo de extremo.

- **Estado de la sincronización de las políticas de usuario**

  Lista de los usuarios, que incluye las políticas que están asignadas actualmente y las políticas que se deben reasignar.

- **Perfil de usuario**

  Lista de los usuarios con toda la información disponible sobre ellos.

- **Derechos del usuario**

  Lista de los usuarios y sus cuentas, funciones y grupos asociados.

Gestión de la conexión

La gestión de la conexión se utiliza para configurar los detalles de la conexión del servidor de base de datos en Identity Manager. Cuando Identity Manager se tiene que conectar a un servidor de base de datos, utiliza los detalles de la conexión para conectarse al servidor de base de datos. La gestión de la conexión permite crear varias conexiones a distintos servidores de base de datos bajo un tipo de conexión. Por cada tipo de conexión se puede especificar una conexión predeterminada. Es necesario configurar un tipo de conexión primario para Identity Manager mediante la Consola de gestión.

Mejoras del aprovisionamiento

En esta versión, se pueden realizar más acciones en la Consola de usuario de Identity Manager. Algunas de estas capacidades ya estaban disponibles en eTrust Admin Manager. Se puede utilizar la Consola de usuario para:

- Explorar y correlacionar cuentas en extremos.
- Correlacionar cuentas huérfanas y cuentas del sistema con un usuario de Identity Manager.
- Auditar acciones de aprovisionamiento, tales como asignar una función de aprovisionamiento a un usuario global.

Además, esta versión incluye:

- Connector Xpress, una herramienta gráfica para crear conectores personalizados.
- Compatibilidad con conectores dinámicos (JNDI y JDBC) para ser utilizados con metadatos XML generados con Connector Xpress.

- Servidor de conector de Java, un servidor que gestiona las solicitudes de los conectores Java.
- Funciones de alta disponibilidad para el servidor de conector de C++, anteriormente denominado Superagente.
- Nuevos conectores de Java para Kerberos para administrar los directores de Kerberos y las políticas de contraseñas de Kerberos en servidores Solaris.
- Nuevos conectores Java para SAP (con compatibilidad CUA).
- Nuevos conectores Java para Oracle, MS-SQL y 0S/400, suministrados con el servidor de conector de Java.

  Estos tres conectores sustituyen las opciones de muestra, que ya no se admiten.
- El Gestor de aprovisionamiento se ha mejorado para proporcionar una interfaz de usuario genérica para tipos de extremos dinámicos JDBC y JNDI creados mediante Connector Xpress.

Interfaz gráfica de usuario de conectores dinámicos

Se ha mejorado la interfaz gráfica de usuario de conectores dinámicos en el Gestor de aprovisionamiento para proporcionar un conjunto mejorado de funciones que permiten manipular objetos de extremo arbitrarios con un único complemento del Gestor de aprovisionamiento.

Por ejemplo, cuando se asigna un campo en Connector Xpress, se coloca un elemento en los metadatos para representar dicho campo. Siempre que se examine cualquier objeto de ese conector, la interfaz gráfica de usuario de conectores dinámicos utilizará los metadatos para mostrar los campos apropiados.

Los cambios en esta versión amplían las capacidades de la interfaz gráfica de usuario de conectores dinámicos con un conjunto mejorado de funciones, facilitan la futura adición de nuevas funciones y proporcionan una mejor presentación para el usuario.

El conector de Lotus Notes/Domino se publica como una tecnología sin desarrollar

Para la versión r12 de Identity Manager, el conector de LND basado en Java se publica sólo como una tecnología sin desarrollar.

Dicho conector **no** está certificado para entornos de producción. El conector certificado estará disponible en una CR. Póngase se en contacto con el representante de la cuenta de CA para obtener más información.

Nota: No instale el conector de LND de C++ ni el conector de LNS basado en Java en el mismo Identity Manager entorno.

Informes de estado mejorados

Identity Manager r12 incluye varias funciones que permiten ver el estado de las tareas de Identity Manager.

Mejoras de la visualización de las tareas enviadas

Identity Manager r12 incluye la ficha Ver tareas enviadas, que permite ver el estado de una tarea, la dependencia de una tarea con respecto a otras tareas, otros eventos y el flujo de trabajo.

En Identity Manager r12, la ficha Ver tareas enviadas incluye las siguientes mejoras:

- La ficha Ver tareas enviadas muestra ahora más detalles sobre las tareas y los eventos asociados.
- Desde la ficha Ver tareas enviadas, se pueden cancelar tareas pendientes y volver a enviar o rechazar las tareas erróneas.
- Ahora se puede configurar la ficha Ver tareas enviadas.

La tarea Ver actividad del usuario

La actividad del usuario comprende un historial de las tareas relacionadas con un determinado usuario. Los administradores pueden utilizar la tarea Ver actividad del usuario para hacer un seguimiento de la siguiente información:

- Tareas realizadas en el usuario
- Tareas realizadas por el usuario
- Aprobaciones de flujo de trabajo realizadas por el usuario

Para ver la actividad del usuario

1. Haga clic en Usuarios, Gestionar usuarios, Ver actividad del usuario.

   Aparecerá la pantalla Seleccionar usuario.

2. Busque un usuario y haga clic en Seleccionar.

   Aparecerá la pantalla Ver actividad del usuario.

   Para obtener más información sobre las actividades del usuario que se muestran, consulte la *Ayuda en línea de la consola de usuario*.

Ficha Historial del usuario

La ficha Historial del usuario permite ver las tareas relacionadas con un usuario. Esta ficha se puede agregar a la tarea Modificar o Ver usuario.

Nota: Esta ficha se incluye en la tarea predeterminada Ver actividad del usuario.

Los detalles de la tarea que se muestran en esta ficha también se pueden ver en la ficha Ver tareas enviadas.

Mejoras del flujo de trabajo

Identity Manager r12 incluye mejoras en las funciones de flujo de trabajo. Estas mejoras simplifican el proceso de creación de flujos de trabajo y agregan nuevas funciones. Las siguientes secciones describen las mejoras.

Plantillas de proceso del flujo de trabajo

Las plantillas de proceso del flujo de trabajo permiten configurar y gestionar el control del flujo de trabajo completamente desde la consola de usuario de Identity Manager. Estas plantillas de proceso genéricas se pueden configurar para controlar la mayoría de tareas y eventos de Identity Manager.

Las nuevas plantillas de proceso permiten controlar el flujo de trabajo a nivel de tareas y a nivel de eventos, facilitan la configuración de resolvedores de participantes para los aprobadores y permiten los procesos de aprobación en varias etapas.

La lista de aprobadores también se puede determinar dinámicamente en tiempo de ejecución, en función de los atributos de la tarea o evento que se estén aprobando.

Flujo de trabajo a nivel de tarea

Los procesos de flujo de trabajo se pueden asociar con tareas y con eventos. Esto significa que los participantes pueden aprobar o rechazar toda una tarea de Identity Manager o un evento específico de una tarea.

El flujo de trabajo a nivel de tarea permite a los participantes revisar todos los eventos antes de decidir si aprueban o rechazan una solicitud. Cuando un proceso de flujo de trabajo se asocia con un evento determinado de una tarea, un aprobador no puede ver el contexto global de la tarea dentro del que se realiza una solicitud.

Botones de acción del flujo de trabajo

Se pueden añadir nuevos botones a las tareas de aprobación del flujo de trabajo para complementar o sustituir a los botones de aprobación y rechazo estándar. Un ejemplo de esta función se muestra en las tareas de solicitud en línea.

Historial y solicitudes en línea

En la consola de usuario, los usuarios pueden solicitar cambios en sus propias cuentas, y los administradores pueden solicitar cambios en las cuentas de usuario. Estas tareas inician una plantilla de proceso del flujo de trabajo que necesita hasta tres aprobadores: un consultor para comentar la solicitud, un usuario del negocio para aprobar la solicitud y un experto técnico para implementar la solicitud.

Las tareas de solicitud en línea también incorporan un nuevo control del historial que permite a los aprobadores adjuntar notas o comentarios a la tarea en diferentes etapas de la realización.

Programación de tareas

La programación le permite automatizar la ejecución de una tarea en una fecha futura. Si se programa una tarea que está asociada con un proceso de flujo de trabajo, Identity Manager ejecuta todas las tareas de la manera definida en dicho proceso. El estado de las tareas programadas se puede ver en la página Ver tareas enviadas.

En la página Ver tareas enviadas se puede volver a programar o cancelar una tarea programada que Identity Manager todavía no haya ejecutado.

Identity Manager muestra el programador como una ficha especial. Para poder acceder al programador, debe configurar la tarea con la ficha del programador.

Mejoras de la consola de usuario

Identity Manager r12 incluye varias mejoras para incluir compatibilidad con nuevas funciones y simplificar el uso. Estas mejoras se describen en las siguientes secciones.

Ayuda personalizada

Identity Manager permite crear su propia ayuda personalizada para las tareas y fichas que haya personalizado en la consola de usuario. Para implementar la ayuda personalizada, se puede crear un sistema de ayuda contextual con archivos de ayuda HTML personalizados o páginas Wiki y redirigir los enlaces de ayuda de la consola de usuario de Identity Manager para que proporcionen acceso a la ayuda personalizada.

Esta función también permite traducir cualquier ayuda predeterminada (escrita en inglés) a otro idioma.

Tareas anidadas

Una tarea anidada es una tarea de administración que se puede abrir desde la ficha Perfil de otra tarea. Para abrir la tarea anidada, los usuarios de la primera tarea deben hacer clic en un enlace o botón. Por ejemplo, puede agregar un botón Suprimir usuario a la tarea Modificar usuario. Si la cuenta de usuario ya no es válida, el administrador puede hacer clic en el botón Suprimir usuario y eliminar la cuenta sin necesidad de regresar al panel de navegación y seleccionar una tarea nueva.

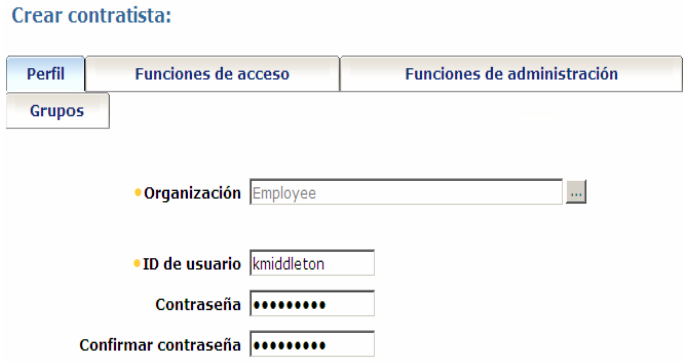
Controladores de fichas

Un controlador de fichas determina la forma en que se muestran las fichas de una tarea. Puede seleccionar uno de los siguientes controladores de fichas:

- **Controlador de fichas estándar**

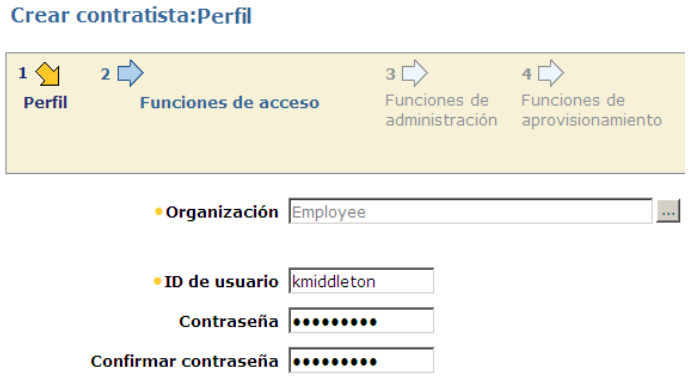
  Muestra las fichas de la tarea como fichas independientes. Los usuarios pueden usar estas fichas en cualquier orden.

