CA Identity Manager™

Guía de configuración

12.6.4

Información de contacto del servicio de Soporte técnico

Para obtener soporte técnico en línea, una lista completa de direcciones y el horario de servicio principal, acceda a la sección de Soporte técnico en la dirección http://www.ca.com/worldwide.

Referencias a productos de CA Technologies

Este documento hace referencia a los productos de CA siguientes:

- CA Identity Manager
- CA Siteminder®
- CA Directory
- CA User Activity Reporting
- CA Identity Governance

Contenido

Capítulo 4: Gestión de bases de datos relacionales 103

Capítulo 5: Directorios de CA Identity Manager 157

Capítulo 1: Introducción a los entornos de CA Identity Manager

Esta sección contiene los siguientes temas:

Componentes de entorno de CA Identity Manager

Un *entorno* de CA Identity Manager es una vista de un espacio de nombres de gestión que permite a administradores de CA Identity Manager gestionar objetos como usuarios, grupos y organizaciones. Estos objetos se asignan a un conjunto de roles y tareas asociados. El entorno de CA Identity Manager controla la presentación gráfica y la gestión de un directorio.

Un almacén de usuarios únicos puede asociar varios entornos (en la página 15) de CA Identity Manager para definir vistas diferentes del directorio. Sin embargo, un entorno de CA Identity Manager se asocia solamente a un almacén de usuarios.

Los entornos de CA Identity Manager contienen los siguientes elementos:

Directorio

Describe un almacén de usuarios para CA Identity Manager. El elemento del directorio incluye lo siguiente:

- Un puntero a un almacén de usuarios, que almacena objetos gestionados como usuarios, grupos y organizaciones.
- Metadatos que describen cómo se almacenan los objetos gestionados en el directorio y su representación en CA Identity Manager.

Directorio de aprovisionamiento (opcional)

Almacena datos relevantes en el servidor de aprovisionamiento para gestionar cuentas adicionales en puntos finales gestionados. Solamente se puede asociar un directorio de aprovisionamiento a un Entorno.

Nota: Para obtener más información sobre el servidor de aprovisionamiento o el directorio de aprovisionamiento, consulte la *Guía de instalación*.

Consola de usuario

Permite que los administradores de CA Identity Manager realicen tareas en un entorno de CA Identity Manager.

Definiciones de tareas y roles

Determina los privilegios de usuario en CA Identity Manager y otras aplicaciones. Estas definiciones de tareas y roles se encuentran inicialmente disponibles en el entorno de CA Identity Manager donde se pueden asignar a usuarios.

Se pueden personalizar los roles y las tareas predeterminados mediante la Consola de usuario.

Autoservicio

Permite a los usuarios crear y mantener sus propias cuentas para acceder a recursos, como el sitio web de un cliente. Esta característica también permite a los usuarios solicitar una contraseña temporal en caso de olvidar la contraseña actual.

Definiciones del flujo de trabajo

CA Identity Manager incluye definiciones del flujo de trabajo predeterminadas que automatizan la aprobación y notificación de tareas de gestión de usuarios, como crear perfiles de usuario o asignar usuarios a roles o grupos. Se pueden modificar los procesos del flujo de trabajo predeterminados en CA Identity Manager para que sean compatibles con cada uno de los requisitos empresariales.

Máscaras

Determina el aspecto de la interfaz de usuario de CA Identity Manager.

Funciones personalizadas

Se puede modificar CA Identity Manager para adaptarse a los requisitos de su negocio mediante las API de CA Identity Manager. Consulte la *Guía de programación para Java*.

Cada entorno de CA Identity Manager requiere uno o más gestores del sistema para personalizar los roles y las tareas iniciales mediante la Consola de usuario. Una vez que un gestor del sistema crea los roles y las tareas iniciales, ese gestor puede conceder privilegios administrativos a usuarios en ese entorno. Estos usuarios se convierten en administradores que gestionan usuarios, grupos y organizaciones. Consulte la *Guía de administración*.

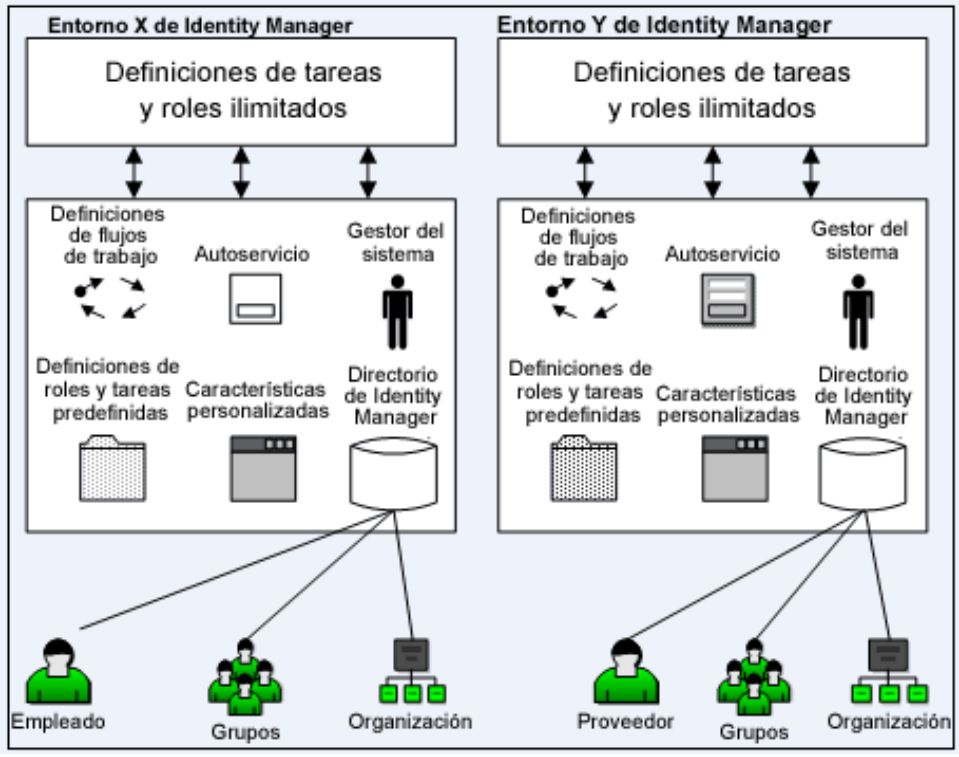
Varios entornos de CA Identity Manager

Cree varios entornos de CA Identity Managercuando desee para llevar a cabo las siguientes acciones:

Gestionar almacenes de usuarios adicionales: se pueden gestionar usuarios en tipos diferentes de almacenes de usuarios. Por ejemplo, su empresa almacena todos sus perfiles de usuario en un directorio LDAP de sistema Sun Java. Se involucra en una empresa conjunta con un partner que utiliza una base de datos de Oracle para almacenar la información de usuarios. Desearía un entorno de CA Identity Manager diferente para cada conjunto de usuarios.

- Gestionar objetos con clases de objeto de LDAP diferentes: se debe considerar la posibilidad de que CA Identity Manager esté gestionando un directorio LDAP. En el mismo directorio, se pueden gestionar objetos del mismo tipo junto con clases de objeto y atributos diferentes. Por ejemplo, en la siguiente ilustración se muestra un directorio que contiene dos tipos de usuarios:
  - Empleados, que tienen un número de ID de empleado.
  - Proveedores, que se identifican con un número de proveedor.

Equation 1: Diagrama que muestra un ejemplo de dos entornos de Identity Manager con directorios que contienen empleados y proveedores.



Consola de gestión de CA Identity Manager

Como administrador del sistema de CA Identity Manager, entre sus responsabilidades se incluyen las siguientes:

- Creación de un directorio de CA Identity Manager
- Configuración de un directorio de aprovisionamiento
- Configuración de un entorno de CA Identity Manager
- Asignación de un gestor del sistema
- Activación de funciones personalizadas para uso inicial

Para configurar un entorno de CA Identity Manager, utilice la Consola de gestión, una aplicación basada en web.

La Consola de gestión se divide en las dos secciones siguientes:

- Directorios: utilice esta sección para crear y gestionar directorios de CA Identity Manager y el directorio de aprovisionamiento, que describe los almacenes de usuarios de CA Identity Manager.
- Entornos: utilice esta sección para crear y gestionar entornos de CA Identity Manager, que controlan la gestión y la presentación gráfica de un directorio.

Cómo acceder a la Consola de gestión de CA Identity Manager

Para acceder a la Consola de gestión, introduzca la siguiente dirección URL en un explorador:

http://*hostname:port*/iam/immanage

nombre de host

Define el nombre de dominio completo o la dirección IP del servidor en el que se ha instalado CA Identity Manager.

Nota: Si está accediendo a la Consola de gestión mediante Internet Explorer 7 y el nombre de host incluye una dirección IPv6, se mostrará de forma incorrecta la Consola de gestión. Para impedir que se produzca esta incidencia, utilice el nombre de host completo o una dirección de IPv4.

puerto

Define el puerto de servidor de aplicaciones.

Nota: Si se está utilizando un agente Web para proporcionar autenticación avanzada para CA Identity Manager, no se tendrá que especificar el número de puerto.

Nota: Active Javascript en el explorador que utiliza para acceder a la Consola de gestión.

Rutas de ejemplo a la Consola de gestión:

- Para Geologic Weblogs:

  http://miservidor.miempresa.org:7001/iam/immanage

- Para JBoss:

  http://miservidor.miempresa.org:8080/iam/immanage

- Para WebSphere:

  http://miservidor.miempresa.org:9080/iam/immanage

Cómo crear un entorno de CA Identity Manager

Para crear un entorno de CA Identity Manager, complete los siguientes pasos en la Consola de gestión:

1. Utilice al asistente de configuración de directorios (en la página 159) para crear un directorio de CA Identity Manager.
2. Si su entorno incluye aprovisionamiento, vuelva a utilizar el asistente de configuración de directorios para crear un directorio de aprovisionamiento (en la página 174).
3. Cree un entorno de CA Identity Manager.
4. Acceda al entorno (en la página 196) para verificar que se está ejecutando.

Capítulo 2: Entorno de CA Identity Manager de ejemplo

Esta sección contiene los siguientes temas:

Descripción general de entorno de CA Identity Manager de ejemplo

CA Identity Manager incluye un entorno de ejemplo que se puede utilizar para obtener información sobre CA Identity Manager y probarlo.

El entorno de ejemplo se basa en una empresa comercial de automóviles denominada "NeteAuto". Los administradores de NeteAuto utilizan CA Identity Manager para gestionar empleados, proveedores y franquicias regionales.

Las configuraciones de almacén de usuarios para utilizar entornos de NeteAuto de ejemplo son las siguientes:

- Almacenes de usuario de LDAP que son compatibles con organizaciones.
- Almacenes de usuario LDAP que no son compatibles con organizaciones.
- Almacenes de usuarios de base de datos relacionales que son compatibles con organizaciones.
- Almacenes de usuario de LDAP que no son compatibles con organizaciones.

Nota: Las capacidades de aprovisionamiento no están disponibles debido a que este entorno no tiene ningún directorio de aprovisionamiento.