  A continuación se muestra el controlador de fichas predeterminado.



- **Controlador de fichas del asistente**

  Muestra las fichas de una tarea en forma de asistente. Los administradores deben utilizar cada ficha en orden.



- **Controlador de ficha de secuencia**

  Muestra una ficha cada vez, y ésta aparece como una sola página. Los usuarios deben completar una ficha y, a continuación, hacer clic en un botón o enlace personalizado para pasar a la ficha siguiente.

  Al configurar el Controlador de ficha de secuencia, se escribe un código JavaScript, que será el encargado de determinar la secuencia de fichas y los botones y enlaces que aparecen en pantalla.

  En el código JavaScript personalizado, puede especificar la apariencia y el orden de las fichas en función de las entradas del usuario. Puede establecer, por ejemplo, que si el usuario selecciona una opción en la primera ficha, Identity Manager se encargue de mostrar una página determinada. Por el contrario, si el usuario selecciona otra opción, se mostrará una página diferente.

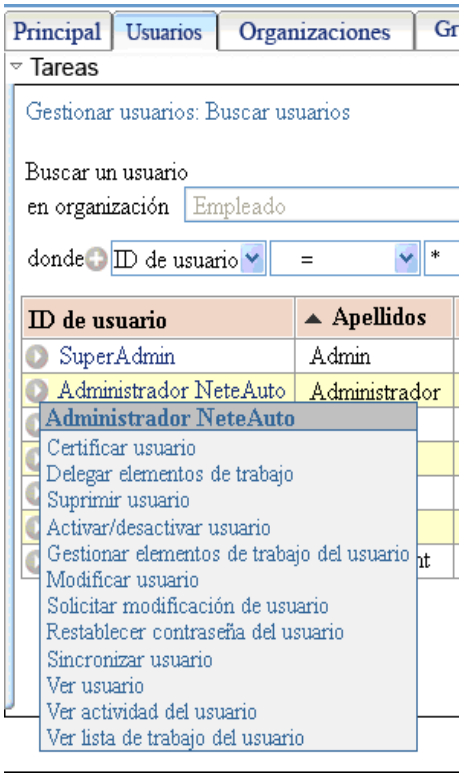
Listas de tareas

Identity Manager r12 incluye estas nuevas tareas predeterminadas que permiten buscar el objeto que se va gestionar:

- Gestionar usuarios
- Gestionar grupos
- Gestionar organizaciones
- Gestionar funciones de administración
- Gestionar tareas de administración
- Gestionar funciones de acceso
- Gestionar tareas de acceso

Una vez que se ha seleccionado el objeto, es posible visualizar una lista de las tareas que se pueden utilizar para gestionar dicho objeto.

Por ejemplo, para modificar un usuario con este método, seleccione la categoría Usuarios y, a continuación, seleccione la tarea Gestionar usuarios. Busque y seleccione el usuario que desea gestionar. En los resultados de búsqueda, haga clic en un icono para ver la lista de las tareas que puede usar para gestionar el usuario seleccionado. En esa lista, puede seleccionar Modificar usuario o cualquier otra tarea adecuada.



También puede configurar listas de tareas en tareas que no sean Gestionar. Por ejemplo, puede agregar una lista de tareas a una ficha Pertenencia a. En este caso, habrá una lista de tareas disponible para cada miembro que aparece en la ficha.

Mejoras de la ficha Perfil

En Identity Manager r12, la ficha Perfil incluye nuevos ajustes de configuración para admitir nuevas funciones. Estos nuevos ajustes se describen en las siguientes secciones.

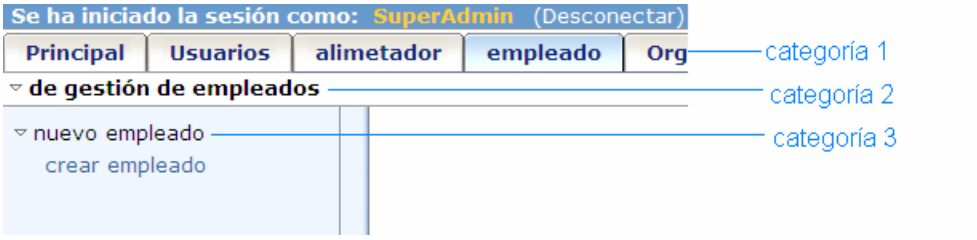
Categorías de tareas

Las categorías de tareas permiten organizar tareas para facilitar su ubicación y búsqueda en la Consola de usuario.

Puede especificar tres categorías de tareas:

- Categoría 1 es la categoría de nivel superior de las tareas. Estas categorías se muestran como fichas en la parte superior de la Consola de usuario.
- La Categoría 2 es una categoría de segundo nivel. Esta categoría le permite agrupar tareas relacionadas entre sí en una categoría de nivel superior. Si no especifica una categoría de segundo nivel, la categoría predeterminada es Tareas.
- La Categoría 3 contiene las tareas que usan los administradores. Cuando los administradores hacen clic en el nombre de la Categoría 3 en la Consola de usuario, se muestra una lista de las tareas de dicha categoría.

Dentro de cada categoría, para controlar el orden en el que se muestran los elementos de dicha categoría debe especificar un orden de categoría. Por ejemplo, en la siguiente ilustración, la ficha Empleados tiene el orden de categoría 3.



Nota: Cuando una categoría contiene varias tareas, el orden de categoría que se especifique en el perfil de cada tarea debe ser el mismo. Si el orden de categoría es diferente, aparecerán varias instancias de dicha ficha de categoría. Por ejemplo, la categoría Empleado incluye dos tareas: Crear empleado y Modificar empleado. Si el orden de categoría de la tarea Crear empleado es 3 y el orden de categoría de Modificar empleado es 6, la categoría Empleado aparece como dos fichas.

Prioridad de la tarea

En Identity Manager r12, ahora se puede especificar la prioridad de las tareas a fin de garantizar que Identity Manager ejecute antes las tareas más urgentes.

En la ficha Perfil de la tarea se puede establecer la prioridad de las tareas a Alta, Media o Baja. La prioridad predeterminada es Media.

Nota: Puede utilizar la tarea Ver tareas enviadas para buscar tareas con una prioridad específica y luego mostrar su estado.

Datos personalizados para cuadros de selección

Las pantallas de tareas de Identity Manager incluyen campos que permiten al usuario seleccionar un valor. Estos campos incluyen lo siguiente:

- Casilla de verificación de multiselección
- Desplegable
- Cuadro combinado desplegable
- Multiselección
- Seleccionador de opciones
- Seleccionador de opciones combinado
- Botón de selección de una única selección
- Selección única

Puede especificar los datos personalizados que desea utilizar para completar los cuadros de selección en archivos XML. Por ejemplo, puede usar los archivos XML Seleccionar datos de cuadro para completar las opciones del cuadro desplegable Ciudad o Estado en una ficha Perfil de la tarea Crear usuario.

También puede utilizar este archivo para configurar una dependencia entre dos campos en una pantalla de tareas. Por ejemplo, las opciones disponibles en el campo Ciudad pueden depender de la opción que el usuario seleccione en el campo Estado.

Control del seleccionador de fecha

La consola de usuario de Identity Manager ahora incluye un estilo Seleccionador de fecha que se puede aplicar a los campos de la ficha Perfil que recopilen y muestren fechas.

Cuando se aplica el estilo Seleccionador de fecha, aparece el icono de calendario junto al campo de fecha. Los usuarios deben hacer clic en dicho icono para mostrar un control de calendario y seleccionar en él la fecha deseada.

Controles de imagen y binario

Ahora se puede configurar Identity Manager para que muestre una imagen en un perfil o incluya un atributo binario. Por ejemplo, se puede configurar una pantalla de perfil de usuario para que muestre una fotografía digital del usuario que se está gestionando, o adjuntar un documento a la pantalla de perfil.

Nota: Sólo se admite para almacenes de usuarios LDAP.

Atributos personalizados de funciones definidos por el usuario

Identity Manager admite atributos personalizados definidos por el usuario que le permiten filtrar funciones de su organización de manera eficaz. Por ejemplo, es posible que en su entorno corporativo deba crear miles de funciones. y que desee clasificarlas por unidades empresariales o por ubicaciones geográficas. Así, si desea buscar funciones específicas de una ubicación geográfica, puede utilizar los atributos personalizados para filtrar las funciones de la organización.

Puede utilizar los atributos personalizados con las tareas Crear, Modificar y Ver para las funciones siguientes:

- Funciones de acceso
- Funciones de administración

Realice los pasos siguientes para añadir atributos personalizados a tareas de administración y pantallas de búsqueda.

1. Añadir atributos personalizados a las tareas de administración definidas por las funciones.
2. Configurar las pantallas de búsqueda para funciones con atributos personalizados.

Cargador masivo

Se puede utilizar la ficha Cargador masivo de la consola de usuario para cargar los archivos del alimentador que se utilizan para manipular simultáneamente un gran número de objetos gestionados. Por ejemplo, puede crear 1.000 usuarios manualmente en Identity Manager, o puede usar el Cargador masivo. La ventaja del método de Cargador masivo es que permite automatizar el proceso de manipular un gran número de objetos gestionados que utilicen un archivo de información (del alimentador). La tarea Cargador masivo también se puede asignar a un proceso de flujo de trabajo.

Nota: CSV es el formato de archivo compatible para el alimentador, pero se puede crear un alimentador personalizado para otros formatos de archivo.

Búsqueda de la organización predeterminada basada en el usuario

Para simplificar la consola de usuario, Identity Manager permite que un administrador configure la organización predeterminada para la tarea Crear usuario basándose en el usuario que intenta ejecutar la tarea. Cuando el usuario ejecuta la tarea Crear usuario, la organización no aparecerá en la ficha Crear perfil de usuario. Sin embargo, se establecerá de forma predeterminada en función de la organización a la que pertenece el usuario.

Para configurar una organización predeterminada basándose en el usuario

1. En la Consola de usuario de Identity Manager, vaya a Funciones y tareas, Tareas de administración, Modificar tarea de administración.
2. Seleccione la tarea Crear usuario.
3. En la ficha Fichas, haga clic en el icono de flecha derecha situada junto a Perfil.
4. Haga clic en el botón ... (puntos suspensivos) para mostrar una lista de las pantallas que se van a editar.
5. Seleccione la pantalla Crear perfil de usuario y haga clic en Editar.
6. Busque la organización y haga clic en el icono de flecha derecha para editarla.

   Nota: Este campo no estará presente en un entorno sin organizaciones.
7. Establezca el Estilo en Oculto.

8. En el campo JavaScript predeterminado, introduzca lo siguiente:

```
function defaultValue(blthContext)
{
return blthContext.getAdministrator().getOrg(null).getUniqueName();
}
```

9. Haga clic en Aplicar.

Compatibilidad con IPv6

Al configurar Identity Manager, puede introducir tanto la dirección IPv4 como la dirección IPv6.

Identity Manager admite IPv6 en los sistemas operativos siguientes:

- Solaris 8 o superior
- Windows 2000 SP1 o superior
- Windows 2003 o superior

Los servidores de aplicaciones tienen requisitos JDK específicos:

- En cuanto a los servidores de aplicaciones JBoss en sistemas Standalone, Identity Manager admite IPv6 con JDK1.4.2_13 o 1.5 (en Solaris) o JDK1.5 (en Windows).
- Para los clusters JBoss, JDK no es compatible con IPv6 en el momento de la publicación de la versión Identity Manager r12. Si se publica un JDK compatible con IPv6, la matriz de soporte de la plataforma se actualizará.
- Aun así, para los clusters JBoss que utilizan pilas IPv4/IPv6, Identity Manager admite IPv6 con JDK1.4.2_13 o 1.5 (en Solaris) o JDK1.5 (en Windows).
- Los servidores de aplicaciones WebLogic y WebSphere incluyen JDK 1.5, que admite direcciones IPv6.