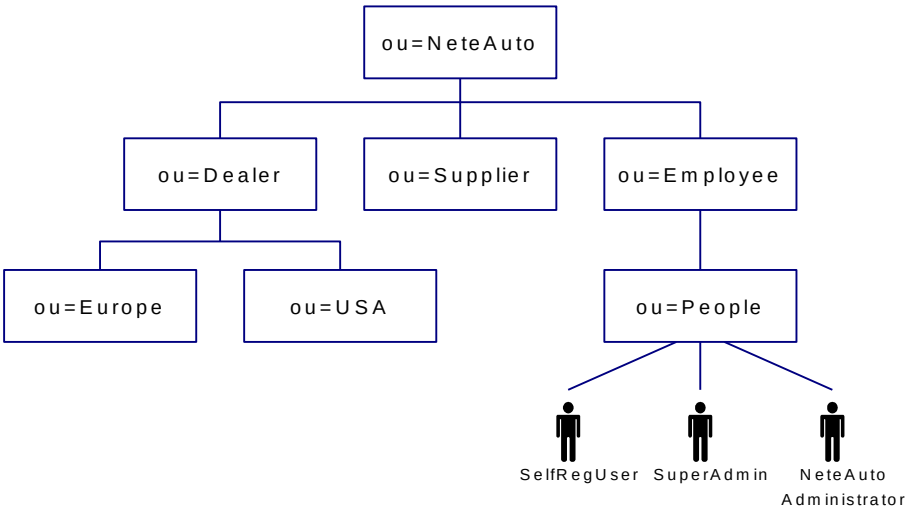
Cómo configurar el ejemplo de NeteAuto con compatibilidad con organizaciones

La configuración del ejemplo de NeteAuto con compatibilidad con organizaciones requiere llevar a cabo los siguientes pasos:

- Instalación del software de requisito previo
- Instalación del entorno de CA Identity Manager de ejemplo
- Configuración de un directorio de usuarios de LDAP
- Configuración de una base de datos relacional
- Creación del directorio de CA Identity Manager
- Creación del entorno de CA Identity Manager de NeteAuto

Estructura de directorios de LDAP para NeteAuto

En la siguiente ilustración se describe el ejemplo de NeteAuto para directorios de LDAP:



El entorno de CA Identity Manager de ejemplo incluye los siguientes usuarios:

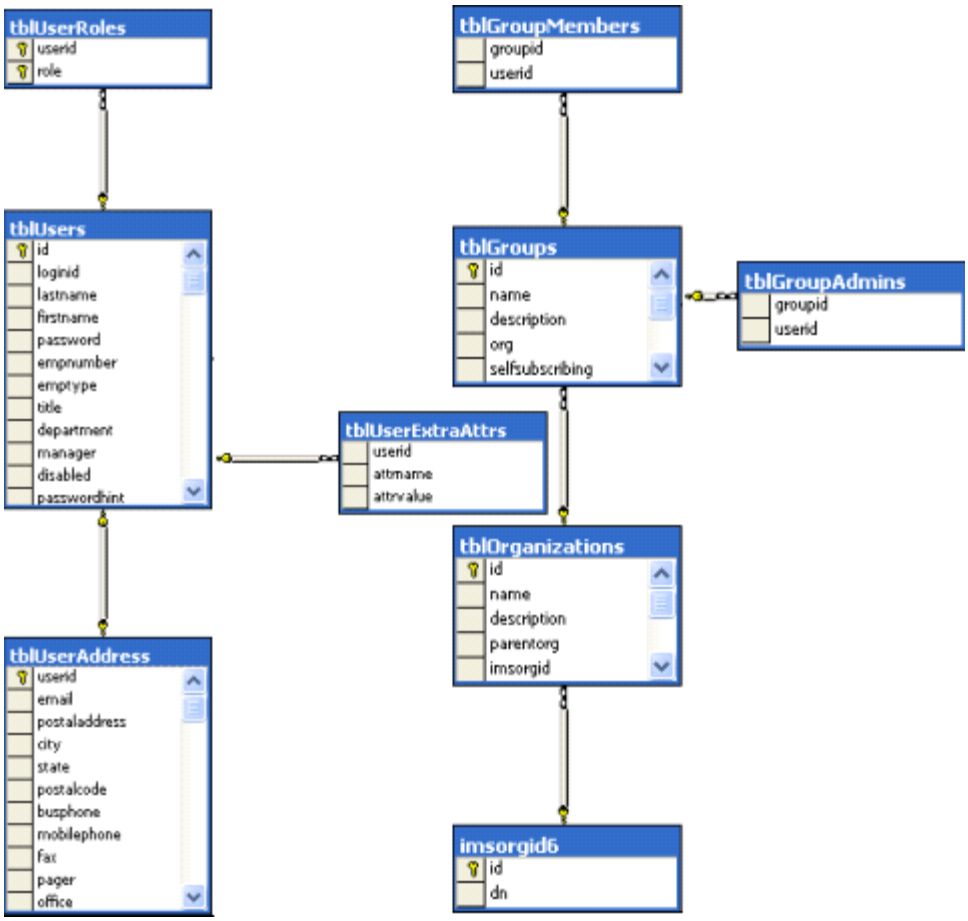
- Superadmin (Superadministrador) es la cuenta de administrador con el rol de gestor del sistema para este entorno de CA Identity Manager. Como Superadmin (Superadministrador), se pueden realizar todas las tareas de administración predeterminadas.

  Nota: Para ver una descripción de las tareas de administración predeterminadas, consulte la *Guía de administración*.

- SelfRegUser es la cuenta de administrador que CA Identity Manager utiliza para activar el autorregistro de este entorno de CA Identity Manager.
- El administrador de NeteAuto no tiene privilegios cuando se instala el entorno de NeteAuto. Sin embargo, se le puede asignar Gestor de grupos como rol de usuario, tal y como se describe en Asignación del rol Gestor de grupos.

Base de datos relacional para NeteAuto

En la siguiente ilustración se describe la base de datos relacional para el ejemplo de NeteAuto que incluye una tabla de organización:



Software de requisito previo para NeteAuto

El entorno de NeteAuto CA Identity Manager tiene los siguientes requisitos previos:

- Instale CA Identity Manager tal y como se describe en la *Guía de instalación*. Asegúrese de instalar las herramientas administrativas de CA Identity Manager.
- Se debe tener acceso a un servidor de directorio de sistema Sun Java (Sun ONE o iPlanet) o una base de datos de Microsoft SQL Server.

Archivos de instalación para el entorno de NeteAuto

CA Identity Manager incluye un conjunto de archivos que se pueden utilizar para configurar un entorno de CA Identity Manager de ejemplo. El entorno de CA Identity Manager es una vista de un espacio de nombres de gestión que permite que los administradores de CA Identity Manager gestionen objetos como usuarios, grupos y organizaciones. Estos objetos se gestionan junto con un conjunto de roles y tareas asociados. El entorno de CA Identity Manager controla la presentación gráfica y la gestión de un directorio.

El entorno de CA Identity Manager de ejemplo incluye lo siguiente:

- Objetos de ejemplo, como usuarios y organizaciones.
- Definiciones de pantallas, tareas y roles.

  Las tareas se muestran en la Consola de usuario al hacer clic en una ficha, como Usuarios o Grupos. En función de los roles asignados, las tareas asociadas se muestran cuando el usuario inicia sesión.

  Nota: Para obtener más información sobre las tareas y los roles, consulte la *Guía de administración*.
- Una máscara de ejemplo que personaliza la Consola de usuario para usuarios de NeteAuto.
- Un archivo de configuración del directorio que utiliza para crear un directorio de CA Identity Manager.

Los archivos para crear el entorno de CA Identity Manager de ejemplo se instalan en la ubicación siguiente:

admin_tools\samples\NeteAuto

En esta ruta, *admin_tools* hace referencia a las herramientas administrativas. Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Instale el entorno de NeteAuto.

Lleve a cabo el siguiente proceso para instalar el entorno de NeteAuto.

Siga estos pasos:

1. Asegúrese de que se instala el software de requisito previo (en la página 22).
2. Configurar el almacén de usuarios e importe los datos de ejemplo.
   - Para usuarios de LDAP: Configuración de un directorio de usuarios de LDAP (en la página 23)
   - Para usuarios de bases de datos relacionales: Configuración de una base de datos relacional
3. Cree el directorio de CA Identity Manager de NeteAuto.
4. Cree el entorno de CA Identity Manager de NeteAuto.
5. Configure la apariencia de la interfaz de usuario de CA Identity Manager para usuarios de NeteAuto (en la página 39).

Configuración de un directorio de usuarios de LDAP

El directorio LDAP está disponible en función de la instalación. Se puede utilizar el siguiente procedimiento para comprobar si el directorio existe, o bien para crearlo.

Siga estos pasos:

1. En la consola de servidor de directorio, cree una instancia de LDAP con la siguiente raíz:

   ```
   dc=security,dc=com
   ```

   Apuntar el número de puerto para futuras referencias.

2. Importe el archivo NeteAuto.ldif en el servidor de directorio desde samples\NeteAuto en las herramientas administrativas.

   Las herramientas administrativas están instaladas en las siguientes ubicaciones predeterminadas:

   - **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Nota: Si se experimentan problemas al importar el archivo LDIF o al crear el directorio de CA Identity Manager, agregue el siguiente texto al inicio del archivo de LDIF:

```
dn: dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

Guarde el archivo y repita los pasos 1 y 2.

Configuración de una base de datos relacional

Lleve a cabo el siguiente procedimiento para configurar una base de datos relacional.

Siga estos pasos:

1. Crear una instancia de base de datos denominado "NeteAuto".
2. Cree un usuario denominado "neteautoadmin" con la prueba de contraseña. Conceda derechos a "neteautoadmin" (como los derechos public y db_owner) a NeteAuto editando las propiedades del usuario.

   Nota: Para crear una base de datos de NeteAuto, el rol de neteautoadmin debe tener, al menos, permisos mínimos (seleccionar, insertar, actualizar y suprimir) para todas las tablas que se creen mediante el script de SQL. Además, neteautoadmin debe ser capaz de ejecutar todos los procedimientos almacenados, si los hay, que se han definido en estos scripts.
3. Al editar propiedades del usuario, convierta NeteAuto en la base de datos predeterminada de neteautoadmin.

4. Ejecute los scripts siguientes en el orden en el que se muestran:
   - *db_type*-rdbuserdirectory.sql: configura las tablas para el ejemplo de NeteAuto y crea las entradas de usuario.
   - ims_*db_type*_rdb.sql: configura la compatibilidad con las organizaciones.

     db_type

     Define Microsoft SQL u Oracle en función del tipo de base de datos que se vaya a configurar.

   Estos archivos de script se encuentran en la carpeta *admin_tools*\samples\NeteAutoRDB\Organization. En este ejemplo, *admin_tools* hace referencia a las herramientas administrativas, que se instalan en las ubicaciones predeterminadas siguientes:
   - **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
5. Defina un origen de datos de JDBC denominado "neteautoDS" que apunte a la base de datos de NeteAuto.

   El procedimiento para configurar un origen de datos depende del tipo de servidor de aplicaciones donde se instale CA Identity Manager. En la sección Cómo crear un origen de datos JDBC (en la página 107) se incluyen instrucciones específicas de servidor de aplicaciones sobre cómo crear un origen de datos de JDBC.

Cree el directorio de CA Identity Manager.

Se debe realizar el procedimiento siguiente para crear un directorio de CA Identity Manager.

Siga estos pasos:

1. Abra la Consola de gestión de introduciendo la siguiente URL en un explorador:

   http://*im_server:port*/iam/immanage

   im_server

   Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager.

   puerto

   Define el número de puerto de servidor de aplicaciones.
2. Haga clic en Directorios.
3. Haga clic en Crear en el asistente para iniciar al asistente de directorio de CA Identity Manager.

4. Busque el archivo configuration.xml del directorio adecuado y haga clic en Siguiente.

   El archivo de configuración del directorio se encuentra en las siguientes carpetas:

   - Para directorios de usuarios de servidor de directorio de sistema Sun Java:

     admin_tools\samples\NeteAuto\Organization\directory.xml

   - Para bases de datos relacionales:

     admin_tools\samples\NeteAutoRDB\Organization*db_type* directory.xml

     admin_tools

     Define la ubicación de instalación de las herramientas administrativas.

     Las herramientas administrativas están instaladas en las siguientes ubicaciones predeterminadas:

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

     UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

     db_type

     Especifica el tipo de base de datos que se va a configurar: Microsoft SQL u Oracle.

   La información de estado se muestra en la pantalla de salida de configuración de directorios.

5. En la segunda página del asistente, indique los siguientes valores:

   - Servidor de directorio de sistema Sun Java

     Nombre

     NeteAuto Directory

     Descripción

     Sample NeteAuto directory (Directorio de NeteAuto de ejemplo)

     Connection Object Name (Nombre del objeto de conexión)

     NeteAuto Users (Usuarios de NeteAuto)

     Host

     Nombre o dirección IP del equipo donde se ha instalado el almacén de usuarios.

     Puerto

     Número de puerto para el almacén de usuarios

     Raíz de búsqueda

     dc=security, dc=com

Nombre de usuario

Nombre de usuario para una cuenta que puede acceder al almacén de usuarios.

Contraseña y Confirmar contraseña

Contraseña de la cuenta de usuario

- Bases de datos de Microsoft SQL Server y Oracle

  Nombre

  NeteAutoRDB Directory

  Descripción

  Sample NeteAuto directory (Directorio de NeteAuto de ejemplo)

  Connection Object Name (Nombre del objeto de conexión)

  NeteAutoRDB

  JDBC Data Source (Origen de datos de JDBC)

  neteautoDS

  Nombre de usuario

  Neteautoadmin

  Contraseña

  Probar

6. Haga clic en Siguiente.
7. Haga clic en Finalizar para salir del asistente.

Creación del entorno de CA Identity Manager de NeteAuto

Se debe llevar a cabo el procedimiento siguiente para crear el entorno de NeteAuto de CA Identity Manager.

Siga estos pasos:

1. En la Consola de gestión, haga clic en Entornos.
2. En la pantalla de entornos de CA Identity Manager, haga clic en New (Nuevo).

   Se mostrará el asistente de entornos de CA Identity Manager.
3. En la primera página del asistente, introduzca los siguientes valores:

   Nombre del entorno

   Entorno de NeteAuto

Descripción

Entorno de ejemplo

Alias

Neteauto

El alias se agrega a la dirección URL para acceder al entorno de CA Identity Manager. Por ejemplo, la dirección URL para acceder al entorno de neteauto es:

http://*server_name*/iam/im/neteauto

server_name

Define el nombre de dominio completo del servidor en el que se ha instalado CA Identity Manager. Por ejemplo:

http://miservidor.miempresa.org/iam/im/neteauto

Nota: El alias mayúsculas de minúsculas.

Haga clic en Siguiente.

4. Seleccione el directorio de CA Identity Manager para asociarlo al entorno que vaya a crear:
   - Para servidores de directorio de sistema Sun Java, use el directorio de NeteAuto.
   - Para bases de datos de Microsoft SQL Server use Oracle, use el directorio de NeteAutoRDB.

   Haga clic en Siguiente.
5. Configure la compatibilidad con tareas públicas (como las de autorregistro y de contraseña olvidada) tal y como se muestra a continuación:
   a. Escriba el siguiente alias para tareas públicas:

      Neteautopublic

   b. Introduzca SelfRegUser como la cuenta de usuario anónima.
   c. Haga clic en Validar para ver el identificador único de usuario.

   Nota: Los usuarios no necesitan iniciar sesión para utilizar tareas públicas.
6. Seleccione las tareas y los roles con objeto de crearlos para el entorno de NeteAuto:
   a. Seleccione la opción de importación de roles del archivo.
   b. Busque una de las siguientes ubicaciones:
      - Busque un almacén de usuarios de servidor de directorio de sistema Sun Java:

        admin_tools\samples\NeteAuto\RoleDefinitions.xml

- Para un almacén de usuarios de Microsoft SQL Server:

  admin_tools\samples\NeteAutoRDB\Organization\mssqlRoleDefinitions.xml

- Para un almacén de usuarios de Oracle:

  admin_tools\samples\NeteAutoRDB\Organization\oracleRoleDefinitions.xml

admin_tools hace referencia a las herramientas administrativas, que se instalan en la siguiente ubicación de forma predeterminada:

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

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

7. Especifique un usuario para que haga las funciones del gestor del sistema para este entorno y haga clic en Siguiente:
   a. Escriba "SuperAdmin" en el campo Gestor del sistema.
   b. Haga clic en Agregar.

      CA Identity Manager agrega el identificador único del usuario Superadmin (Superadministrador) a la lista de usuarios.
   c. Haga clic en Siguiente.
8. Consulte la configuración del entorno y lleve a cabo las siguientes tareas:
   - (Opcional) Haga clic en Anterior para modificar.
   - Haga clic en Finalizar para crear el entorno de CA Identity Manager con la configuración actual.

     La pantalla de salida de configuración del entorno muestra el progreso de la creación de este.
9. Haga clic en Continuar para salir del asistente de entornos de CA Identity Manager.
10. Inicie el entorno de CA Identity Manager.

Una vez que se cree el entorno de NeteAuto, podrá hacer lo siguiente:

- Creación de una máscara para este entorno de CA Identity Manager (en la página 39).
- Acceso al entorno. (en la página 37)

Cómo configurar el ejemplo NeteAuto sin compatibilidad con organizaciones

La configuración del ejemplo de NeteAuto sin compatibilidad con organizaciones requiere llevar a cabo los siguientes pasos:

- Instalación del software de requisito previo (en la página 22)
- Instalación del entorno de CA Identity Manager de ejemplo
- Configuración de la base de datos
- Creación de un origen de datos de JDBC
- Creación del directorio de CA Identity Manager
- Creación del entorno de CA Identity Manager de NeteAuto

Descripción del entorno de CA Identity Manager de ejemplo

Para bases de datos de Microsoft SQL Server y Oracle, CA Identity Manager incluye una versión del entorno de NeteAuto que no incluye organizaciones. Este entorno de CA Identity Manager incluye los tres usuarios siguientes:

- Superadmin (Superadministrador) es la cuenta de administrador con el rol de gestor del sistema para este entorno de CA Identity Manager. Como Superadmin (Superadministrador), se pueden realizar todas las tareas de administración predeterminadas.

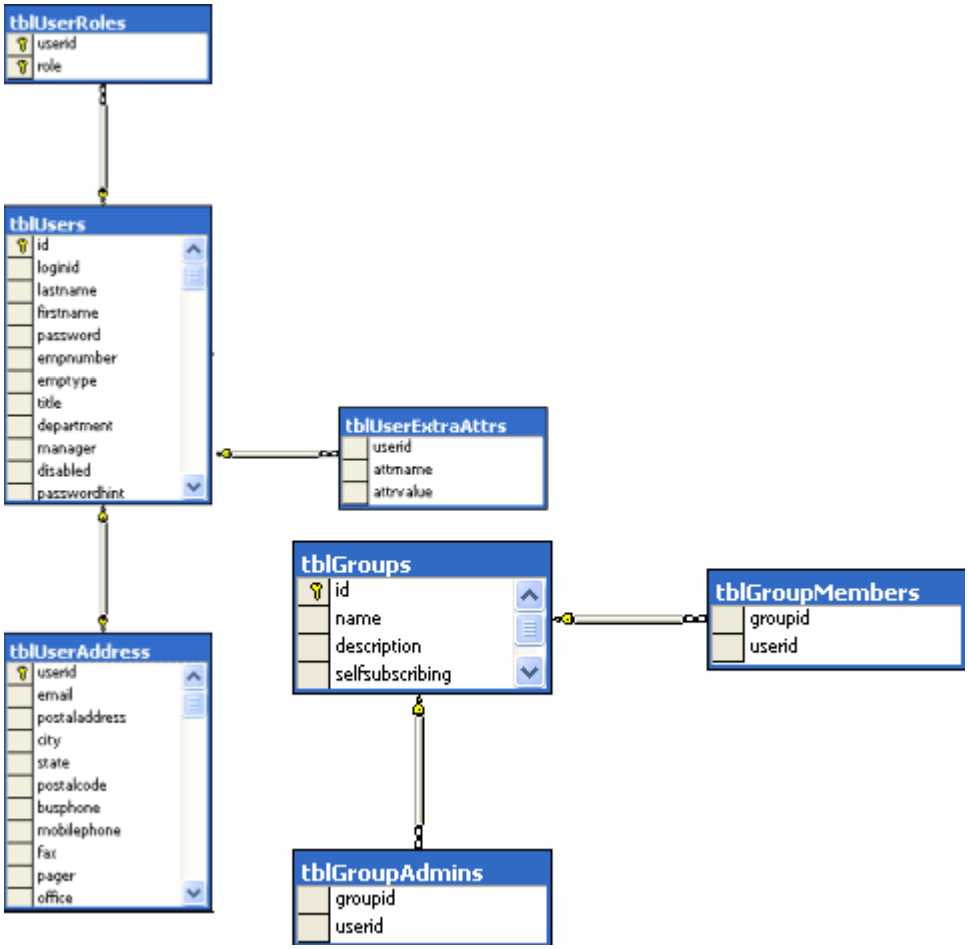
  Nota: Para ver una descripción de las tareas de administración predeterminadas, consulte la *Guía de administración*.

- SelfRegUser es la cuenta de administrador que CA Identity Manager utiliza para activar el autorregistro de este entorno de CA Identity Manager.

- El administrador de NeteAuto no tiene privilegios cuando se instala el entorno de NeteAuto.

  Sin embargo, se puede asignar el rol de gestor de grupos a la cuenta de administrador de NeteAuto.

En la siguiente ilustración se describe el ejemplo de NeteAuto para una base de datos relacional sin organizaciones:



Archivos de instalación para el entorno de Neteauto

CA Identity Manager incluye un conjunto de archivos que se pueden utilizar para configurar un entorno de CA Identity Manager de ejemplo. Un entorno de CA Identity Manager es una vista de un espacio de nombres de gestión que permite a los administradores de CA Identity Manager gestionar objetos. Estos objetos (como usuarios y grupos) tienen asociados un conjunto de roles y tareas. Un entorno de CA Identity Manager controla la presentación gráfica y la gestión de un almacén de usuarios.

El entorno de CA Identity Manager de ejemplo incluye lo siguiente:

- Usuarios de ejemplo
- Definiciones de pantallas, tareas y roles.

  Las tareas se muestran en la Consola de usuario al hacer clic en una categoría, como usuarios o grupos. Las tareas que se muestran se basan en los roles que se hayan asignado al usuario.

  Nota: Para obtener más información sobre las tareas y los roles, consulte la *Guía de administración*.
- Una máscara de ejemplo que personaliza la Consola de usuario para usuarios de NeteAuto.
- Un archivo de configuración del directorio que utiliza para crear un directorio de CA Identity Manager.

Los archivos para crear el entorno de CA Identity Manager de ejemplo se instalan en la ubicación siguiente:

admin_tools\samples\NeteAutoRDB\NoOrganization

En esta ruta, *admin_tools* hace referencia a las herramientas administrativas.

Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Cómo instalar el entorno de NeteAuto Environment (sin compatibilidad con organizaciones)

Lleve a cabo el siguiente proceso para instalar el entorno de NeteAuto.

Siga estos pasos:

1. Verifique que el software de requisito previo (en la página 33) se haya instalado.
2. Configure la base de datos. (en la página 24)
3. Cree el directorio de CA Identity Manager. (en la página 34)
4. Cree el entorno de CA Identity Manager de NeteAuto. (en la página 36)
5. Configure la apariencia de la interfaz de usuario de CA Identity Manager (en la página 39) para usuarios de NeteAuto.

Software de requisito previo

El entorno de NeteAuto CA Identity Manager tiene los siguientes requisitos previos:

- Instale CA Identity Manager tal y como se describe en la *Guía de instalación*. Compruébela para instalar las herramientas administrativas de CA Identity Manager.
- Se debe tener acceso a una base de datos de Microsoft SQL Server u Oracle.

Configuración de una base de datos relacional

Lleve a cabo el siguiente procedimiento para configurar una base de datos relacional.

Siga estos pasos:

1. Crear una instancia de base de datos denominado "NeteAuto".
2. Cree un usuario denominado "neteautoadmin" con la prueba de contraseña. Conceda derechos a "neteautoadmin" (como los derechos public y db_owner) a NeteAuto editando las propiedades del usuario.

   Nota: Para crear una base de datos de NeteAuto, el rol de neteautoadmin debe tener, al menos, permisos mínimos (seleccionar, insertar, actualizar y suprimir) para todas las tablas que se creen mediante el script de SQL. Además, neteautoadmin debe ser capaz de ejecutar todos los procedimientos almacenados, si los hay, que se han definido en estos scripts.
3. Al editar propiedades del usuario, convierta NeteAuto en la base de datos predeterminada de neteautoadmin.