Tenga en cuenta lo siguiente antes de configurar un entorno compatible con IPv6:

- Para que Identity Manager admita las direcciones IPv6, todos los componentes de la implementación de Identity Manager, incluyendo el sistema operativo, JDK, los servidores de directorios y las bases de datos deben admitir también las direcciones IPv6.
- Si Identity Manager se integra con SiteMinder, el complemento del servidor web del servidor de aplicaciones también debe ser compatible con IPv6.

- Al conectar SiteMinder o una base de datos de Identity Manager mediante una conexión JDBC, no introduzca la dirección IP sino el nombre de host.
- El servidor de informes de IAM se puede instalar en un host de doble pila que admita IPv4 e IPv6, pero la comunicación con el servidor debe ser IPv4.

  Al configurar una conexión con el servidor de informes en la consola de gestión, el nombre del servidor debe tener formato IPV4.

Conformidad con FIPS 140-2

Identity Manager r12 *únicamente* admite FIPS 140-2 en la nueva instalación. Además, Identity Manager cuenta con una herramienta de contraseña para proporcionar una clave de cifrado FIPS, que se ubica en el directorio siguiente:

```
Windows: C:\Archivos de programa\CA\IAM Suite\Identity
Manager\tools\Herramientacontraseña
```

Tenga en cuenta lo siguiente a la hora de habilitar FIPS 140-2 en un entorno de Identity Manager:

- Si habilita la compatibilidad de FIPS 140-2 en una instalación de Identity Manager, después no podrá deshabilitarla. Asimismo, si no habilita la compatibilidad de FIPS 140-2 en una instalación de Identity Manager, no podrá hacerlo más tarde.
- Si desea habilitar FIPS 140-2 en una instalación de Identity Manager que incluya SiteMinder, debe utilizar la versión r12 de SiteMinder.

Mejor asistencia localizada

La Consola de usuario de Identity Manager y la Ayuda en línea de la Consola de usuario están disponibles en los idiomas siguientes:

- Francés
- Coreano
- Japonés
- Alemán
- Chino simplificado
- Español
- Italiano

Nota: Para obtener más información sobre el uso de Identity Manager en uno de estos idiomas, consulte la *Guía de configuración*.

Más información:

Instalación de entornos de Identity Manager localizados (en la página 39)

Capítulo 3: Cambios en las funciones existentes

Esta sección contiene los siguientes puntos:

Agente de filtros de servlet desaprobado

El agente de filtros de servlet está desaprobado en Identity Manager r12. Se recomienda utilizar un agente Web en lugar del agente de filtros de servlet. Si ya tiene implementado un agente de filtros de servlet en un entorno Identity Manager *existente*, continuará funcionando y será compatible.

Mejoras de la consola de gestión

La consola de gestión de Identity Manager incluye las siguientes pantallas nuevas o modificadas:

- Página de la consola de usuario: utilice esta página para configurar los ajustes generales de la consola de usuario de Identity Manager, incluyendo el icono y el título, así como la clase de autentificación y la página de cierre de sesión.

  Nota: En Identity Manager, los ajustes del icono y el título se configuran en la página Temas. Las funciones de la página Temas se han movido a la página de la consola de usuario, y la página Temas se ha eliminado.

- Página de entornos: ahora puede detener e iniciar un entorno Identity Manager desde la página de entornos. No tiene que reiniciar el servidor de aplicaciones para aplicar los cambios del entorno.

- Página de aprovisionamiento: esta página ya no incluye la configuración de la sincronización entrante. Para configurar la sincronización entrante, consulte la *Guía de aprovisionamiento*.

- Página de persistencia de tareas: la persistencia de tareas ahora se configura automáticamente durante la instalación. Ya no es necesario activar manualmente la persistencia de tareas. Esta página se ha eliminado.

Cambios de la política de contraseñas

Dado que las nuevas instalaciones de Identity Manager r12 ya no necesitan SiteMinder, hay algunos cambios en las funciones predeterminadas de la política de contraseñas. En las implementaciones que no se integran con SiteMinder, Identity Manager permite crear políticas de contraseñas básicas que gestionan las contraseñas de usuario mediante la imposición de reglas y restricciones que rigen la caducidad, la composición y el uso de las contraseñas.

Si se configura Identity Manager para integrarse con SiteMinder, se pueden crear políticas avanzadas de contraseñas que permitan definir otras reglas y restricciones:

- Filtros de directorios
- Caducidad de contraseña:
  - Seguir los inicios de sesión erróneos o satisfactorios
  - Autenticar al iniciar sesión
  - La contraseña caduca si no se cambia
  - Inactividad de contraseña
  - Contraseña incorrecta
- Varias expresiones regulares
- Restricciones de la contraseña:
  - Número mínimo de días antes de la reutilización
  - Número mínimo de contraseñas antes de la reutilización
  - Porcentaje de diferencia con respecto a la contraseña anterior
  - Ignorar secuencia cuando se comprueban diferencias
  - Coincidencia de atributos de perfil
  - Coincidencia de diccionario

Herramienta imrexport desaprobada

Las funciones de la herramienta imrexport se han integrado en la consola de usuario de Identity Manager. La tarea Datos de la instantánea de captura de la ficha Informes realiza ahora las funciones de la herramienta imrexport en Identity Manager r12.

Cambio en la arquitectura de los conectores z/OS

Los conectores z/OS (CA ACF2, CA Top Secret y RACF) se han rediseñado por motivos de rendimiento, y ahora se utiliza el servidor LDAP de CA para z/OS en lugar del servidor DSI de CA en z/OS.

Las opciones del archivo de configuración del servidor de aprovisionamiento correspondientes al servidor LDAP de CA ahora se introducen y se almacenan en z/OS cuando se instala el servidor LDAP de CA. Además, la información de conexión del servidor LDAP ahora se introduce mediante la vista de tareas de extremo del Gestor de aprovisionamiento.

Funciones que ya no se admiten

Algunas funciones de eTrust Admin ya no están disponibles en Identity Manager r12. En la siguiente tabla se listan las nuevas funciones que se utilizan en Identity Manager r12.

Función eTrust Admin	Función Identity Manager
Advanced Workflow	WorkPoint Workflow
Legacy Workflow	WorkPoint Workflow
Interfaz web de autoadministración (SAWI)	Autoservicio de Identity Manager
Interfaz Web de administración delegada (DAWI)	Administración delegada de Identity Manager
Gestor de IA	Tareas de autoservicio de Identity Manager y administración delegada
Generación de informes de eTrust Admin etaReport	Generación de informes de Identity Manager
Opción PeopleSoft Feed	Cargador masivo
Opción Universal Feed	Cargador masivo
Opción SAP (versión C++)	Conector de SAP (versión Java)
Opción MS SQL (versión C++)	Conector de MS SQL (versión Java)
Opción Oracle (versión C++)	Conector de Oracle (versión Java)
Opción OS/400	Conector de OS/400 (versión Java)
Opción CleverPath Portal	Sin sustitución

Nota: Las versiones existentes (disponibles con eTrust Admin 8.1 SP2) de la opción PeopleSoft Feed y la opción Universal Feed continuarán funcionando con Identity Manager r12.

Capítulo 4: Requisitos del sistema

El sistema que va a alojar el servidor de Identity Manager necesita el siguiente hardware mínimo:

- CPU: procesador único o doble, Intel Pentium III (o compatible) a 700-900 MHz, o estación de trabajo Sparc a 440MHz
- Memoria: 2 GB
- Espacio en disco disponible: 1 GB

Nota: Estos requisitos de hardware tienen en cuenta los requisitos del servidor de aplicaciones que se debe instalar en el sistema en el que se instala el servidor de Identity Manager.

Capítulo 5: Consideraciones acerca de la instalación

Esta sección contiene los siguientes puntos:

Ubicación de la matriz de soporte

Para obtener una lista completa de versiones de software, consulte la matriz de soporte de Identity Manager.

Para localizar la matriz de soporte

1. Inicie sesión en support.ca.com.
2. Haga clic en Asistencia por producto o solución.
3. En la lista Seleccione una página de producto, en la sección Productos, seleccione CA Identity Manager.

   Se abre la página CA Identity Manager.
4. Desplácese hasta Lectura recomendada.
5. Haga clic en Índice de documentación de información de CA Identity Manager.

En la página que aparece, puede comprobar las matrices de soporte de la plataforma de versiones admitidas de Identity Manager.

Se requiere un parque Solaris

Antes de instalar aprovisionamiento en Solaris 9 o 10, descargue e instale los parches:

Para descargar los parches de Sun Studio 10 para SDK

1. Vaya a la URL siguiente:
   http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html
2. Descargue e instale el parche 117830.

   Nota: Sun Studio 11 no necesita parches.

Para descargar los parches de Solaris 9 para todos los componentes

1. Vaya a la URL siguiente:

   http://search.sun.com/search/onesearch/index.jsp
2. Descargue e instale 9_recommended.zip

Para la integración de SiteMinder Integration, es necesaria una variable de entorno.

Al instalar Identity Manager en un sistema Solaris y habilitar la integración con SiteMinder, puede que aparezca el error siguiente en el registro del servidor de aplicaciones, y es posible que Identity Manager no pueda iniciarse:

error "java: fatal: libetpki2.so: open failed: No such file or directory"

Esto ocurre si la instalación de ETPKI, que se encarga de instalar una biblioteca de codificación exigida por SiteMinder, no agrega la variable de entorno de CALIB correctamente.

Nota: El instalador de Identity Manager instala el ETPKI automáticamente.

Solución temporal

Agregue la variable de entorno CALIB de la forma siguiente antes de iniciar el servidor de Identity Manager:

```
bash# export CALIB=/opt/CA/SharedComponents/ETPKI/lib
```

Instalación de entornos de Identity Manager localizados

Identity Manager cuenta con versiones traducidas de la Consola de usuario de Identity Manager y de la Ayuda en línea de la Consola de usuario. La mayoría de los archivos necesarios para utilizar una versión traducida de la aplicación están instalados en la ubicación siguiente:

im_admin_tools_dir\samples\Localization*language*

im_admin_tools_dir

Especifica la ubicación instalada de las herramientas administrativas de Identity Manager.

idioma

Especifica el idioma que desea utilizar.

Nota: Para obtener instrucciones sobre la instalación, consulte la *Guía de configuración*.

Aun así, hay archivos adicionales necesarios para utilizar una versión traducida de Identity Manager:

- Notas de la versión
- Archivos de ayuda en línea

  Nota: No utilice la versión de los archivos de ayuda en línea de *im_admin_tools_dir*\samples\Localization*language.*

Estos archivos están disponibles en los recursos localizados de la versión r12 de CA Identity Manager para descargar, en el sitio web de soporte de CA.

Para instalar los archivos de ayuda en línea

1. Descargue el archivo ZIP de recursos localizados de la versión r12 de CA Identity Manager.
2. Descomprima los archivos en un sistema accesible para el servidor de aplicaciones que alberga Identity Manager.
3. Copie el archivo ZIP im_help_*language* del idioma que desee a *IdentityMinder.ear*\user_console.war\

   IdentityMinder.ear

   Esta es la ubicación desarrollada de la aplicación Identity Manager (IdentityManager.ear) en el servidor de aplicaciones.

   Nota: es recomendable que realice una copia de seguridad de la ayuda en línea predeterminada antes de reemplazarla con la versión traducida. La versión predeterminada se sobrescribe con la versión traducida.