4. Ejecute los scripts siguientes en el orden en el que se muestran:
   - *db_type*-rdbuserdirectory.sql: configura las tablas para el ejemplo de NeteAuto y crea las entradas de usuario.
   - ims_*db_type*_rdb.sql: configura la compatibilidad con las organizaciones.

     db_type

     Define Microsoft SQL u Oracle en función del tipo de base de datos que se vaya a configurar.

   Estos archivos de script se encuentran en la carpeta *admin_tools*\samples\NeteAutoRDB\Organization. En este ejemplo, *admin_tools* hace referencia a las herramientas administrativas, que se instalan en las ubicaciones predeterminadas siguientes:

   - **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

5. Defina un origen de datos de JDBC denominado "neteautoDS" que apunte a la base de datos de NeteAuto.

   El procedimiento para configurar un origen de datos depende del tipo de servidor de aplicaciones donde se instale CA Identity Manager. En la sección Cómo crear un origen de datos JDBC (en la página 107) se incluyen instrucciones específicas de servidor de aplicaciones sobre cómo crear un origen de datos de JDBC.

Cree el directorio de CA Identity Manager.

Se debe realizar el procedimiento siguiente para crear el directorio de CA Identity Manager.

Siga estos pasos:

1. Abra la Consola de gestión de introduciendo la siguiente URL en un explorador:

   http://*im_server*:*port*/iam/immanage

   im_server

   Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager.

   puerto

   Define el número de puerto de servidor de aplicaciones.

2. Haga clic en Directorios.

   Se mostrará la pantalla de directorios de CA Identity Manager.

3. Haga clic en Nuevo para iniciar al asistente de directorios de CA Identity Manager.

4. Busque uno de los archivos XML de configuración del directorio siguientes y haga clic en Siguiente:

   - Sistemas Sun Java:

     admin_tools\samples\NeteAuto\NoOrganization\directory.xml

   - Bases de datos de SQL Server:

     admin_tools\samples\NeteAuto\NoOrganization\mssql-directory.xml

   - Bases de datos de Oracle:

     admin_tools\samples\NeteAuto\NoOrganization\oracle-directory.xml

   admin_tools hace referencia a las herramientas administrativas, que se instalan en la siguiente ubicación de forma predeterminada:

   - **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   La información de estado se muestra en la pantalla de salida de configuración de directorios.

5. En la segunda página del asistente, indique los siguientes valores:

   Nombre

   NeteAutoRDB Directory

   Descripción

   Directorio de NeteAuto de ejemplo sin compatibilidad con organizaciones

   Connection Object Name (Nombre del objeto de conexión)

   NeteAutoRDB

   JDBC Data Source (Origen de datos de JDBC)

   neteautoDS

   Nombre de usuario

   neteautoadmin

   Contraseña

   test

6. Haga clic en Siguiente.
7. Haga clic en Finalizar para salir del asistente.

Creación del entorno de CA Identity Manager de NeteAuto

Se debe llevar a cabo el procedimiento siguiente para crear el entorno de NeteAuto de CA Identity Manager.

Siga estos pasos:

1. En la Consola de gestión, haga clic en Entornos.
2. En la pantalla de entornos de CA Identity Manager, haga clic en New (Nuevo).

   Se abrirá el asistente de entornos de CA Identity Manager.
3. En la primera página del asistente, escriba los valores siguientes:
   - Nombre de entorno: entorno de NeteAuto
   - Descripción: NeteAuto es un entorno de ejemplo.
   - Alias: neteautoRDB

     El alias se agrega a la dirección URL para acceder al entorno de CA Identity Manager. Por ejemplo, la dirección URL para acceder al entorno de neteauto es:

     `http://domain/iam/im/neteautoRDB`

     En esta ruta, el *dominio* define el nombre de dominio completo del servidor donde se ha instalado CA Identity Manager, como en el siguiente ejemplo:

     `http://myserver.mycompany.org/iam/im/neteautoRDB`

     Nota: El alias mayúsculas de minúsculas.

   Haga clic en Siguiente.
4. Seleccione el directorio de CA Identity Manager de directorio de NeteAutoRDB para asociarse al entorno que se va a crear y haga clic en Siguiente.
5. Configure la compatibilidad con tareas públicas (como las de autorregistro y de contraseña olvidada).

   Nota: Los usuarios no necesitan iniciar sesión para acceder a las tareas públicas.

   a. Escriba el siguiente alias para tareas públicas:

      neteautoRDBpublic

   b. Escriba SelfRegUser como la cuenta de usuario anónima.

   c. Haga clic en Validar para ver el identificador único de usuario (2, en este caso).
6. Seleccione las tareas y los roles con objeto de crearlos para el entorno de NeteAuto:
   - Seleccione la opción de importación de roles del archivo.

- Vaya hasta la siguiente ubicación:

  im_admin_tools_dir\samples\NeteAutoRDB\NoOrganizations\RoleDefinitions.xml

  En esta ruta, *im_admin_tools_dir* define la ubicación de instalación de las herramientas administrativas de CA Identity Manager.

7. Especifique un usuario para que haga las funciones del gestor del sistema para este entorno y haga clic en Siguiente:
   a. Escriba "SuperAdmin" en el campo Gestor del sistema.
   b. Haga clic en Agregar.
   c. Haga clic en Siguiente.
8. Revise la configuración del entorno.
   - Haga clic en Anterior para modificar.
   - Haga clic en Finalizar para crear el entorno de CA Identity Manager con la configuración actual.

     La pantalla de salida de configuración del entorno muestra el progreso de la creación de este.
9. Haga clic en Finalizar para salir del asistente de entornos de CA Identity Manager.
10. Inicie el entorno de CA Identity Manager.

Una vez que se cree el entorno de NeteAuto, podrá hacer lo siguiente:

- Cree una máscara para este entorno de CA Identity Manager tal y como se describe en la sección de configuración de la máscara de NeteAuto (en la página 39).
- Acceda al entorno tal y como se describe en la sección de uso del entorno de CA Identity Manager de NeteAuto.

Cómo usar el entorno de CA Identity Manager de NeteAuto

Se puede utilizar el entorno de CA Identity Manager de NeteAuto para gestionar las tareas y los usuarios de autoservicio.

Gestión de tareas de autoservicio

Entre las tareas de autoservicio se incluyen las siguientes:

- Registro como nuevo usuario
- Inicio de sesión como un usuario autorregistrado
- Uso de la función de contraseña olvidada

Registro como nuevo usuario

Lleve a cabo el siguiente procedimiento para registrarse como nuevo usuario.

Siga estos pasos:

1. Escriba la siguiente dirección URL en un explorador:

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration`

   nombre de host

   Define el nombre de dominio completo del sistema en el que se ha instalado CA Identity Manager.

   Nota: Si no se ha configurado la máscara (en la página 39) de Neteauto, se puede omitir imcss de la dirección URL tal y como se muestra a continuación:

   http://*hostname*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   Esta dirección URL redirige a la consola de gestión predeterminada.

   En el autorregistro: página de acuerdo de licencia de usuario final, CA Identity Manager muestra el sitio web de CA.

   Nota: Se puede configurar la tarea de autorregistro predeterminada para mostrar el acuerdo de licencia de usuario final personalizado. Para obtener instrucciones, consulte la *Guía de administración*.

2. Haga clic en Aceptar para continuar.
3. En la ficha Perfil, indique los siguientes detalles:
   a. Escriba valores para los campos obligatorios e indíquelos con un asterisco (*).
   b. Escriba respuestas y sugerencias de contraseña.

      Para casos de contraseñas olvidadas, CA Identity Manager proporciona la sugerencia de contraseña y solicita la respuesta. Si la respuesta es correcta, CA Identity Manager pide al usuario que especifique y confirme una contraseña nueva.
4. Deje sin cambios la ficha Grupos.
5. Haga clic en Enviar.

Inicio de sesión como usuario autorregistrado

Se debe llevar a cabo el procedimiento siguiente para conectarse como un usuario autorregistrado.

Siga estos pasos:

1. Escriba la siguiente dirección URL para el entorno de CA Identity Manager de NeteAuto en un explorador:

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   nombre de host

   Define el nombre de dominio completo del sistema en el que se ha instalado CA Identity Manager.

2. Inicie sesión utilizando el nombre del usuario y la contraseña que se especificó al registrarse.

Configuración de la máscara de NeteAuto

Para configurar la máscara de NeteAuto, cree una respuesta de SiteMinder en el servidor de políticas de SiteMinder.

Siga estos pasos:

1. Inicie sesión en una de las siguientes interfaces como administrador con privilegios del dominio:

   - Para CA SiteMinder Web Access Manager r12 o posterior, inicie sesión en la interfaz de usuario administrativa.
   - Para CA eTrust SiteMinder 6.0 SP5, inicie sesión en la interfaz de usuario del servidor de políticas.

   Nota: Para obtener información sobre el uso de estas interfaces, consulte la documentación de la versión de SiteMinder que esté utilizando.

2. Abra neteautoDomain.

3. En neteautoDomain, seleccione Territorios.

   Se mostrarán los siguientes mensajes:

   neteauto_ims_realm

   Protege el entorno de CA Identity Manager.

   neteauto_pub_realm

   Permite la compatibilidad con tareas públicas, como las de autorregistro y contraseña olvidada.

4. Cree una regla en cada uno de los territorios. Especifique los siguientes detalles:
   - Recurso: *
   - Acciones: GET y POST

   Para simplificar la administración, incluya la máscara de NeteAuto en el nombre de la regla.
5. Cree una respuesta para el dominio con los siguientes atributos de respuesta:
   - Atributo: WebAgent-HTTP-Header-Variable

     Este atributo agrega un encabezado HTTP nuevo a la respuesta.
   - Tipo de atributo: estático
   - Nombre de variable: máscara

     Valor variable: neteauto
6. Modifique la política que CA Identity Manager ha creado en neteautoDomain. Especifique los siguientes detalles:
   - Usuarios
     - Para LDAP: seleccione ou=Persona, ou=Empleados, ou=NeteAuto en los miembros disponibles y agréguelos a los miembros actuales. Haga clic en Aceptar.
     - Para bases de datos relacionales: busque usuarios cuyos atributos de ID sean equivalentes a *. Seleccione todos los usuarios en los miembros disponibles y agréguelos a los miembros actuales. Haga clic en Aceptar.
   - Reglas:
     - Agregue las reglas creadas en el paso 4.
     - Para cada regla, haga clic en la opción de establecer respuesta. Asocie cada regla con la respuesta creada en el paso 5.

Nota: La máscara de neteauto se basa en la consola de imcss. Para ver la máscara, anexe /imcss/index.jsp a la dirección URL para el entorno de CA Identity Manager de NeteAuto tal y como se muestra a continuación:

http://*hostname*/iam/im/neteauto/imcss/index.jsp

Acceda al entorno (en la página 42) de CA Identity Manager de NeteAuto para obtener instrucciones detalladas sobre cómo acceder al entorno de Neteauto.

Uso de la función de contraseña olvidada

Se debe llevar a cabo el procedimiento siguiente para utilizar la función de contraseña olvidada.

Siga estos pasos:

1. Escriba la siguiente dirección URL en un explorador:

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset`

   nombre de host

   Define el nombre de dominio completo del sistema en el que se ha instalado CA Identity Manager.

2. Escriba el identificador único para el usuario autorregistrado creado en Registro como nuevo usuario (en la página 38) y haga clic en Siguiente.
3. Cada vez que se le pregunte, responda a la pregunta de verificación. La respuesta es la que se haya indicado durante el registro.

   Nota: Se requiere una respuesta correcta para cada pregunta. Al cancelar la tarea o cerrar el explorador se cuenta como un intento fallido.
4. Haga clic en Enviar.

   CA Identity Manager pide que indique una contraseña nueva.

Gestión de usuarios

La gestión de usuarios incluye las operaciones siguientes:

- Acceso al entorno de CA Identity Manager de NeteAuto
- Modificación de un usuario
- Asignación de un rol de gestor de grupos
- Creación de un grupo
- Gestión de usuarios autorregistrados

Acceso al entorno de CA Identity Manager de NeteAuto

Se debe llevar a cabo el procedimiento siguiente para acceder el entorno de CA Identity Manager de NeteAuto.

Siga estos pasos:

1. Escriba la siguiente dirección URL en un explorador:

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   nombre de host

   Define el nombre de dominio completo, como en el ejemplo siguiente:

   http://miservidor.miempresa.com/iam/im/neteauto/imcss/index.jsp.

   Nota: Si no se ha configurado la máscara de Neteauto, se puede utilizar la siguiente dirección URL para acceder al entorno de Neteauto:

   http://*hostname*/iam/im/neteauto

2. En la pantalla de inicio de sesión, escriba las credenciales siguientes:

   Nombre del usuario

   SuperAdmin

   Contraseña

   test

Modificación de un usuario

Se debe llevar a cabo el procedimiento siguiente para modificar un usuario.

Siga estos pasos:

1. Inicie sesión en el entorno de NeteAuto como SuperAdmin utilizando la prueba de contraseña.
2. Seleccione Usuarios, Gestionar usuarios, Modificar usuario.

   Aparecerá la pantalla Seleccionar usuario.
3. Haga clic en Buscar.

   CA Identity Manager muestra una lista de usuarios en el entorno de NeteAuto.
4. Seleccione el administrador de NeteAuto, tal y como se muestra a continuación:
   - Para directorios de LDAP: administrador de NeteAuto
   - Para bases de datos relacionales: administrador de NeteAuto

   Haga clic en Seleccionar. CA Identity Manager muestra el perfil para el administrador de NeteAuto.

5. En el campo Cargo, escriba Gestor. Haga clic en Enviar.

   CA Identity Manager confirma el envío de la tarea.

6. Haga clic en Aceptar para volver a la lista principal.

Asignación del rol de gestor de grupos

Es necesario asignar un rol de gestor de grupos. Se debe llevar a cabo el procedimiento siguiente para asignar a gestores de grupos.

Siga estos pasos:

1. Como SuperAdmin (Superadministrador), seleccione la ficha Roles y tareas; a continuación, seleccione Roles de administrador, Modificar Roles de administrador.
2. Seleccione el rol Gestor de grupos y haga clic en Seleccionar.

   Se muestra el perfil para el rol de gestor de grupos.

3. Haga clic en la ficha Miembros y haga clic en Agregar en Políticas de miembros.

   Aparecerá la pantalla Política de miembros.

4. En Regla de miembros, haga clic en la flecha abajo en el campo Usuarios.

   En la lista desplegable, seleccionar donde <filtro-usuario>.

   Los cambios del campo Usuarios permiten introducir un filtro para la regla.

5. Introduzca una regla de pertenencia tal y como se muestra a continuación:
   a. En el primer campo, seleccionar Cargo en la lista desplegable.
   b. En el segundo campo, asegúrese de seleccionar el signo igual (=).
   c. En el tercer campo, escriba Gestor.
6. En la sección de Reglas del ámbito, defina las reglas para los usuarios, los grupos y las organizaciones (cuando sea compatible) tal y como se muestra a continuación:
   a. En el campo Usuarios, haga clic en la flecha abajo para ver una lista de opciones. Seleccione una de las siguientes opciones de la lista o todas:
   b. Repita el paso A en los campos Grupo y Organización (cuando sea compatible).
   c. Deje vacío el campo Tareas de acceso.
7. Haga clic en Aceptar.

   CA Identity Manager muestra la política de miembros creada.

8. Haga clic en Enviar.

   CA Identity Manager confirma el envío de la tarea.

9. Haga clic en Aceptar para volver a la lista principal.
10. Cierre CA Identity Manager.

Creación de grupos

Se debe realizar el procedimiento siguiente para crear un grupo.

Siga estos pasos:

1. Inicie sesión en CA Identity Manager como administrador de NeteAuto, tal y como se muestra a continuación:
   - Para directorios de LDAP, escriba el nombre de usuario de administrador de NeteAuto y la prueba de contraseña.
   - Para bases de datos relacionales, escriba el nombre de usuario de administrador de NeteAuto y la prueba de contraseña.

   Se muestra la lista de tareas que el administrador de NeteAuto puede realizar. Debido que el administrador de NeteAuto puede realizar solamente un número limitado de tareas, CA Identity Manager muestra las tareas en lugar de las categorías.
2. Haga clic en Crear grupo.
3. Verifique que Crear un nuevo objeto está seleccionado y haga clic en Aceptar.
4. Implemente uno de los pasos siguientes que se ajuste a sus necesidades:
   - Si el entorno de NeteAuto es compatible con organizaciones:
     a. En el campo de nombre de organización, haga clic en el símbolo de tres puntos (...) para seleccionar la organización donde CA Identity Manager crea el grupo.
     b. En la parte inferior de la pantalla Seleccionar organización, expanda NeteAuto.
     c. Seleccionar la organización de distribuidores.
   - Si el entorno de NeteAuto no es compatible con organizaciones, vaya al paso siguiente.
5. Escriba la información siguiente para el grupo:
   - Nombre de grupo: administradores de distribuidores
   - Descripción del grupo: administradores para franquicias de NeteAuto.
6. Haga clic en la ficha Pertenencia y Agregar un usuario.

   Aparecerá la pantalla Seleccionar usuario.
7. Haga clic en Buscar.
8. Seleccione el administrador de NeteAuto y haga clic en Seleccionar.
9. Haga clic en Enviar para crear el grupo.

Gestión de usuarios autorregistrados

Se debe realizar el procedimiento siguiente cuando se desean gestionar usuarios autorregistrados.

Siga estos pasos:

1. Inicie sesión enCA Identity Manager como un administrador de NeteAuto utilizando las credenciales siguientes:

   - Para directorios de LDAP:

     Nombre de usuario

     Administrador de NeteAuto

     Contraseña

     test

   - Para bases de datos relacionales:

     Nombre de usuario

     Administrador de NeteAuto

     Contraseña

     test

   La lista de tareas que el administrador de NeteAuto puede realizar aparece en la parte izquierda de la Consola de usuario. Debido que el administrador de NeteAuto puede realizar solamente un número limitado de tareas, CA Identity Manager muestra las tareas en lugar de las categorías.

2. Haga clic en Modificar grupo.
3. Haga clic en Buscar.

   CA Identity Manager muestra una lista de grupos.

4. Seleccione los administradores de distribuidor y haga clic en Seleccionar.
5. Haga clic en la ficha Pertenencia y haga clic Agregar un usuario.

   Aparecerá la pantalla Seleccionar usuario.

6. Haga clic en Buscar.
7. En la pantalla de búsqueda de Usuario, seleccione el usuario escrito en Registro como nuevo usuario (en la página 38). Haga clic en Seleccionar.

8. Haga clic en Enviar.

   CA Identity Manager confirma el envío de la tarea.

9. Haga clic en Aceptar para volver a la lista principal.

Para confirmar que el usuario es un miembro del grupo creado, utilice la tarea Ver grupo.

Cómo configurar funciones adicionales

Una vez que se ha instalado el ejemplo de NeteAuto y la funcionalidad de CA Identity Manager basada en práctica, utilice el entorno de NeteAuto para practicar y probar funciones de CA Identity Manager adicionales, incluidas notificaciones de correo electrónico y flujo de trabajo.

Nota: Para obtener más información sobre estas funciones, consulte la *Guía de administración*.

Restricción de nombre de inicio de sesión de SiteMinder para el nombre de usuario global

Los siguientes caracteres o cadenas de caracteres no pueden formar parte de un nombre de usuario global si el usuario debe iniciar sesión en el servidor de políticas de SiteMinder:

&
*
:
()

Solución

Evite utilizar estos caracteres en el nombre de usuario global.

Capítulo 3: Gestión de almacén de usuarios de LDAP

Esta sección contiene los siguientes temas:

Directorios de CA Identity Manager

En un *directorio de CA Identity Manager* se describen cómo objetos como usuarios, grupos y organizaciones se almacenan en el directorio de usuarios, además de cómo se representan en CA Identity Manager. Un directorio de CA Identity Manager se asocia con uno o varios entornos de CA Identity Manager.

Cómo crear un directorio de CA Identity Manager

Al crear un directorio de CA Identity Manager para un almacén de usuarios de LDAP se requiere realizar los siguientes pasos:

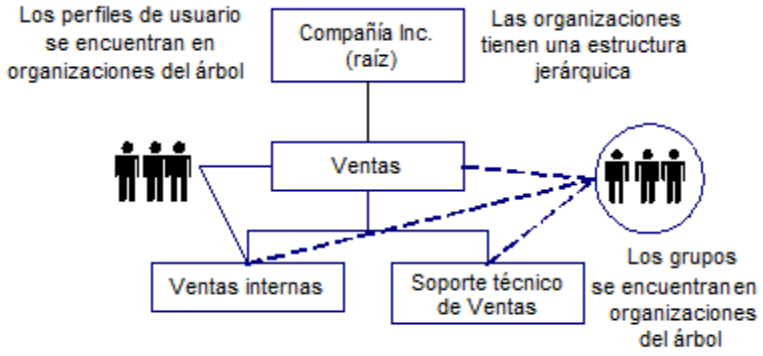
1. Determine la estructura de directorios.
2. Describa los objetos en el almacén de usuarios modificando un archivo de configuración del directorio (directory.xml) (en la página 53).
3. Importe el archivo de configuración del directorio y cree el directorio (en la página 158).

Nota: Al utilizar SiteMinder, verifique que se ha aplicado el esquema de almacén de políticas antes de crear un directorio de CA Identity Manager. Para obtener más información sobre los esquemas de almacén de políticas específicos y cómo aplicarlos, consulte la *Guía de instalación*.

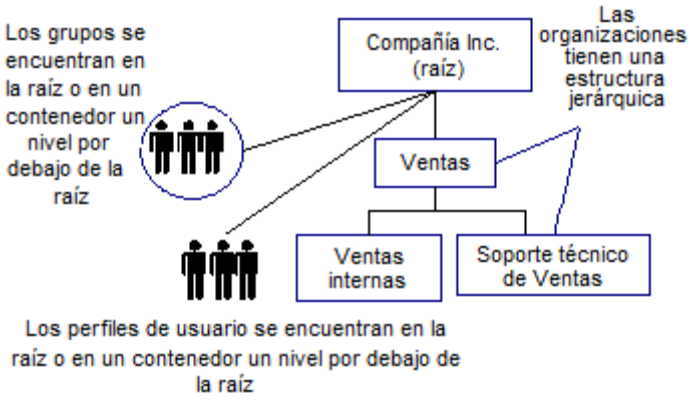
Estructura de directorios

CA Identity Manager es compatible con las siguientes estructuras de directorios:

- Jerárquica: contiene una organización principal (raíz) y suborganizaciones. Las suborganizaciones pueden tener también suborganizaciones, lo que crea una estructura de varios niveles, tal y como se muestra en la siguiente ilustración:

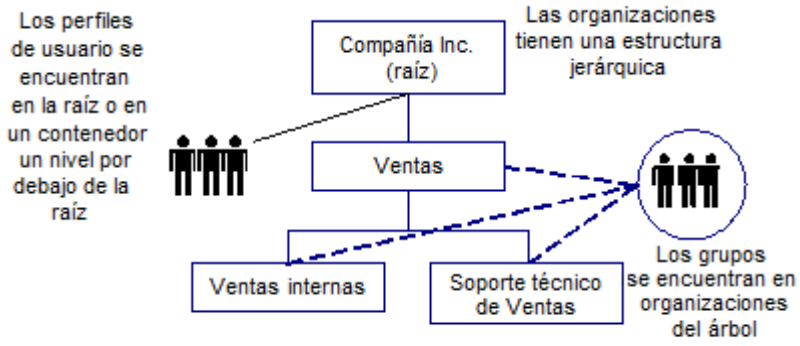


- Plana: se almacenan usuarios y grupos en la raíz de búsqueda o en un contenedor un nivel por debajo de la raíz de búsqueda. Las organizaciones tienen una estructura jerárquica, tal y como se muestra en la siguiente ilustración de una estructura de directorios plana:



  Para facilitar la gestión de usuarios y delegación en estructuras de directorios planas, los usuarios y los grupos pertenecen a organizaciones lógicas. La organización lógica se almacena como atributo de perfiles de usuarios y grupos.

- De usuarios plana: se almacenan organizaciones y grupos jerárquicamente, pero se almacenan usuarios en la raíz de búsqueda o en un contenedor un nivel por debajo de la raíz de búsqueda. Se muestra una ilustración de una estructura del directorio de usuarios plana en el diagrama siguiente:



  En estructuras del directorio de usuarios planas, los usuarios pertenecen a organizaciones lógicas. La organización lógica de un usuario se almacena como atributo en un perfil de usuario.

- Ninguna organización: el directorio no incluye organizaciones. Se almacenan usuarios y grupos en la raíz de búsqueda o en un contenedor un nivel por debajo de la raíz de búsqueda. Se muestra una estructura de directorios sin organizaciones en la siguiente ilustración:

Nota: Un directorio puede contener más de un tipo de estructura. Por ejemplo, los perfiles de usuario se pueden almacenar en una estructura plana en una parte del directorio y jerárquicamente en otra. Para que sea compatible con una estructura de directorios híbrida, cree varios entornos de CA Identity Manager.

Archivo de configuración del directorio

Para describir la estructura de un directorio de usuarios a CA Identity Manager, cree un archivo de configuración del directorio.

El archivo de configuración del directorio contiene una o varias de las secciones siguientes:

Información del directorio de CA Identity Manager

Contiene información sobre el directorio de CA Identity Manager.

Nota: No modifique información en esta sección. CA Identity Manager solicita que se proporcione esta información cuando se crea un directorio de CA Identity Manager en la Consola de gestión.

Validación del atributo

Define las reglas de validación que se aplican al directorio de CA Identity Manager.

Información del proveedor

Describe el almacén de usuarios que gestiona CA Identity Manager.

Información de búsqueda de directorios

Permite especificar cómo busca CA Identity Manager en el almacén de usuarios.

Objeto de usuario

Describe cómo se almacenan los usuarios en el almacén de usuarios y cómo se representan en CA Identity Manager.

Objeto de grupo

Describe cómo se almacenan los grupos en el almacén de usuarios y cómo se representan en CA Identity Manager.

Objeto de organización

Describe cómo se almacenan las organizaciones y cómo se representan en CA Identity Manager. El objeto de organización proporciona detalles solamente cuando el almacén de usuarios incluye organizaciones.

Objeto Self-Subscribing

Configura la compatibilidad con grupos a los que se pueden unir los usuarios de autoservicio.

Comportamiento de los grupos del directorio

Especifica si el directorio de CA Identity Manager es compatible con los grupos dinámicos y anidados.

Para crear un archivo de configuración del directorio, modifique una plantilla de configuración.

Cómo seleccionar una plantilla de configuración del directorio

CA Identity Manager proporciona plantillas de configuración del directorio que son compatibles con estructuras y tipos de directorio diferentes. Para crear un directorio de CA Identity Manager, modifique la plantilla que coincida lo máximo posible con la estructura de directorios.

Las plantillas descritas en la tabla siguiente se instalan con las herramientas administrativas:

admin_tools\directoryTemplates*directory_type*\

Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Los tipos de directorios y las plantillas de configuración correspondientes se muestran en la tabla siguiente:

Tipo de directorio	Plantilla
Directorio LDAP de Active Directory (ADSI) con una estructura jerárquica	ActiveDirectory\directory.xml
Directorio de Microsoft ADAM con una estructura jerárquica	ADAM\directory.xml
Directorio de servidor de directorios de IBM con una estructura jerárquica	IBMDirectoryServer\directory.xml
Directorio de usuarios de Novell eDirectory con una estructura jerárquica	eDirectory\directory.xml
Directorio de Internet de Oracle con una estructura jerárquica	OracleInternetDirectory\directory.xml
Directorio LDAP del sistema Sun Java (SunOne o iPlanet) con una estructura jerárquica	IPlanetHierarchical\directory.xml
Directorio LDAP del sistema Sun Java (SunOne o iPlanet) con una estructura plana	IPlanetFlat\directory.xml
Directorio LDAP del sistema Sun Java (SunOne o iPlanet) que no incluye organizaciones.	IPlanetNoOrganizations\directory.xml
Almacén de usuarios de CA Directory con una estructura jerárquica	eTrustDirectory\directory.xml

Tipo de directorio	Plantilla
Directorio de aprovisionamiento Esta plantilla configura el directorio de aprovisionamiento para un entorno de CA Identity Manager. **Nota:** Se puede utilizar esta plantilla de configuración como instalada. No es necesario modificar esta plantilla.	ProvisioningServer\directory.xml
Directorio personalizado	Utilice la plantilla que se parezca lo máximo posible al directorio.

Se debe copiar la plantilla de configuración en un directorio nuevo o guardarlo con un nombre diferente para evitar que se sobrescriba.

Cómo describir un directorio de usuarios en CA Identity Manager