4. Descomprima el archivo im_help.zip en el directorio user_console.war.
5. Reinicie el entorno Identity Manager.

   La versión traducida de la ayuda en línea ya se puede utilizar.

Los caracteres no ASCII provocan un fallo de instalación en los sistemas no ingleses

Durante la instalación de Identity Manager, el instalador extrae archivos a un directorio temporal. En algunos sistemas localizados, la ruta predeterminada del directorio temporal contiene caracteres no ASCII. Por ejemplo, la ruta predeterminada del directorio temporal en un sistema Windows español es la siguiente:

C:\Documents and Settings\Administrador\Configuración local\Temp

Los caracteres no ASCII harán que el instalador muestre una página de resumen previa a la instalación en blanco, y a continuación se producirá el fallo de la instalación.

Para evitar que la instalación falle

Cambie la variable de entorno temporal para que apunte a una carpeta que sólo contenga caracteres ASCII.

Cambios de configuración necesarios para el modo sólo FIPS 140-2 de SiteMinder

Si SiteMinder está en modo sólo FIPS 140-2, se requiere un paso más en la configuración.

Para que Identity Manager funcione con SiteMinder en modo sólo FIPS 140-2 en WebLogic o JBoss

1. Abra *IdentityMinder.ear*\policyserver.rar\META-INF\ra.xml.
2. Busque el elemento siguiente:

```
<config-property>
<config-property-name>ModoFIPS</config-property-name>
<config-property-type>java.lang.String</config-property-type>
<config-property-value>falso</config-property-value>
</config-property>
```

3. Sustituya "falso" por "verdadero" en el elemento <config-property-value>.
4. Reinicie el servidor de aplicaciones.

Para que Identity Manager funcione con SiteMinder en modo sólo FIPS 140-2 en WebSphere

1. Abra la consola de administración de WebSphere.
2. Desplácese hasta la ubicación siguiente:

   Aplicaciones empresariales > IdentityMinder > Módulos de administrador > policyserver.rar > IdentityMinder.PolicyServerRA > fábricas de conexiones de J2C > PolicyServerConnection > Propiedades personalizadas
3. Haga clic en el valor ModoFIPS y cambie el valor a verdadero. Haga clic en Aceptar y, a continuación, en el vínculo "guardar" que aparece en la parte superior de la página.

JBoss: Configuración de la compatibilidad con IPv6

Si se instala la versión JBoss de Identity Manager en un sistema compatible con IPv6, son necesarios ciertos ajustes de configuración.

Para configurar IPv6 en un servidor de aplicaciones JBoss

1. Abra el archivo run_idm.sh, que se encuentra en:

   jboss_installation\bin
2. Modifique *una* de las siguientes propiedades en la entrada JAVA_OPTS:
   - Para entornos sólo IPv6, elimine el comentario de la siguiente entrada:

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv6Addresses=true
   - Para entornos IPv6/IPv4, elimine el comentario de la siguiente entrada:

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true
3. Guarde el archivo.

Compatibilidad SPML con FIPS 140-2

En cuanto a la versión r12 de Identity Manager, el servidor SPML es compatible con FIPS 140-2. Le recomendamos que desarrolle el servicio SPML en:

- Apache Tomcat Server 4.1.36 o una versión posterior a la 4.1
- JDK 1.5.11 o una versión posterior a la JDK 1.5. Tenga en cuenta que Tomcat se debe habilitar para ser ejecutado en modo SSL. Para obtener más información, consulte la sección “Cómo configurar SSL” de la guía del administrador de Apache para Tomcat 4, (http://jakarta.apache.org/tomcat/).

Si utiliza CA Tomcat en vez de Apache Tomcat, la versión r12 de Identity Manager requerirá las soluciones temporales siguientes para SPML:

- Si utiliza JDK 1.4.xx con CA Tomcat, debe deshabilitar FIPS 140-2. JDK 1.4.xx no es compatible con CA Tomcat porque la biblioteca RSA Jsafe CryptoJ 4.0 requerida para la compatibilidad de FIPS 140-2 no se puede configurar como proveedor de seguridad prioritario de JDK1.4.

  Para deshabilitar la compatibilidad de FIPS 140-2, pase el indicador JVM "-Dcom.ca.commons.security.fips=false" al iniciar Tomcat.

  - Si ejecuta Tomcat des de la línea de comandos, puede incluir el indicador JVM catalina.bat. El archivo de proceso contiene más información.
  - Si ejecuta Tomcat como un servicio de Windows, pase el indicador tal y como se indica a continuación:

    a. Mediante el editor de registro, desplácese a "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CA Tomcat 4.1.29 eTrustIAMWebServer\Parameters"

    b. Agregue un valor de cadena llamado "Opción de JVM número n" en que "n" es el número que sigue al parámetro JVM anterior. Para el valor, especifique:

    Dcom.ca.commons.security.fips=false

    c. Incremente en uno el valor de Editar valor DWORD "Recuento de opciones JVM" para explicar el nuevo parámetro agregado.

- Si utiliza JDK 1.5 con CA Tomcat, se encontrará con un problema de incompatibilidad. Para resolver este problema:

  a. Elimine manualmente las dos bibliotecas Xerces (xercesImpl.jar y xmlParserAPIs.jar) de %TOMCATHOME%\common\endorsed.

  b. Reinicie Tomcat.

Cambio en la arquitectura de los conectores de z/OS

Los conectores z/OS (CA ACF2, CA Top Secret y RACF) se han rediseñado por motivos de rendimiento, y ahora se utiliza el servidor LDAP de CA para z/OS en lugar del servidor DSI de CA en z/OS.

Antes de intentar configurar cualquier conector de z/OS debe instalar el servidor LDAP de CA para z/OS r12, que se puede descargar en la dirección http://www.ca.com/worldwide.

Ubicación de eTrust Directory

El esquema del directorio de aprovisionamiento se instala en eTrust Directory. eTrust Directory se puede instalar desde el medio de instalación de Identity Manager.

Corrección necesaria antes de desinstalar eTrust Directory

Si es necesario desinstalar eTrust Directory de un sistema Windows, se debe aplicar un parche antes de comenzar con el procedimiento de desinstalación.

Si no se aplica el parche, el procedimiento de desinstalación podría suprimir los archivos de licencia que necesitan otros productos de CA.

El parche se puede descargar en el sitio web de soporte técnico de CA.

Para localizar el parche

1. Inicie sesión en http://www.ca.com/worldwide.

   Se abrirá el sitio web de CA. Seleccione su país y acceda a la sección de soporte técnico.

2. Haga clic en Licencias (Licensing) en la lista de enlaces del lado izquierdo de la página.

3. Ya está disponible el paquete de licencia 1.8.

   Se abrirá una página que describe los cambios del paquete de licencia, y que incluye un enlace para descargarlo.

4. Siga las instrucciones para descargar e instalar el parche de Windows.

Capítulo 6: Problemas conocidos

Esta sección contiene los siguientes puntos:

General

Los puntos siguientes son problemas conocidos generales de la versión r12 de Identity Manager.

El EAR de Identity Manager no se implementa automáticamente con WebLogic

Si se está utilizando WebLogic 8 ó 9 en modo de producción, es posible que el EAR de Identity Manager no se implemente automáticamente la primera vez que se inicie el servidor de aplicaciones tras una instalación o una actualización. Si esto ocurre, implemente el IdentityMinder.ear manualmente desde la carpeta user_projects\applications.

Flujos de trabajo y miembros de grupos como aprobadores

Si se configura un proceso de flujo de trabajo en Diseñador del punto de trabajo para que los miembros de un determinado grupo sean sus aprobadores, es posible que no se cree el elemento de flujo de trabajo para el evento bajo el control del flujo de trabajo. De esta forma, podrían producirse errores en la sesión de tarea.

La solución es colocar la tarea bajo el control del flujo de trabajo utilizando el método con plantilla (con la plantilla SingleStepApproval o TwoStageApprovalProcess), y definir los miembros del grupo como aprobadores (o resolvedores del participante).

Es posible que sea necesario establecer nuevas propiedades de Workpoint

Identity Manager incluye una nueva versión de Workpoint. En esta versión, se pueden configurar nuevas propiedades en GeneralMonitor.properties y en workpoint-server.properties. Tenga en cuenta que estas nuevas propiedades son opcionales, y sólo se deben agregar si es necesario.

Las nuevas propiedades del flujo de trabajo son las siguientes:

- En el archivo GeneralMonitor.properties:
  - #JMX_HTML_ADAPTOR_PORT=9092

    Esta propiedad se ha comentado de forma predeterminada. La propiedad, cuando se establece como verdadera, activa una página HTML que utiliza el adaptador Sun JMX genérico, que es un puerto web inseguro independiente de la aplicación de la Consola de gestión de Workpoint. Se recomienda que los usuarios dejen esta propiedad sin comentar o establecida como falsa, y en su lugar utilicen la Consola de gestión de Workpoint para el acceso de JMX a Workpoint.
  - JOB_ERROR_STATE_ON_MAIL_ERROR=false

    Esta propiedad sólo se aplica a los usuarios que estén utilizando la función de correo electrónico de Workpoint. Esta propiedad controla el tratamiento de errores en el controlador de correo electrónico. Si los usuarios de Identity Manager están utilizando la función de correo electrónico de Workpoint, se puede aplicar esta propiedad.

    Nota: La propiedad JOB_ERROR_STATE_ON_MAIL_ERROR es verdadera de forma predeterminada si no se establece. Es posible que desee establecerla en falso si está utilizando el correo electrónico del flujo de trabajo, pero no desea que los errores del correo electrónico afecten al estado de las tareas.
  - ENABLE_SCRIPT_TASK_GROUPING=false

    Esta propiedad controla si el controlador de secuencias de comandos debe agrupar todas las secuencias de comandos simultáneas que se ejecutan desde la misma tarea. Si está establecida en verdadero, tendrá el efecto de asignar todas las secuencias de comandos de una tarea concreta al mismo subproceso del trabajador, en donde se ejecutarán una por una. Resulta muy útil para evitar las excepciones de simultaneidad cuando se tienen varias actividades en una tarea y esas actividades utilizan una secuencia de comandos asíncrona para la automatización y pueden estar activas al mismo tiempo.

    Si tiene secuencias de comandos del flujo de trabajo personalizadas y experimenta excepciones de simultaneidad, investigue esta propiedad.

    El archivo GeneralMonitor.properties contiene otras propiedades relacionadas con el correo electrónico.

- En el archivo workpoint-server.properties:
  - server.automated.delay=500

    Esta propiedad controla los nodos automatizados del servidor para garantizar que estos nodos no sean puestos en cola antes de que la transacción de base de datos que los puso en ella tenga la posibilidad de persistir. Esto evitará el fallo de los nodos automatizados del servidor debido a problemas de control de tiempo. Esta propiedad se recomienda cuando se utilizan nodos automatizados del servidor.

No se puede crear una copia del identificador de atributos lógicos

Si intenta crear una copia del identificador de atributos lógicos de la Consola de usuario, aparece el error siguiente:

"This object is not connected"

Si crea un identificador de atributos lógicos nuevo que no esté basado en un identificador anterior, este funciona correctamente.

Uso de filtros de grupo en políticas de función

Cuando Identity Manager gestiona un almacén de usuarios en una base de datos relacional, es posible que los filtros de grupo de las políticas de miembros y de administración no funcionen correctamente. Por ejemplo, si se especifica un filtro tal como "Usuarios que son miembros de grupos cuyo nombre empieza por A" en una política de miembros, es posible que Identity Manager aplique de forma incorrecta la política a todos los usuarios, en lugar de a los usuarios de los grupos que comienzan con la letra A.