Para gestionar un directorio, CA Identity Manager debe entender la estructura y el contenido de un directorio. Para describirle el directorio en CA Identity Manager, modifique el archivo de configuración del directorio (directory.xml) en el directorio de la plantilla adecuado.

El archivo de configuración del directorio tiene las convenciones importantes:

- ##: indica valores requeridos.

  Para proporcionar toda la información obligatoria, busque todos los signos dobles de almohadilla (##) y sustitúyalos por los valores adecuados. Por ejemplo, ##DISABLED_STATE indica que se debe proporcionar un atributo para almacenar el estado de la cuenta de un usuario.

- @: indica valores que rellena CA Identity Manager. No se deben modificar estos valores en el archivo de configuración del directorio. CA Identity Manager pide que se proporcionen los valores cuando se importa el archivo de configuración del directorio.

Antes de modificar el archivo de configuración del directorio, se necesita la información siguiente:

- Las clases de objeto de LDAP para el usuario, el grupo y los objetos de organización.
- La lista de atributos en perfiles de usuarios, grupos y organizaciones.

Cómo modificar el archivo de configuración del directorio

Realice los siguientes pasos para modificar el archivo de configuración del directorio.

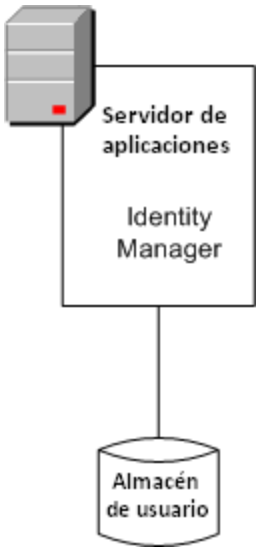
Nota: Se especifican los pasos que son obligatorios.

1. Limite el tamaño de los resultados de la búsqueda (en la página 59).
2. Modifique los objetos gestionados de usuarios, organizaciones o grupos predeterminados.
3. Cambie las descripciones del atributo predeterminadas.
4. Modifique los atributos conocidos (en la página 79). (obligatorio)

   Los atributos conocidos identifican atributos especiales, como el atributo de contraseña, en CA Identity Manager.
5. Configure CA Identity Manager para la estructura de directorios (en la página 86) (obligatorio).
6. Permita que los usuarios se suscriban a grupos (en la página 87).

Conexión al directorio de usuarios

CA Identity Manager se conecta a un directorio de usuarios para almacenar información de usuarios, grupos y organizaciones tal y como se muestra en la siguiente ilustración:



No se requiere nuevos directorios o bases de datos. Sin embargo, el directorio o la base de datos existentes deben estar en un sistema que tenga un nombre de dominio completo (FQDN).

Para consultar una lista de directorios y tipos de bases de datos compatibles, consulte el cuadro de compatibilidad de CA Identity Manager en el sitio de Soporte de CA.

Configure una conexión al almacén de usuarios al crear un directorio de CA Identity Manager en la Consola de gestión.

Si se exporta la configuración del directorio después de haber creado un directorio de CA Identity Manager, la información de conexión con el directorio de usuarios se muestra en el elemento de proveedor del archivo de configuración del directorio.

Elemento de proveedor

La información de la configuración se almacena en el elemento de proveedor y sus subelementos en el archivo directory.xml.

Nota: Si se está creando un directorio de CA Identity Manager, no es necesario proporcionar información de conexión del directorio en el archivo directory.xml. La información de conexión se proporciona en el asistente del directorio de CA Identity Manager en la Consola de gestión. Modifique el elemento de proveedor solamente para realizar actualizaciones.

El elemento de proveedor incluye los subelementos siguientes:

LDAP

Describe el directorio de usuarios al que se va a conectar.

Credenciales

Proporciona el nombre de usuario y la contraseña para acceder al almacén de usuarios de LDAP.

Conexión

Proporciona el nombre de host para el equipo donde se encuentra el almacén de usuarios.

Dominio de aprovisionamiento

Define el dominio de Aprovisionamiento que CA Identity Manager gestiona (solamente para usuarios de aprovisionamiento).

Un elemento de proveedor completado se parece al código siguiente:

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

El elemento de proveedor incluye los parámetros siguientes:

type

Especifica el tipo de base de datos. Para todos los almacenes de usuarios de LDAP, especifique LDAP (valor predeterminado).

userdirectory

Especifica el nombre de la conexión del directorio de usuarios.

Nota: No se debe especificar un nombre para la conexión con el directorio de usuarios en el archivo directory.xml. CA Identity Manager pide que se proporcione el nombre cuando se crea el directorio de CA Identity Manager en la Consola de gestión.

Nota: Los parámetros son opcionales.

Subelemento de LDAP

El subelemento de LDAP incluye los parámetros siguientes:

searchroot

Especifica la ubicación en un directorio LDAP que sirve del punto de partida para el directorio, normalmente, una organización (o) o una unidad organizativa (ou).

secure

Se obliga a utilizar una conexión de Secure Sockets Layer (SSL) en el directorio de usuarios de LDAP, tal y como se muestra a continuación:

- True: CA Identity Manager utiliza una conexión segura.
- False: CA Identity Manager se conecta al directorio de usuarios sin SSL (valor predeterminado).

Nota: Los parámetros son opcionales.

Subelemento de credenciales

Para conectarse a un directorio LDAP, CA Identity Manager debe proporcionar credenciales válidas. Las credenciales se definen en el subelemento Credenciales, que se parece al código siguiente:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Si no se especifica una contraseña en el subelemento Credentials (Credenciales), se solicitará la contraseña cuando se crea el directorio de CA Identity Manager en la Consola de gestión.

Nota: Se recomienda que se especifique la contraseña en la Consola de gestión.

Si se especifica la contraseña en la Consola de gestión, CA Identity Manager cifrará la contraseña. En caso contrario, si no se desea que la contraseña aparezca en texto no cifrado, la contraseña se cifra mediante la herramienta de contraseñas que se instala con CA Identity Manager.

Nota: Se puede especificar solamente un conjunto de credenciales. Si se definen varios directorios, tal y como se describe en el subelemento Connection (Conexión), las credenciales que se especifiquen deben aplicarse a todos los directorios.

El subelemento Credentials (Credenciales) incluye los parámetros siguientes:

usuario

Especifica el ID de inicio de sesión para una cuenta que puede acceder al directorio.

Para usuarios de aprovisionamiento, la cuenta de usuario que se especifique debe tener el perfil de administrador de dominios o un conjunto equivalente de privilegios en el servidor de aprovisionamiento.

Nota: No especifique un valor para el parámetro de usuario en el archivo directory.xml. CA Identity Manager pide que se proporcione el ID de inicio de sesión al crear el directorio de CA Identity Manager en la Consola de gestión.

cleartext

Determina si la contraseña se muestra en texto sencillo en el archivo directory.xml, tal y como se muestra a continuación:

- True: la contraseña se muestra en texto no cifrado.
- False: la contraseña se cifra (valor predeterminado).

Nota: Los parámetros son opcionales.

Subelemento Connection (Conexión)

El subelemento Connection (Conexión) describe la ubicación del almacén de usuarios que CA Identity Manager gestiona. Este subelemento incluye los parámetros siguientes:

host

Especifica el nombre de host o la dirección IP del servidor en el que se ha implementado el servidor de usuarios.

Nota: Si el sistema de conexión tiene una dirección IPv6, agregue la dirección IP entre paréntesis ([ ]) como se muestra a continuación:

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"

failover="[2::9255:214:22ff:fe72:525a]:20389"/>

puerto

Especifica el número de puerto para el directorio de usuarios.

failover

Especifica el nombre de host y dirección IP del sistema donde se encuentran almacenes de usuarios redundantes, en caso de que el sistema principal no esté disponible. Cuando el sistema principal vuelva a estar disponible, el sistema de conmutación por error se continúa utilizando. Para volver a utilizar el sistema principal, reinicie el sistema secundario. Si se muestran varios servidores, CA Identity Manager intentará conectarse a los sistemas en el orden que se indica.

Especifique el nombre de host y la dirección IP en el atributo de conmutación por error en una lista *separada por espacios,* tal y como se muestra a continuación:

failover="IPaddress:port IPaddress:port"

Por ejemplo:

<Connection host="123.456.789.001" port="20389"

failover="123.456.789.002:20389 123.456.789.003:20389"/>

Nota: El puerto 20389 es el puerto predeterminado para el servidor de aprovisionamiento.

Nota: Los parámetros son opcionales.

Subelemento Provisioning (Aprovisionamiento)

Si el entorno de CA Identity Manager incluye aprovisionamiento, defina el dominio de aprovisionamiento tal y como se muestra a continuación:

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

El subelemento Provisioning (Aprovisionamiento) incluye el parámetro siguiente:

domain

Contiene el nombre del dominio de aprovisionamiento que CA Identity Manager gestiona.

Al crear el directorio de CA Identity Manager en la Consola de gestión, se solicitará el nombre de dominio. Por tanto, verifique que especifica un valor para el parámetro de dominio en el archivo de configuración del directorio (directory.xml).

Parámetros de búsqueda de directorios

Se pueden establecer los parámetros de búsqueda siguientes en el elemento DirectorySearch:

maxrows

Especifica el número máximo de objetos que CA Identity Manager puede devolver al buscar un directorio de usuarios. Cuando el número de objetos supera el límite, se muestra un error.

Al establecer un valor para el parámetro maxrows, se puede anular la configuración en el directorio LDAP que limita los resultados de la búsqueda. Al aplicar una configuración que entre en conflicto, el servidor de LDAP utiliza la configuración de menor nivel.

Nota: El parámetro maxrows no limita el número de objetos que se muestran en una pantalla de tarea de CA Identity Manager. Para configurar la configuración de visualización, modifique la definición de la pantalla de lista en la Consola de usuario de CA Identity Manager. Para obtener instrucciones, consulte la *Guía de diseño de la Consola de usuario*.

maxpagesize

Especifica el número de objetos que se pueden devolver en una búsqueda única. Si el número de objetos supera el tamaño de la página, CA Identity Manager realizará varias búsquedas.

Tenga en cuenta los puntos siguientes al especificar maxpagesize:

- Para utilizar la opción de maxpagesize, el almacén de usuarios que gestiona CA Identity Manager debe ser compatible con la paginación. Algunos tipos de almacén de usuarios requieren configuración adicional para ser compatibles con la paginación. Para obtener más información, consulte Cómo mejorar el rendimiento de las búsquedas grandes (en la página 97).
- Si el almacén de usuarios no es compatible con la paginación y también se especifica un valor para maxrows, CA Identity Manager utilizará solamente el valor de maxrows para controlar el tamaño de la búsqueda.

tiempo de espera

Determina el número máximo de segundos que CA Identity Manager busca un directorio antes de finalizar la búsqueda.

Nota: El elemento DirectorySearch es opcional. Sin embargo, el directorio es compatible con la paginación (en la página 97). Se recomienda especificar el elemento de DirectorySearch.

Más información:

Cómo mejorar el rendimiento de las búsquedas en directorios (en la página 96)
Cómo mejorar el rendimiento de las búsquedas grandes (en la página 97)

Descripciones de objetos gestionados de usuario, grupo y organización

En CA Identity Manager, gestione los tipos siguientes de objetos que se corresponden con entradas de un directorio de usuarios:

Usuarios

Representa usuarios en una empresa. Un usuario pertenece a una única organización.

Grupos

Representa asociaciones de usuarios que tienen algo en común.

Organizaciones

Representa unidades de negocio. Las organizaciones contienen detalles como usuarios, grupos y otras organizaciones.

Una descripción de objeto contiene la siguiente información:

- La información sobre el objeto (en la página 117), como la clase de objeto de LDAP y el contenedor en el que se almacenan objetos.
- Los atributos que almacenan información acerca de una entrada (en la página 122). Por ejemplo, el atributo de buscapersonas almacena un número de buscapersonas.

Nota: Un entorno de CA Identity Manager es compatible solamente con un tipo de objeto de organización, usuario y grupo. Por ejemplo, todos los objetos de usuario tienen la misma clase de objeto.

Descripciones de objetos gestionados

Un objeto gestionado se describe especificando la información del objeto en las secciones de objeto de usuario, objeto de grupo y objeto de organización del archivo de configuración del directorio.

Nota: Al utilizar la plantilla de configuración (archivo directory.xml), la sección de objeto de organización no está disponible para esos directorios de usuarios que no son compatibles con organizaciones.

Cada una de estas secciones contiene elementos ImsManagedObject, como el ejemplo siguiente:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

Si se desea, el elemento ImsManagedObject puede incluir un elemento Container, como el ejemplo siguiente:

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people" />
```