Para evitar este problema, asegúrese de que las tablas, tblGroupMembers y tblGroupAdministrators, estén definidas para el objeto usuario en el archivo de configuración del directorio (directory.xml).

La definición del objeto usuario en directory.xml debería parecerse a la siguiente:

```
<ImsManagedObject name="Usuario" description="Mis usuarios" objecttype="USER">
<!-- COMMENT Table -->
    <Table name="tblUsers" primary="true" />
    <Table name="tblUserAddress">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserRoles">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserDelegators">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserPasswordhints">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserIdentityPolicy">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblOrganizations">
    <Reference childcol="id" primarycol="org"/>
    </Table>

    <Table name="tblGroupMemebers">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblGroupAdmins">
    <Reference childcol="userid" primarycol="id"/>
    </Table>
```

Una vez modificado el archivo de configuración del directorio, impórtelo utilizando la consola de gestión.

Nota: Para obtener más información sobre la modificación de los archivos de configuración del directorio, consulte la *Guía de configuración*.

Configuración de las pantallas de búsqueda de funciones y tareas

Al configurar pantallas de búsqueda de funciones o tareas, es posible limitar las funciones y tareas que devuelve la búsqueda. Para ello, utilice la opción "Mostrar sólo aquellos objetos que cumplan las siguientes reglas". Los atributos que se utilizan al configurar esta opción no se deben incluir como campos de búsqueda disponibles en la pantalla de búsqueda.

Por ejemplo, si la pantalla de búsqueda se configura para que muestre sólo las funciones con el atributo Activado establecido en Sí, suprima el atributo Activado de la lista de atributos que pueden especificar los usuarios en los criterios de búsqueda.

De lo contrario, se ignorarán los criterios introducidos por el usuario.

Creación de entornos de Identity Manager en un navegador Firefox

Si accede a la Consola de administración a través de un navegador Firefox, es posible que la creación del entorno de Identity Manager sea lenta y se cuelgue. En este caso, la creación de entorno prosigue pero el navegador no se actualiza, por lo que no puede visualizar el fin del proceso.

Nota: Si cierra la ventana del navegador, Identity Manager continua creando el entorno.

Actualizaciones

Los problemas siguientes están relacionados con las actualizaciones de la versión r12 de Identity Manager.

Extremos de MS SQL y Oracle no disponibles tras la actualización desde eTrust Admin 8.1 SP2

Tras actualizar desde eTrust Admin 8.1 SP2 a Identity Manager r12, los extremos de MS SQL u Oracle adquiridos antes de la actualización deberán ser reconfigurados de forma manual mediante el Gestor de aprovisionamiento, para que utilicen direcciones URL de JDBC en lugar de nombres de orígenes de datos (DSN). Esto se debe a que se pasa de utilizar el Superagente a utilizar Java CS para gestionar los extremos de MS SQL y Oracle.

Oracle: modifique los datos de la hoja de propiedades de extremos de Oracle.

Ejemplo:

```
jdbc:oracle:thin:@oracle_server_host:1521:ORACLE
```

MS SQL: haga clic con el botón secundario en el extremo y seleccione Personalizar, Cambiar contraseña del administrador. Las credenciales de la URL y de la conexión se pueden cambiar en este momento sin necesidad de ver el resto de datos del extremo.

Ejemplo:

```
jdbc:sqlserver://serverHost:1433;instanceName=instancia1
```

Nota: En el capítulo 4 "Conectores de base de datos" de la *Guía de conectores* se pueden encontrar las etapas de migración y una lista completa de posibles sintaxis de URL.

El agente remoto de UNIX no está disponible para la plataforma Solaris x86 (Intel)

Faltan archivos en el paquete del agente remoto de UNIX necesarios para la instalación o la actualización del agente remoto de UNIX en la plataforma Solaris x86 (Intel).

Cambio de la arquitectura de los conectores de z/OS

Los conectores z/OS (CA ACF2, CA Top Secret y RACF) se han rediseñado por motivos de rendimiento, y ahora se utiliza el servidor LDAP de CA para z/OS en lugar del servidor DSI de CA en z/OS.

Antes de intentar configurar cualquier conector de z/OS debe instalar el servidor LDAP de CA para z/OS r12, que se puede descargar en la dirección http://www.ca.com/worldwide.

Una vez que haya actualizado a Identity Manager r12, lleve a cabo lo siguiente en cada extremo definido en el sistema:

En la vista de tareas de extremo

1. Seleccione el extremo CA ACF2, CA Top Secret, o RACF en Tipo de objeto.
2. Haga clic en el botón de búsqueda. Haga clic con el botón secundario en el extremo y seleccione las propiedades. Complete la siguiente información:

   En la sección de información del servidor de Mainframe:

   - **Dirección IP/Nombre del equipo** especifica la dirección IP del sistema gestionado por RACF en el que está configurado y se está ejecutando el servidor LDAP de CA.
   - **Puerto LDAP** especifica el número de puerto que se ha indicado durante la instalación del servidor LDAP de CA para z/OS. Si no está seguro del puerto LDAP de Mainframe, consulte la sección "Comprobación de la información de configuración del servidor LDAP de CA para z/OS".
   - **Sufijo LDAP** especifica el sufijo que se debe utilizar para este extremo. Si hace clic en el botón "Obtener sufijos", este cuadro combinado se rellena automáticamente con todos los sufijos disponibles válidos. Los sufijos se pueden recuperar tras proporcionar valores válidos para los campos de dirección IP/nombre del equipo de Mainframe y puerto LDAP de Mainframe.

Información

Los problemas siguientes están relacionados con los informes de la versión r12 de Identity Manager.

Limitación de informes

Si existen varias instantáneas asociadas a una única tarea de informe, estas no deben utilizar el mismo tiempo de repetición.

Satisfy=All No funciona correctamente en el archivo XML

En un archivo XML de parámetros de instantáneas, satisfy=all y satisfy=any funcionan como satisfy=any (de manera similar a un operador OR).

Habilitar las cookies para la tarea Ver Mis informes

Para ver los informes de Identity Manager mediante la tarea Ver Mis tareas, habilite las cookies de sesión de terceros del navegador.

ExportALL.xml y entornos que no admiten organizaciones

Al utilizar un archivo XML de parámetros de instantánea (por ejemplo ExportAll.xml) que exporta los atributos y los objetos de la organización, se producirá una excepción si el entorno no admite organizaciones. Para resolver este problema, elimine el comentario de los atributos y del objeto de organización en el archivo ExportAll.xml.

Aprovisionamiento

Las abreviaturas de los componentes de aprovisionamiento para la siguiente lista de temas se definen del modo siguiente:

- ACC: Conector de control de acceso de CA
- ADS: Conector de Servicios de Active Directory
- DBZ: Conector de base de datos DB2 Universal para z/OS
- DYN: Conector dinámico
- E2K: Conector de Exchange 2000
- EEM: Conector de Embedded Entitlements Manager
- ETC: UNIX ETC
- FND: Conector de aplicaciones de Oracle
- INS: Instalación
- KRB: Conector de Kerberos
- LND: Conector de Lotus Notes/Domino
- NDS: Conector de servicios del directorio Novell
- N16: Agente remoto de Windows NT
- AS4: Conector de OS/400
- PKI: Conector de Entrust PKI
- PLS: Conector de CA SSO para el servidor de políticas avanzadas
- PSA: Agente de sincronización de contraseñas
- RSA: Conector de RSA SecurID
- SAP: Conector de SAP

- SBL: Conector de Siebel
- UPO: Conector de aprovisionamiento universal
- VMS: Conector de OpenVMS
- z/OS: Conectores de CA ACF2, CA Top Secret, RACF

General

Los puntos siguientes son problemas de aprovisionamiento generales de la versión r12 de Identity Manager.

Sincronización de cuentas para la tarea Restablecer contraseña del usuario

Para habilitar el aprovisionamiento de un entorno de Identity Manager, debe importar un archivo de configuración (ProvisioningOnly-RoleDefinitions.xml), que crea las funciones y tareas para dar respuesta al usuario.

En este archivo, la configuración de sincronización de cuentas predeterminada para la tarea Restablecer contraseña del usuario está definida a Desactivada. (Antes de habilitar el aprovisionamiento, la configuración de sincronización está definida a Al completar la tarea.)

Para utilizar la función Restablecer contraseña del usuario para sincronizar la cuenta, defina la opción de sincronización de la cuenta una vez importado el archivo ProvisioningOnly-RoleDefinitions.xml para habilitar el aprovisionamiento.

La Consola de usuario no puede explorar y correlacionar algunos tipos de extremos

Las tareas Explorar y Correlacionar de la Consola de usuario no encuentran los siguientes tipos de extremo:

- Kerberos
- UNIX NIS
- Entrust PKI
- Siebel
- Base de datos Universal para z/OS
- Tipos de extremos desarrollados personalizados

Para explorar y correlacionar estos tipos de extremos, se puede utilizar el Gestor de aprovisionamiento. Después podrá realizar funciones de cuentas rutinarias en la Consola de usuario, como por ejemplo asignar una cuenta a uno de estos extremos.

Explorar y Correlacionar trabajos en una misma zona horaria

En la Consola de usuario, puede programar la definición de Explorar y correlacionar. Esta acción requiere que el navegador cliente se encuentre en la misma zona horaria que el servidor. Por ejemplo, si para el cliente son las 10:00 PM del martes y para el servidor son las 7:00 AM, la definición de Explorar y correlacionar no funcionará.

Volcado de memoria del servidor de aprovisionamiento en Solaris

El servidor de aprovisionamiento en Solaris generará un archivo principal al cerrar el servicio.

Esto no afecta a ninguna función y se puede ignorar con total seguridad.

El instalador del directorio de aprovisionamiento necesita un nombre del host correctamente resuelto

Si el directorio de aprovisionamiento y el servidor de aprovisionamiento se instalan en el mismo equipo, el instalador necesitará un nombre del host con una resolución del nombre configurada correctamente. La instalación del servidor de aprovisionamiento fallará o producirá resultados no esperados si el equipo no puede resolver su propio nombre de equipo en la dirección IP prevista. Existen dos escenarios posibles:

- Se tiene un resultado de la resolución de nombre diferente para FQDN y nombre del host. (Por ejemplo, en una red IPv4/6, se registra una dirección IPv6 en DNS, pero se tiene una dirección IPv4 para el nombre del host mediante net bios o el archivo del host). Si se configura el directorio de aprovisionamiento para que sólo escuche en IPv6, y a continuación se instala el servidor de aprovisionamiento utilizando FQDN, la instalación fallará porque el programa de instalación intenta resolver el nombre del host en lugar de FQDN durante determinadas etapas de la instalación. La solución para este problema es agregar el nombre del host y su dirección IPv6 al archivo del host. Sin embargo, continúa siendo una configuración errónea.
- Si en un equipo sin DNS o cualquier otra búsqueda de nombre, se intenta instalar el directorio de aprovisionamiento y el servidor de aprovisionamiento utilizando una dirección IP, la instalación fallará por el mismo motivo.

  Nota: CA no admite la instalación mediante una dirección IP.

Determinadas configuraciones de dominio realizadas con cambios simultáneos de la contraseña de usuario global pueden bloquear el servidor de aprovisionamiento

Si la configuración de dominio "Servidor de Identity Manager/Usar políticas de contraseñas externas" está establecida en Sí y se realizan muchos cambios simultáneos de la contraseña de usuario global. El resultado será la disminución del rendimiento, y es posible que el servidor de aprovisionamiento se bloquee.