Especificación de la información del objeto

La información del objeto se especifica proporcionando valores para diversos parámetros.

Siga estos pasos:

1. Busque el elemento ImsManagedObject en la sección de objeto de usuario, objeto de grupo u objeto de organización.
2. Proporcione valores para los siguientes parámetros:

   name

   Especifica un nombre único para el objeto gestionado.

   Nota: Este parámetro es obligatorio.

   descripción

   Contiene una descripción del objeto gestionado.

   objectclass

   Especifica el nombre de la clase de objeto de LDAP para el tipo de objeto (usuario, grupo u organización). La clase de objeto determina la lista de atributos disponibles para un objeto.

   Si los atributos de varias clases de objeto se aplican a un tipo de objeto, enumere las clases de objeto en una lista delimitada por comas. Por ejemplo, si un objeto contiene atributos de la persona, las clases de objeto organizationalperson e inetorgperson, agregue estas clases de objeto tal y como se muestra a continuación:

   objectclass="top,person,organizationalperson,inetorgperson"

   Cada directorio LDAP incluye un conjunto de clases de objeto predeterminadas. Consulte la documentación del servidor de directorio para obtener información sobre las clases de objeto predeterminadas.

   Nota: Este parámetro es obligatorio.

objecttype

Especifica el tipo del objeto gestionado. Los valores válidos son los siguientes:

- Usuario
- Organización
- Grupo

Nota: Este parámetro es obligatorio.

maxrows

Especifica el número máximo de objetos que CA Identity Manager puede devolver al buscar un directorio de usuarios. Cuando el número de objetos supera el límite, se muestra un error.

Al establecer un valor para el parámetro maxrows, se puede anular la configuración en el directorio LDAP que limita los resultados de la búsqueda. Al aplicar una configuración que entre en conflicto, el servidor de LDAP utiliza la configuración de menor nivel.

Nota: El parámetro maxrows no limita el número de objetos que se muestran en una pantalla de tarea de CA Identity Manager. Para configurar la configuración de visualización, modifique la definición de la pantalla de lista en la Consola de usuario de CA Identity Manager. Para obtener instrucciones, consulte la *Guía de diseño de la Consola de usuario*.

maxpagesize

Especifica el número de objetos que se pueden devolver en una búsqueda única. Si el número de objetos supera el tamaño de la página, CA Identity Manager realizará varias búsquedas.

Se deben tener en cuenta los siguientes aspectos al especificar el tamaño de la página de búsqueda:

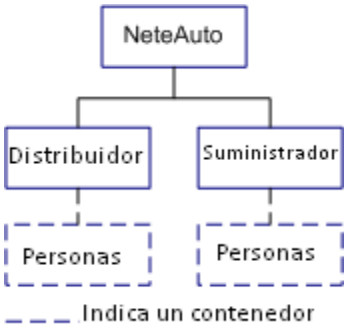
- Para utilizar la opción Search Page Size (Tamaño de la página de búsqueda), el almacén de usuarios que gestiona CA Identity Manager debe ser compatible con la paginación. Algunos tipos de almacén de usuarios requieren configuración adicional para ser compatibles con la paginación. Para obtener más información, consulte la sección sobre cómo mejorar el rendimiento de las búsqueda (en la página 97)s.
- Si el almacén de usuarios no es compatible con la paginación y también se especifica un valor para maxrows, CA Identity Manager utilizará solamente el valor de maxrows para controlar el tamaño de la búsqueda.

3. Si se desea, proporcione la información del contenedor.

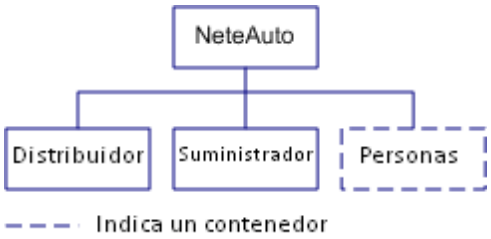
Contenedores

Para simplificar la administración, se pueden agrupar objetos de grupo de un tipo específico en un contenedor. Cuando se especifica un contenedor en el archivo de configuración del directorio, CA Identity Manager gestiona solamente las entradas del contenedor. Por ejemplo, si se especifica un contenedor de usuario denominado "Persona", CA Identity Manager gestiona usuarios en el contenedor Persona, tal y como se muestra en las siguientes imágenes:

- Directorio jerárquico



- Directorio plano



En estos ejemplos, todos los usuarios se encuentran en los contenedores de Persona.

Cuando se especifica un contenedor, se deben tener en cuenta los siguientes puntos:

- Si no existe ningún contenedor en una organización, CA Identity Manager creará el contenedor en cuanto se agregue la primera entrada. Para un directorio jerárquico, CA Identity Manager creará el contenedor en la organización donde se agregue la entrada. Para directorios planos y directorios que no son compatibles con organizaciones, CA Identity Manager creará el contenedor en la raíz de búsqueda, que especifica cuando se crea el directorio de CA Identity Manager.
- CA Identity Manager ignora las entradas que no están en el contenedor especificado. Por ejemplo, cuando se especifica el contenedor Persona, no se pueden gestionar usuarios que existen fuera del contenedor Persona.

  Nota: Para gestionar usuarios que no están en el contenedor especificado, se puede crear otro entorno de CA Identity Manager.

Contenedores y atributos conocidos

Los atributos conocidos son aquellos que tienen un significado especial en CA Identity Manager. Cuando CA Identity Manager gestiona un almacén de usuarios con contenedores, los atributos conocidos siguientes identifican información sobre el contenedor:

%ORG_MEMBERSHIP%

Identifica el atributo que almacena el nombre completo (nombre destacado) del contenedor.

Por ejemplo, el nombre completo se parece a esto:

ou=Persona, ou=Empleado, ou=NeteAuto, dc=seguridad y dc=com

%ORG_MEMBERSHIP_NAME%

Identifica el atributo que almacena el nombre sencillo del atributo.

Por ejemplo, el nombre sencillo del contenedor en el ejemplo anterior es Persona.

Estos atributos conocidos se muestran en las descripciones del atributo en las secciones de objeto de usuario y objeto de grupo del archivo directory.xml, tal y como se muestra a continuación:

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

Para estructuras del almacén de usuarios jerárquicas, se asignan los parámetros physicalname y los parámetros conocidos al atributo conocido tal y como se muestra a continuación:

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

En el ejemplo se indica que CA Identity Manager obtiene automáticamente el nombre destacado del contenedor y el nombre sencillo de otra información del archivo directory.xml.

Para estructuras del almacén de usuarios planas, proporcione los nombres de atributo físico.

Nota: Consulte la sección Cómo describir una estructura del directorio de usuarios plana (en la página 87) para obtener instrucciones.

Especificación de un contenedor de grupo o usuario

Se debe llevar a cabo el procedimiento siguiente para especificar un contenedor de usuario o grupo.

Siga estos pasos:

1. Busque el elemento Container (Contenedor) en la sección de objeto de usuario, objeto de grupo u objeto de organización.
2. Proporcione valores para los siguientes parámetros:

   objectclass

   Determina la clase de objeto de LDAP del contenedor donde se crean objetos de un tipo específico. Por ejemplo, el valor predeterminado para el contenedor de usuario es "top,organizationalUnit", lo que indica que se crean usuarios en unidades organizativas de LDAP (ou).

   Cuando se gestionan grupos dinámicos o anidados, asegúrese de especificar un objectclass que sea compatible con estos tipos de grupo (en la página 89).

   Nota: Este parámetro es obligatorio.

   attribute

   Especifica el atributo que se almacena el nombre del contenedor, por ejemplo, ou.

   El atributo se equipara con el valor para formar el nombre destacado relativo del contenedor, como en el ejemplo siguiente:

   ou=Persona

   Nota: Este parámetro es obligatorio.

   value

   Especifica el nombre del contenedor.

   Nota: Este parámetro es obligatorio.

Nota: No se pueden especificar contenedores para organizaciones.

Descripciones del atributo

Un atributo almacena información sobre una entrada, como un número de teléfono o una dirección. Un atributo de entrada determina su perfil.

En el archivo de configuración del directorio, los atributos están descritos en los elementos ImsManagedObjectAttr. En las secciones de objeto de usuario, objeto de grupo y objeto de organización del archivo de configuración del directorio, se pueden realizar las siguientes acciones:

- Modifique las descripciones del atributo predeterminadas para describir los atributos en el almacén de usuarios.
- Cree nuevas descripciones de atributos copiando una descripción existente y modificando los valores según sea necesario.

Para cada atributo de los perfiles de usuario, grupo y organización, solamente hay un elemento ImsManagedObjectAttr. Por ejemplo, un elemento ImsManagedObjectAttr se describe como ID de usuario.