El inicio de sesión de Solaris ECS sobre el nivel INFO puede afectar al rendimiento del servidor de aprovisionamiento

Si se activa el inicio de sesión de ECS sobre el nivel INFO los registros se escribirán antes de recibir una respuesta. Esto hará que su solicitud se retrase mientras se escribe el registro. Si se observa un bajo rendimiento del servidor de aprovisionamiento al utilizar el inicio de sesión de ECS, la solución es desactivarlo.

Las actualizaciones de SPML fallan cuando JIAM especifica nombres de clases de objetos incorrectos

Es posible que en ocasiones la API de JIAM comience a utilizar nombres de clases de objetos abreviados e incorrectos en las solicitudes enviadas al servidor de aprovisionamiento. El servidor de aprovisionamiento rechazará la solicitud y emitirá un "Error de consistencia interna en el servidor de aprovisionamiento". Por ejemplo, al realizar una actualización del objeto "eTSBLDirectory", se envía la clase de objeto incorrecta "eTDirectory" al servidor de aprovisionamiento. Este problema se puede solucionar reiniciando el servicio SPML.

Caracteres especiales de los nombres de usuario global

El Gestor de aprovisionamiento permite crear nombres de usuario global que incluyan caracteres especiales, como el carácter de contrabarra (\). No obstante, el servidor de Identity Manager, no admite nombres de usuario con caracteres especiales.

Al crear un usuario global con caracteres especiales en el Gestor de aprovisionamiento, Identity Manager intenta entonces crear un usuario en el almacén de usuarios de Identity Manager. Al hacerlo, se producen errores y la tarea Crear usuario falla en el almacén de usuarios de Identity Manager.

También se producen errores si intenta eliminar un usuario global con caracteres especiales en el Gestor de aprovisionamiento.

El Gestor de aprovisionamiento incluye referencias SAWI/DAWI obsoletas

El Gestor de aprovisionamiento incluye cuadros de diálogo que controlan las funciones SAWI y DAWI, las cuales ya no son compatibles. Utilice las funciones autoservicio del Gestor de aprovisionamiento en lugar de SAWI o DAWI.

Ya existe un error al agregar un extremo

Si se elimina y se vuelve a agregar un extremo con un nombre exactamente igual, algunas veces el servidor de aprovisionamiento genera un error que indica que ya existe un extremo con ese nombre. Esto puede ocurrir cuando se han configurado varios servidores de conectar para gestionar dicho extremo. El fallo deriva de un problema durante la eliminación del extremo por el que no se ha notificado la eliminación a todos los servidores de conector.

Para resolver este problema, reinicie todos los servidores de conector que estén configurados para gestionar el extremo.

Servidor de conector de Java (Java CS)

Los siguientes puntos están relacionados con el servidor de conector de Java en Identity Manager r12.

La exploración del conector de Java falla cuando se utiliza la secuencia de caracteres " / para representar nombres distintivos.

En Java CS existe un problema sin resolver relacionado con la siguiente secuencia de dos caracteres:

"/

Esto es importante para la gestión de los nombres compuestos utilizados por la API de JNDI estándar para representar nombres distintivos que abarcan varias tecnologías.

Para obtener más información sobre otros caracteres especiales en los nombres distintivos que se pasan a Java CS, consulte LDAP RFC 2253 en:

http://ietf.org

y en JavaDoc para javax.naming.ldap.LdapName

Error de puntero nulo en Connector Xpress

Si intenta modificar la información de direccionamiento del servidor de conector ya sea haciendo clic con el botón derecho del ratón en un tipo de extremo y seleccionando el conjunto de gestión de CS, o bien directamente editando la configuración de CS en entornos de varios servidores de aprovisionamiento mediante Connector Xpress, es posible que Connector Xpress muestre un error de puntero nulo. Si necesita realizar un direccionamiento de conector avanzado, utilice la herramienta csfconfig.

Al reiniciar el servicio CS de Java con servicios Windows, se produce un error

Si reinicia el servicio CS de Java mediante servicios Windows, se puede iniciar el servicio Java antes de que este se haya finalizado por completo, cosa que impide que el servicio de pueda iniciar. Si ocurre esto, utilice los botones Iniciar/detener antes que los botones de reinicio en el Panel de control del servicio de Windows.

Si no selecciona un procedimiento almacenado, aparecerá un mensaje de error incorrecto

Si no selecciona un procedimiento almacenado de la lista desplegable Seleccionar procedimiento, las pantallas de asignación de tablas del asistente de Connector X y hace clic en Siguiente, aparece el mensaje de error incorrecto:

Especifique una tabla para asignar.

El mensaje correcto es:

Especifique un procedimiento para asignar.

Faltan los contenedores explorados del extremo DYN JNDI en el Gestor de aprovisionamiento

Tras realizar una exploración de un nivel de un contenedor en extremos DYN JNDI recién adquiridos, es posible que el panel de contenido del Gestor de aprovisionamiento no muestre el contenedor que se acaba de explorar a pesar de que el recuento de la exploración indique que se ha agregado el nuevo registro. Si el Gestor de aprovisionamiento se cierra y se vuelve a abrir, se forzará a que aparezca el contenedor.

Los atributos suspendidos de la plantilla de cuenta de DYN se muestran en negrita en el Gestor de aprovisionamiento

El Gestor de aprovisionamiento muestra el atributo de estado de suspensión de cuenta para plantillas de cuenta de DYN en negrita, lo que indica erróneamente que es un atributo de capacidad.

Es posible que las etiquetas de los atributos de capacidad de DYN estén truncadas en el Gestor de aprovisionamiento

Es posible que en los atributos de capacidad especificados al crear los tipos de extremo DYN JDBC ó DYN JNDI en Connector Xpress falten etiquetas o tengan etiquetas truncadas cuando se muestran en el Gestor de aprovisionamiento. Esto se puede solucionar especificando un carácter adicional al final de la etiqueta, por ejemplo "*NombreEtiqueta a*" cuando se especifica el nombre en pantalla en Connector Xpress. Esto no ocurre en los atributos de capacidad de pertenencia de miembros.

También se pueden modificar los metadatos existentes de una de las siguientes formas:

Después de cargar el proyecto guardado en Connector Xpress

- Ejecución mediante el asistente
- Expanda el árbol de metadatos, desplácese hasta Clases -> eTDYNPolicy -> Propiedades -> Atributo de capacidad -> Metatadatos, y modifique el valor del nombre en pantalla (displayName).

Si se selecciona uno de los dos métodos para modificar los metadatos existentes para un tipo de extremo DYN, asegúrese de que su tipo de extremo DYN se actualiza con los nuevos metadatos.

Conectores

Los problemas siguientes están relacionados con los conectores de aprovisionamiento de la versión r12 de Identity Manager.

Resultados incorrectos durante una búsqueda en un árbol secundario con el conector de ADS

Durante una búsqueda en un árbol secundario que contiene varias unidades de organización con un gran número de objetos en cada unidad de organización, la búsqueda podría, incorrectamente, no devolver ningún objeto. Por ejemplo, con un tamaño del límite de búsqueda establecido en 500 y el número de objetos de cada OU por encima de dicho límite, no se devolverán resultados. Incluso si el filtro de búsqueda reduce el tamaño del límite de búsqueda a un valor por debajo de 500, la búsqueda podría continuar sin devolver ningún objeto. La solución a este problema es aumentar el tamaño del límite de búsqueda.

Evitar el establecimiento de fechas de vencimiento de ADS posteriores a 2038

Si se establece la fecha de vencimiento de una cuenta ADS en una fecha posterior a 2038, el Gestor de aprovisionamiento se bloqueará.

Incompatibilidad del conector EEM con IE7

El conector EEM no se admite si el servidor de conector de C++ (CCS) para el conector EEM en cuestión se instala en un equipo que tenga instalado IE7.

Nota: En la documentación del producto de Identity Manager r12, EEM (Embedded Entittlements Manager) hace referencia al conector de EIAM (Embedded Identity and Access Manager).

Visualización de plantillas de cuenta de EEM con el Gestor de aprovisionamiento

Es posible que el Gestor de aprovisionamiento deje de responder al visualizar plantillas de cuenta de EEM.

La solución es cerrar y reiniciar el Gestor de aprovisionamiento.

Reapertura del Gestor de aprovisionamiento para adquirir un nuevo extremo de EEM

Una vez que se ha establecido un nombre del host durante una adquisición, se debe cerrar y volver a abrir el Gestor de aprovisionamiento para adquirir otro extremo. Esto se aplica aunque la operación haya sido cancelada.

No se pueden seleccionar o modificar atributos de usuario en la plantilla de cuenta de EEM

Para crear plantillas de cuenta para un extremo de EEM, haga clic en la ficha de propiedades de la aplicación tras seleccionar el extremo. A continuación, haga clic en Aceptar para finalizar el proceso de creación de la plantilla de cuenta.

La adquisición del extremo DB2 z/OS bloquea CCS

Los conectores DB2 UDB y DB2 z/OS no deben enrutar solicitudes al mismo servidor de conector de C++ (CCS).

La solución es instalar un segundo CCS en un equipo independiente para que cada uno de los conectores DB2 UDB y DB2 z/OS se alojen en sus propios servidores de conector de C++.

Actualización desatendida del agente remoto de UNIX ETC no compatible

No se admiten las actualizaciones desatendidas del agente remoto de UNIX ETC desde eTrust Admin r8.1 SP2 hasta Identity Manager r12. La actualización se debe realizar en modo atendido.

Fallo en el agente remoto de ETC en un SO Linux que se ejecuta en un S390

Cuando se intenta instalar el agente remoto de ETC en un sistema operativo Linux que se ejecuta en un host S390, se produce el error:

"linux098:/home/marty/LinuxS390 # ./IdentityManager.LinuxS390.sh
lsm.exe: error al cargar las bibliotecas compartidas: libncurses.so.4: no se puede abrir el archivo de objeto compartido: El archivo o directorio no existe."

Para resolver este problema, será necesario localizar la versión 4 de ncurses para el sistema operativo e instalarla.

La ejecución del comando Cafthost genera un error para HP-UX UNIX

Es posible que aparezca un "Error de bus (volcado de memoria)" al ejecutar el siguiente comando:

```
cafthost -a <nombre_host>
```

Para agregar uno o varios host, modifique manualmente el archivo de configuración "cafthost.cfg" mediante un editor de archivos de texto en el directorio "`cat /etc/catngcampath` y agregue cada host en una nueva línea.

La desinstalación del agente remoto de ETC puede dejar archivos huérfanos

Cuando se actualiza el agente remoto de ETC de r8.1SP2 a r12, es posible que se dejen atrás varios archivos. Estos archivos se pueden suprimir si no los utilizan otros paquetes instalados:

- /usr/bin/uxsautil
- `cat /etc/catngdmopath.tng`/bin/uxsautil
- `cat /etc/catngdmopath.tng`/scripts/Config
- `cat /etc/catngdmopath.tng`/etc/ExitSetup.ini
- `cat /etc/catngdmopath.tng`/scripts/caftexec
- `cat /etc/catngdmopath.tng`/scripts/caftexec.cfg
- `cat /etc/catngdmopath.tng`/setup.gif

La eliminación de derechos de cuentas VMS falla con SPML

No se puede eliminar un valor del atributo accountRights en una cuenta VMS mediante SPML. El cliente SPML devolverá un mensaje indicando que la tarea se ha realizado correctamente, pero la cuenta no se actualizará.

La solución es utilizar el Gestor de aprovisionamiento para realizar dichas modificaciones.

No se puede establecer una contraseña secundaria para cuentas OpenVMS

La utilidad del agente remoto de OpenVMS 'vmsautil' no exige la semántica de la contraseña PRIMARIA/SECUNDARIA de OpenVMS para las cuentas de usuario. Si se intenta especificar una contraseña secundaria cuando no se ha establecido la contraseña primaria, la operación fallará con un mensaje de error "la contraseña es demasiado corta".

La solución es restablecer siempre la contraseña primaria al intentar establecer una contraseña secundaria para la cuenta.

Falta una instrucción de CAM/CAFT para OpenVMS

Falta información en el archivo ETRUST_ADMIN_OPENVMS_INSTALLATION.TXT sobre cómo configurar CAMCAFT.EXE en un sistema OpenVMS. Debe definir el nombre simbólico de CAFTHOST antes de instalar CAM/CAFT. Para definir CAFTHOST, añada el comando siguiente al archivo LOGIN.COM:

```
CAFTHOST :==$CAPOLY$BIN:CAFTHOST.EXE
```

A continuación, inicie sesión de nuevo en el sistema OpenVMS.

El atributo de VMS eTVMSPWDLifeTime aparece no sincronizado

El atributo del tiempo de vida de la contraseña (eTVMSPWDLifeTime) se muestra como no sincronizado después de la operación de comprobación de la sincronización de la cuenta si el atributo de la plantilla de cuenta "No caduca nunca" se establece en verdadero (activado).

SPML informa incorrectamente del estado de la cuenta VMS como Falso

Si se suspende una cuenta de VMS, el Gestor de aprovisionamiento informa correctamente del estado de la cuenta como "Activa (suspendida en eTrust Admin)". Sin embargo, SPML informa de que el estado suspendido es falso.

No se pueden establecer los indicadores de la contraseña de VMS

El atributo eTVMSPwdFlags no se establece correctamente en una operación de agregación o modificación de cuenta si la solicitud no establece también un valor para eTVMSAccessFlags.

Para resolver este problema, la solicitud de agregación o modificación debe contener un valor para el atributo eTVMSAccessFlags y para el atributo eTVMSPwdFlags.

El atributo de contraseña de migración de VMS aparece no sincronizado

Cualquier cuenta o plantilla de cuenta de VMS con el campo MIGRATEPW establecido en verdadero (activado), muestra eTVMSPwdFlags como no sincronizado tras la operación de comprobación de la sincronización de la cuenta.

Suspensión de cuentas VMS

Suspender una cuenta en el nivel de cuenta utilizando el Gestor de aprovisionamiento suspende correctamente la cuenta. Sin embargo, no mantiene "Suspendida" en la página de propiedades y vuelve a cambiar a "Activa" al aplicar el cambio. De este modo, existe una cuenta que está suspendida, pero la página de propiedades de la cuenta tiene el atributo que muestra "Activa", lo que significa que realmente no se puede a volver a activar la cuenta.

En la propia cuenta no hay solución para este problema. La única forma de resolverlo es correlacionar la cuenta a un usuario global y controlar la suspensión de cuentas mediante la suspensión del usuario global.

Los nombres de usuario de VMS no pueden contener caracteres Unicode no de escape

Si se intenta crear una cuenta de VMS con un nombre incorrecto se puede bloquear el servidor de aprovisionamiento que está instalado en Solaris.

El conector de NDS no puede explorar nuevos contenedores

La primera exploración intenta encontrar y agregar contenedores tras adquirir un extremo NDS. Si se agregan contenedores utilizando las herramientas locales de NDS y, a continuación, se intenta volver a explorar el extremo, ni los contenedores recién agregados ni las entradas secundarias aparecerán en el árbol.

El extremo se debe suprimir del servidor de aprovisionamiento y, a continuación, se debe volver a adquirir y explorar para ver los nuevos contenedores.

La descripción del conector de NDS es un campo de un único valor

En el conector de NDS, la descripción de la cuenta es un campo de valor único, pero en el extremo NDS, la descripción de la cuenta es un campo de valor múltiple.

La variable de entorno se debe eliminar o cambiar tras la actualización para evitar problemas con el tipo de extremo del conector UPO

Durante la actualización del superagente remoto al servidor de conector de C++ r12, la variable de entorno ETAHOME puede contener una ruta de instalación incorrecta del CCS y causar problemas con el tipo de extremo del conector UPO. Se debe eliminar manualmente la variable de entorno ETAHOME o cambiarla a la ruta de instalación correcta del CCS después de la actualización antes de intentar adquirir o utilizar el extremo UPO.

La adquisición del extremo UPO no valida el campo de dominio

Un extremo UPO con un valor especificado incorrectamente en el atributo de dominio se adquirirá correctamente. Sin embargo, el extremo generará errores de "Fallo en la búsqueda del servidor de conector: acceso insuficiente" durante la exploración.

Esto se puede solucionar haciendo clic con el botón secundario en el extremo en el Gestor de aprovisionamiento, seleccionado Personalizar -> Actualizar credenciales... y especificando el valor correcto para el dominio.

La comprobación de los parámetros del kernel requeridos no se realiza antes de actualizar los servicios comunes de eTrust a los servicios comunes Enterprise en Solaris

La comprobación de los parámetros del kernel requeridos no se realiza en los productos que actualizan los servicios comunes de eTrust a los servicios comunes Enterprise en Solaris (es más probable que afecte a Solaris 9 que a Solaris 10). Si los parámetros del kernel no son suficientes, se permite que la instalación continúe en lugar de detenerla con una advertencia. Esto afecta a:

- El agente remoto de RSA en Solaris
- IMPS en Solaris
- IMPS SDK

Para resolver este problema:

Ejecute

```
'<directorio del instalador del producto>/solaris/ecs-installation/eCSinstall.sh'
```

Si el kernel no cumple los requisitos, se verá un mensaje informativo. Si se cumplen los requisitos del kernel, el instalador se iniciará.

No se pueden duplicar las cuentas KRB

Si intenta duplicar una cuenta Kerberos en el Gestor de aprovisionamiento, se produce el error "eTKRBFullNameCorrelate not found in the attribute registry! (...) - Return Code: 111". Para solucionar este problema, agregue una cuenta nueva en vez de duplicar la cuenta.

Se produce un error cuando se especifica un territorio no válido al adquirir un extremo KRB

Si intenta adquirir un extremo KRB y especifica un valor no válido para el territorio, aparece un mensaje de error de puntero nulo.

El extremo de seguridad de z/OS bloquea el servidor de aprovisionamiento de Solaris

Si el extremo no se puede conectar al servidor LDAP de CA para z/OS r12, el servidor de aprovisionamiento se bloqueará.

Para resolver este problema, asegúrese de configurar el extremo con la información de conexión válida.

Sincronización de z/OS mediante el extremo de LDS

El agente de sincronización de LDS no está incluido en el DVD del producto de Identity Manager r12. Si necesita este agente, póngase en contacto con soporte técnico.

Mensaje de error de E2K al gestionar los derechos del buzón con Exchange 2007

Los derechos del buzón no se pueden gestionar con Exchange 2007. Se recibirá un mensaje de error del tipo "Mensaje de CAFT: Acceso denegado, o el comando no se ha podido ejecutar".

Error de E2K CAFT al gestionar los derechos del buzón

Es posible que se devuelva un mensaje de error “Mensaje de CAFT: Acceso denegado, o el comando no se ha podido ejecutar” durante la gestión de los derechos del buzón incluso cuando el agente remoto de Exchange esté configurado correctamente.

Esto puede ocurrir cuando la lista de derechos del buzón contiene varios privilegios para el mismo objeto, y ocurre normalmente cuando los objetos de Exchange gestionados heredan derechos del objeto principal.

No se permiten varias direcciones de correo principales de E2K

Mediante el Gestor de aprovisionamiento es posible agregar nuevas direcciones de correo electrónico a una lista existente de direcciones de correo y establecer la nueva dirección como la dirección de correo electrónico principal. Sin embargo, no se disminuye el nivel de la dirección de correo electrónico existente. De esta manera, una cuenta puede tener varias direcciones de correo principales, lo cual no está permitido en el sistema nativo. Para evitar esto, disminuya en primer lugar el nivel de la dirección de correo electrónico principal existente antes de agregar la nueva dirección de correo principal.

Una ruta larga de PKI al archivo INI puede reiniciar el servidor de aprovisionamiento

Las rutas UNC de más de 77 caracteres reiniciarán el sistema operativo. Para resolver este problema, evite utilizar rutas largas.

Las cuentas de PKI aparecen como duplicados

El conector de PKI no es compatible con los extremos jerárquicos de Entrust PKI y almacena todas las cuentas en una lista plana. Por este motivo, aparece una única cuenta de Entrust PKI como duplicado del conector de PKI.

La hoja de propiedades de los grupos PKI no se muestra correctamente

Al intentar abrir una hoja de propiedades de un grupo PKI en el Gestor de aprovisionamiento, se muestra un mensaje de error "No se puede mostrar la hoja de propiedades solicitada".

Advertencia de notificación de correo al crear cuentas PKI

Si se adquiere un extremo PKI utilizando un perfil de proxy y la notificación de correo electrónico está activada, no se puede crear una nueva cuenta PKI sin especificar la opción de crear perfil.

Para solucionar este problema, lleve a cabo una de las siguientes opciones:

- Adquiera el extremo sin el perfil de proxy.
- Desactive las notificaciones de correo electrónico al adquirir el extremo y vaya al extremo para comprobar manualmente el número de referencia

Asignación de tipos de usuario contractuales de SAP

Al asignar un tipo de usuario contractual a un usuario en la ficha de datos de licencia, el cambio sólo se puede aplicar al sistema principal, no a ninguno de los sistemas secundarios.

Los tipos de licencia contractuales para los sistemas secundarios se pueden cambiar de forma nativa.

Campos obligatorios en el atributo de tipo de usuario contractual de SAP

El tipo de usuario contractual que se puede especificar en la ficha de datos de licencia de la cuenta sólo puede tener el campo obligatorio LIC_TYPE. Por ejemplo, si se tiene que especificar el nombre de un sistema SAP R3 (SYSID) para utilizar un tipo de usuario contractual, la asignación fallará y se producirá un error indicando que falta un valor para el nombre del sistema SAP R3.

El servidor de conector de C++ se puede bloquear durante una solicitud al conector de PLS

Si el CCS se ha bloqueado durante una solicitud a un conector PLS, se debe investigar la instalación del servidor de políticas, ya que esta podría ser la causa del problema. El síntoma que se verá será una ralentización significativa en las solicitudes al servidor de políticas debida al reinicio constante del servicio de control de acceso.

Suspensión de cuentas de SBL

Al modificar una cuenta de SBL o una plantilla de cuenta de SBL y sincronizar los cambios con una cuenta, no establezca sTSuspended junto con otras modificaciones, ya que se ignorarán otras modificaciones del atributo.

Para resolver este problema, divida los cambios en dos solicitudes independientes, una que contenga las modificaciones de eTSuspended y otra que contenga los cambios de los valores de cualquier otro atributo.

La función de comprobación de la sincronización de cuenta JIAM RSA funciona incorrectamente

Cuando realiza una operación de comprobación de la sincronización de cuentas en una cuenta RSA mediante JIAM, si el extremo no tiene cuenta, el servidor de conector devuelve, incorrectamente, el error “Connector Server Read failed: Sd_GetSerialByLogin Error Invalid user”, en lugar de devolverlo correctamente con el mensaje “Account missing from endpoint”. Compruebe que la sincronización de la cuenta funciona correctamente en el Gestor de aprovisionamiento.

La supresión de varios grupos del usuario de OS/400 bloquea el Gestor de aprovisionamiento

La supresión de varios grupos de un usuario, en una única operación en la que uno o más grupos comienzan por "#", puede hacer que el Gestor de aprovisionamiento deje de responder.

Para resolver este problema, suprima un grupo cada vez.

La cuenta de OS/400 no puede tener el grupo principal suprimido

Para cambiar la pertenencia al grupo de OS/400, modifique la cuenta que es un miembro del grupo o modifique la pertenencia al grupo. Si se modifica la pertenencia al grupo, las cuentas no se pueden suprimir si su pertenencia al grupo es la pertenencia al grupo principal.

Para resolver este problema, modifique la cuenta y suprima la pertenencia al grupo principal.

El conector de FND debe contener una fecha "Desde" y una fecha "Hasta" en la lista de responsabilidades

El conector de FND debe contener una fecha "Desde" y una fecha "Hasta" en la lista de responsabilidades o, de lo contrario, la lista de responsabilidades se volverá inestable e irrecuperable.

Para resolver este problema, siempre se debe especificar una fecha "Desde" y una fecha "Hasta" en la lista de responsabilidades durante la creación o la modificación de la cuenta FND o de la plantilla de cuenta (por ejemplo, utilizando fechas lejanas en el pasado o en el futuro en lugar de dejar en blanco las fechas "Desde" y "Hasta").

La definición de Host to Caft en Windows Vista no funciona

Si ha instalado el agente remoto de N16 en un extremo de Windows Vista o Windows Vista SP1, y ha intentado agregar el servidor de gestión mediante Todos los programas -> CA - > Identity Manager -> Definición de Host to Caft, y después se intenta adquirir dicho equipo de Windows Vista como extremo, se obtendrá un mensaje de error de "Acceso denegado".

Para resolver este problema, abra una ventana de símbolo del sistema y emita el siguiente comando para adquirir el extremo.

```
cafthost -a <nombrehost/IP>
```

Uso de rutas absolutas para acceder a las ubicaciones de ID personalizados de cuentas LND y a los ID de certificados de unidades de organización

El uso de rutas UNC al acceder a ubicaciones de ID personalizados de cuentas e ID de certificados de unidades de organización no siempre funciona con carpetas compartidas en una ruta relativa. Se recomienda el uso de rutas absolutas (que incluyan la letra de la unidad).

La solicitud de búsqueda LND en SPML no devuelve resultados

La realización de una solicitud de búsqueda en SPML o mediante el servidor de SPML para una cuenta no devuelve resultados cuando se utilizan otros atributos además de lastName y homeServer

La correlación de las cuentas LND y los usuarios globales creados mediante SPML no funciona

En el Gestor de aprovisionamiento, la correlación de las cuentas y de los usuarios globales creados mediante SPML no funciona actualmente.

No utilice caracteres japoneses en los nombres de cuenta LND

En este momento, el cambio de la contraseña del ID no funciona con cuentas que contienen caracteres japoneses en el nombre de cuenta. La utilización de caracteres ingleses en el ID de la cuenta soluciona este problema.

No se pueden crear cuentas LND con "OU único de usuario"

No se pueden crear cuentas con "OU único de usuario". La cuenta resultante no se podrá buscar ni se puede acceder en el Gestor de aprovisionamiento.

El atributo del nombre corto de la cuenta LND no puede contener más de 85 caracteres japoneses.

Se sabe que si se utilizan más de 85 caracteres japoneses en el atributo de nombre corto de la cuenta se produce el bloqueo del servidor Domino. Este problema sólo se produce cuando el nombre de la cuenta también contiene caracteres japoneses.

El Gestor de aprovisionamiento no muestra las pertenencias a grupos de la cuenta LND si contienen caracteres japoneses

En el Gestor de aprovisionamiento, las cuentas creadas en Organización y Unidades de organización que contienen caracteres japoneses no muestran sus pertenencias a grupo en la ficha Miembro de.

No se puede acceder a los ID de cuenta LND y de certificador que contienen caracteres japoneses mediante el conector de LND JCS

No se puede acceder mediante el conector de LND JCS a los ID de cuenta y de certificador que contienen caracteres japoneses. Se sabe que todas las funciones que necesiten acceder a estos archivos de ID fallan en esta versión.

Los caracteres japoneses de las rutas DN del objeto LND pueden causar problemas durante la exploración de directorios

Se sabe que algunos caracteres japoneses de las rutas DN de objetos hacen que el servidor de aprovisionamiento se bloquee durante la exploración de directorios. Entre los ejemplos se incluyen caracteres japoneses con Unicode 0x80fd, 0x4e88, y 0x5642.

El conector de LND no puede realizar un cambio de nombre o un movimiento en la jerarquía en las cuentas LND exploradas

Esta versión del conector de LND no puede realizar las acciones personalizadas Renombrar o Mover en jerarquía en las cuentas LND exploradas. Los campos de atributos están desactivados para estas acciones.

No hay ninguna solución para estas acciones.

La cuenta LND y su archivo de correo no se pueden eliminar utilizando la acción personalizada

La eliminación de una cuenta y del archivo de correo de la cuenta utilizando la acción "personalizada" falla.

El Gestor de aprovisionamiento no genera ningún mensaje de error, pero una inspección del extremo muestra que tanto la cuenta como su archivo de correo todavía siguen presentes. No hay ninguna solución para este problema mediante el Gestor de aprovisionamiento.

Durante el registro no se crean los archivos de correo de la cuenta LND

La ventana de creación de cuentas LND del Gestor de aprovisionamiento contiene una casilla de verificación de creación de réplicas en la página de la ficha Perfil.

Si se está administrando un extremo Domino que se encuentra en un entorno con clústeres, cuando se selecciona la casilla de verificación de creación de réplicas, las réplicas de la cuenta se deben crear en el entorno con clústeres, junto con su archivo de correo asociado. En esta versión, la creación de archivos de correo de réplica no se gestiona durante el registro.

Capítulo 7: Documentación

A continuación se especifican los nombres de archivo de las guías de Identity Manager r12:

Nombre de la guía	Nombre del archivo
Notas de la versión	im_release_enu.pdf
Guía de implementación	im_impl_enu.pdf
Guía de instalación para WebLogic	im_install_weblogic_enu.pdf
Guía de instalación para WebSphere	im_install_websphere_enu.pdf
Guía de instalación para JBoss	im_install_jboss_enu.pdf
Guía de configuración	im_config_enu.pdf
Guía de High Availability	im_high_avail_enu.pdf
Guía de administración	im_admin_enu.pdf
Guía de programación para Java	im_dev_enu.pdf
Guía de programación para aprovisionamiento	im_dev_provisioning_enu.pdf
Guía de aprovisionamiento	im_provisioning_enu.pdf
Guía de conectores	im_connectors_enu.pdf
Guía de Connector Xpress	im_connector_xpress_enu.pdf
Guía de implementación del servidor de conector de Java	im_jcs_impl_enu.pdf
Guía de programación para el servidor de conector de Java	im_jcsProg_Enu.pdf
Guía de integración de iRecorder	audit_im_irec_ref_enu.pdf
Glosario	im_glossary.pdf
Biblioteca	im_bookshelf_enu.zip

Las guías de Identity Manager r12 pueden descargarse en la siguiente ubicación:

- Sitio web de soporte técnico de CA

Para ver los archivos PDF, debe descargar e instalar la versión 7 o superior de Adobe Reader desde el sitio Web de Adobe en caso de que el programa no esté ya instalado en su equipo.

Nota: Para obtener el mejor rendimiento, al instalar la biblioteca en un sistema remoto, haga que se pueda acceder a ella desde un servidor web.

Esta sección contiene los siguientes puntos:

Biblioteca

La biblioteca permite acceder a toda la documentación de Identity Manager desde una única interfaz. Incluye la siguiente información:

- Lista ampliable de contenidos para todas las guías en formato HTML.
- Búsqueda de texto completo en todas las guías con los resultados de la búsqueda clasificados y los términos de la búsqueda resaltados en el contenido.
- Rutas de navegación que enlazan con temas de nivel más alto.
- Un único índice HTML para los temas de todas las guías.
- Enlaces a las versiones en PDF de las guías para imprimirlas.

Para usar la biblioteca

1. Descargue la biblioteca desde el Sitio de soporte de CA.
2. Extraiga el contenido del archivo ZIP.
3. Visualice la biblioteca de esta forma:
   - Si la biblioteca se encuentra en el sistema local y se está utilizando Internet Explorer, abra el archivo Bookshelf.hta.
   - Si la biblioteca se encuentra en un sistema remoto o si se está utilizando Mozilla Firefox, abra el archivo Bookshelf.html.

     Nota: Para obtener el mejor rendimiento, al instalar la biblioteca en un sistema remoto, haga que se pueda acceder a ella desde un servidor web.

La biblioteca necesita Internet Explorer 6 ó 7 o Mozilla Firefox 2. Para los enlaces a las guías en PDF, se necesita Adobe Reader 7 u 8. Adobe Reader se puede descargar en www.adobe.com.

Nota: La biblioteca de CA SiteMinder se ha publicado para r12 y r6.0 SP5 en el sitio Web de soporte técnico de CA utilizando el mismo formato de biblioteca utilizado por Identity Manager.

Mejoras de la ayuda en línea

Tanto la ayuda en línea de la consola de usuario como la ayuda en línea de la consola de gestión presentan ahora las siguientes características:

Rutas de navegación

Indican su posición en la jerarquía de ayuda para facilitar la navegación. Están ubicadas en la parte superior de la página de ayuda.

Búsqueda resaltada

Identifica el contexto de la búsqueda en las páginas de resultados mediante un resalte de color amarillo.

Botones de navegación

Muestra los botones de flecha anterior y siguiente para facilitar la navegación. Están ubicados en la parte superior de la página de ayuda, bajo las rutas de navegación.

Cambio de marca de eTrust a CA

La marca de algunos productos de seguridad de CA actualmente se encuentra en transición de “eTrust” a “CA". Durante esta transición, puede ver referencias tanto a productos de eTrust como a productos de CA en la documentación. Por ejemplo, en la siguiente versión, eTrust Directory cambiará a CA Directory. Cualquier mención a un producto de eTrust dentro de la documentación es equivalente al mismo producto con la nueva marca de CA.

Cambios de la terminología de aprovisionamiento

Los usuarios existentes de eTrust Admin pueden detectar que determinados términos han cambiado ahora que eTrust Admin forma parte de CA Identity Manager. La siguiente tabla muestra estos cambios.

Término de eTrust Admin	Nuevo término en Identity Manager
Servidor de eTrust Admin	Servidor de aprovisionamiento
eTrust Admin Manager	Gestor de aprovisionamiento
Directorio	Extremo, extremos
Espacio de nombres	Tipo de extremo
Política o Política de aprovisionamiento	Plantilla de cuenta
Funciones	Funciones de aprovisionamiento
Marco distribuido del superagente	Marco del servidor de conector
Superagente	Servidor de conector de C++
Opción	Conector
Directorio administrativo o repositorio administrativo	Directorio de aprovisionamiento
Directorio corporativo de Identity Manager	Almacén de usuarios de Identity Manager
Usuario corporativo	Administrador entrante

Nuevo nombre para el conector de EIAM (Embedded IAM)

En la documentación del producto de CA Identity Manager r12, EEM (Embedded Entitlements Manager o Gestor de derechos integrado) hace referencia al conector del EIAM (Embedded Identity and Accesss Manager o Gestor de acceso e identidad integrado).

Documentación de programación

En la documentación de Identity Manager r12 se incluyen dos guías de programación.

Guía de programación para Java

Antes denominada Identity Manager Developer's Guide, esta guía proporciona información sobre el uso de las API para Java de Identity Manager. La versión en HTML está integrada con páginas Javadoc, e incluye los hipervínculos necesarios para establecer referencias cruzadas a la información importante.

Guía de programación para aprovisionamiento

Antes denominada eTrust Admin SDK Developer's Guide, esta guía proporciona información sobre el SDK del servidor de aprovisionamiento de Identity Manager. Los desarrolladores deben tener conocimientos de programación con C++.