Un elemento ImsManagedObjectAttr tiene el aspecto del siguiente código:

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User
ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%"
maxlength="0" />
```

ImsManagedObjectAttr tiene los parámetros siguientes:

physicalname

Este parámetro debe contener uno de los siguientes elementos:

- El nombre del atributo de LDAP donde se almacena el valor de perfil. Por ejemplo, se almacena el ID de usuario en el atributo uid del directorio de usuarios.

  Nota: Para mejorar el rendimiento, indexe los atributos de LDAP que se utilizan en consultas de búsqueda en la Consola de usuario.

- Un atributo conocido (en la página 79). Cuando se proporciona un atributo conocido, CA Identity Manager calcula el valor automáticamente. Por ejemplo, al especificar un atributo conocido %ORG_MEMBERSHIP%, CA Identity Manager determina la organización a la que pertenece la entrada, según el nombre destacado de una entrada.

descripción

Contiene la descripción del atributo.

displayname

Especifica un nombre único para el atributo.

En la Consola de usuario, el nombre para mostrar aparece en la lista de atributos que están disponibles para agregar a una pantalla de tarea. Este parámetro es obligatorio.

Nota: No se debe modificar el displayname de un atributo en el archivo de configuración del directorio (directory.xml). Para cambiar el nombre de un atributo en una pantalla de tarea, se puede especificar una etiqueta para el atributo en la definición de pantalla de tarea. Para obtener más información, consulte la *Guía de administración*.

valuetype

Especifica tipo de datos del atributo. Los valores válidos son los siguientes:

STRING

El valor puede ser cualquier cadena.

Éste es el valor predeterminado.

Integer

El valor debe ser un número entero.

Nota: Entero no admite números decimales.

Number

El valor debe ser un número entero. La opción de número admite números decimales.

Fecha

El valor debe analizar una fecha válida mediante el patrón:

DD/MM/AAAA

ISODate

El valor debe analizar una fecha válida mediante el patrón aaaa-MM-dd.

UnicenterDate

El valor debe analizar una fecha válida mediante el patrón YYYYYYYDDD, donde:

YYYYYYY es una representación del año de siete números que empieza con tres ceros. Por ejemplo: 0002008

DDD es una representación del día de tres números que empieza con ceros, según sea necesario. Los valores válidos oscilan de 001 a 366.

Estructurado

Este tipo de atributo consta de datos estructurados que permiten que un valor de atributo único almacene varios valores relacionados. Por ejemplo, un atributo estructurado contiene valores como Nombre, Apellidos y Dirección de correo electrónico.

Algunos tipos de punto final utilizan estos atributos, pero se gestionan a través de CA Identity Manager.

Nota: CA Identity Manager puede mostrar atributos estructurados en una tabla en la Consola de usuario. Cuando los usuarios editan valores en la tabla, los valores se almacenan en el almacén de usuarios, por lo que se vuelve a propagar al punto final. Para obtener más información sobre las tareas con varios valores, consulte la *Guía de administración*.

required

Indica si el atributo es obligatorio, tal y como se muestra a continuación:

- True: el atributo es obligatorio.
- False: el atributo es opcional (valor predeterminado).

Nota: Si un atributo es obligatorio para un servidor de directorio LDAP, establezca el parámetro obligatorio a true.

multivalued

Indica si el atributo puede tener varios valores. Por ejemplo, el atributo de pertenencia a grupo contiene varios valores para almacenar el nombre destacado de usuario de cada miembro del grupo. Los valores válidos son los siguientes:

- True: el atributo puede tener varios valores.
- False: un atributo puede tener solamente un valor único (valor predeterminado).

Importante: Los atributos de pertenencia a grupo y roles de administrador en la definición del objeto de usuario deben tener varios valores.

wellknown

Define el nombre del atributo conocido.

Los atributos conocidos tienen un significado específico en CA Identity Manager. (en la página 79) Se identifican en la sintaxis:

%ATTRIBUTENAME%

maxlength

Define la longitud máxima que puede tener el valor de un atributo. Establezca el parámetro maxlength en 0 para especificar una longitud ilimitada.

Nota: Este parámetro es obligatorio.

permission

Indica si el valor de un atributo se puede modificar en una pantalla de tarea. Los valores válidos son los siguientes:

READONLY

El valor se muestra pero no se puede modificar.

WRITEONCE

No se puede modificar el valor una vez que el objeto se haya creado. Por ejemplo, no se puede cambiar un ID de usuario después de que el usuario se haya creado.

READWRITE

El valor se puede modificar (valor predeterminado).

oculto

Indica si un atributo se muestra en formularios de tarea de CA Identity Manager. Los valores válidos son los siguientes:

- True: el atributo no se muestra a usuarios.
- False: el atributo se muestra a usuarios (valor predeterminado).

Los atributos lógicos utilizan atributos ocultos.

Nota: Para obtener más información, consulte la *Guía de programación para Java*.

system

Especifica solamente atributos utilizados de CA Identity Manager. Los usuarios de la Consola de usuario no pueden modificar los atributos. Los valores válidos son los siguientes:

- True: los usuarios no pueden modificar el atributo. El atributo se oculta en la interfaz de usuario de CA Identity Manager.
- False: los usuarios no pueden modificar este atributo. El atributo está disponible para agregarse a pantallas de tarea en la interfaz de usuario de CA Identity Manager. (predeterminado)

validationruleset

Asocia un conjunto de reglas de validación con el atributo.

Es necesario verificar que el conjunto de reglas de validación que se especifica está definido en un elemento ValidationRuleSet en el archivo de configuración del directorio.

objectclass

Indica la clase auxiliar de LDAP para un atributo de usuario, grupo u organización cuando el atributo no forma parte del objectclass principal especificado en el elemento ImsManagedObject.

Por ejemplo, la clase de objeto primario para usuarios es top, person y organizationalperson, que define los atributos de usuario siguientes:

- nombre común (cn)
- apellidos (sn)
- ID de usuario (uid)
- contraseña (userPassword)

Para incluir el atributo employeeID, que se define en la clase de auxiliar de empleado, debe agregar la descripción del atributo siguiente:

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true" multivalued="false"
maxlength="0" objectclass="Employee"/>
```

Especificación de descripciones del atributo

Al describir atributos, se deben realizar los siguientes pasos:

1. Lea las secciones pertinentes entre los temas siguientes:
   - Consideraciones sobre CA Directory (en la página 77)
   - Consideraciones sobre Microsoft Active Directory (en la página 78)
   - Consideraciones sobre el servidor de directorios de IBM (en la página 78)
   - Consideraciones de directorio de Internet de Oracle (en la página 79)
2. En las secciones de objeto de usuario, objeto de grupo y objeto de organización del archivo de configuración del directorio, se pueden realizar las siguientes acciones:
   - Modifique las descripciones predeterminadas de los atributos para describir los atributos de directorio.
   - Cree nuevas descripciones de atributos copiando una descripción existente y modificando los valores según sea necesario.

   Nota: Por ejemplo, una nueva descripción del atributo se crea y se especifica un atributo físico. Se debe asegurar de que el atributo físico se encuentre en la clase de objeto (o clases) que se haya especificado para el tipo de objeto.
3. (Opcional) Cambie la configuración del atributo (en la página 74) para que se evite mostrar información confidencial, como contraseñas o salarios, en la Consola de usuario.
4. (Opcional) Configure un orden de clasificación predeterminado.
5. Si se está gestionando un directorio con una estructura de usuarios plana o un directorio sin organizaciones, vaya a Descripción de la estructura del directorio de usuarios (en la página 86).

Gestión de atributos confidenciales

CA Identity Manager proporciona los siguientes métodos para gestionar atributos confidenciales:

- Clasificaciones de datos para atributos

  Las clasificaciones de los datos permiten especificar las propiedades de visualización y cifrado para los atributos en el archivo de configuración del directorio (directory.xml).

  Se pueden definir clasificaciones de datos que gestionan atributos confidenciales de la siguiente forma:

  - En pantallas de tarea de CA Identity Manager, se muestra el valor de un atributo como una serie de asteriscos.

    Por ejemplo, se pueden mostrar contraseñas como asteriscos en lugar de mostrarlas en texto no cifrado.

  - En las pantallas Ver tareas enviadas, oculte el valor de atributo.

    Esta opción permite ocultar atributos de administradores. Por ejemplo, ocultar detalles de salario como el salario de los administradores que ven el estado de las tareas en CA Identity Manager pero no deben consultar detalles de salario.

  - Ignore determinados atributos al crear una copia de un objeto existente.
  - Cifre un atributo.

- Estilos del campo en pantallas de perfil de tarea

  Si no se desea modificar un atributo en el archivo directory.xml, establezca la propiedad de visualización para el atributo en las definiciones de la pantalla donde se muestra el atributo confidencial.

  El estilo del campo permite mostrar atributos, como las contraseñas, como una serie de asteriscos en vez de texto no cifrado.

  Nota: Para obtener más información sobre el estilo del campo de atributos confidenciales, busque "estilos de campo" en la ayuda de la Consola de usuario.

Atributos de clasificación de datos

El elemento de clasificación de datos proporciona una forma de asociar propiedades adicionales con una descripción del atributo. Los valores de este elemento determinan cómo CA Identity Manager gestiona el atributo. Este elemento es compatible con los siguientes parámetros:

- sensitive

  Hace que CA Identity Manager muestre el atributo como una serie de asteriscos (*) en las pantallas Ver tareas enviadas. Este parámetro impide que los atributos antiguos y nuevos del atributo se muestren en texto no cifrado en las pantallas Ver tareas enviadas.

  Además, si se crea una copia de un usuario existente en la Consola de usuario, este parámetro impide que el atributo se copie en el usuario nuevo.

- vst_hide

  Oculta el atributo en la pantalla Detalles del evento para la ficha Ver tareas enviadas. A diferencia de los atributos confidenciales, que se muestran como asteriscos, los atributos vst_hidden no se mostrarán.

  Se puede utilizar este parámetro para impedir que se muestren cambios en un atributo, como el salario, que en la pantalla Ver tareas enviadas.

- ignore_on_copy

  Hace que CA Identity Manager ignore un atributo cuando un administrador crea una copia de un objeto en la Consola de usuario. Por ejemplo, suponga que se ha especificado ignore_on_copy para el atributo de contraseña en un objeto de usuario. Al copiar un perfil de usuario, CA Identity Manager no aplica la contraseña del usuario actual al nuevo perfil de usuario.

- AttributeLevelEncrypt

  Cifra valores de atributo cuando se almacenan en el almacén de usuarios. Si se ha activado FIPS 140-2 para CA Identity Manager, este utilizará el cifrado RC2 o FIPS 140-2.

  Para obtener más información sobre la compatibilidad de FIPS 140-2 en CA Identity Manager, consulte la *Guía de configuración*.

  Los atributos se muestran en texto no cifrado durante el tiempo de ejecución.

  Nota: Para impedir que los atributos se muestren en texto no cifrado en las pantallas, se puede agregar también un elemento de clasificación de datos confidenciales en atributos cifrados. Para obtener más información, consulte Cómo agregar cifrado de nivel de atributo (en la página 75).

- PreviouslyEncrypted

  Hace que CA Identity Manager detecte y descifre algunos valores cifrados en el atributo cuando accede al objeto en el almacén de usuarios.

  Utilice esta clasificación de datos para descifrar algunos valores previamente cifrados.

  El valor de texto no cifrado se guarda en el almacén cuando se guarda el objeto.

Configuración de atributos de clasificación de datos

Siga estos pasos:

1. Busque el atributo en el archivo de configuración del directorio.
2. Después de la descripción del atributo, agregue el siguiente atributo:

   <DataClassification name="*parameter*">

   parameter

   Representa uno de los parámetros siguientes:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Por ejemplo, una descripción del atributo que incluye el atributo de clasificación de los datos de vst_hide se parece al siguiente código:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Cifrado de nivel de atributo

Se puede cifrar un atributo en el almacén de usuarios especificando una clasificación de los datos de AttributeLevelEncypt para ese atributo en el archivo de configuración del directorio (directory.xml). Cuando el cifrado de nivel de atributo se activa, CA Identity Manager cifra el valor de ese atributo antes de almacenarlo en el almacén de usuarios. El atributo se muestra como texto no cifrado en la Consola de usuario.

Nota: Para impedir que los atributos se muestren en texto no cifrado en las pantallas, se puede agregar también un elemento de clasificación de datos confidenciales en atributos cifrados. Para obtener más información, consulte Cómo agregar cifrado de nivel de atributo (en la página 75).

Si se ha activado el soporte de FIPS 140-2, el atributo se cifra mediante el cifrado RC2 o FIPS 140-2.

Antes de que se implemente el cifrado de nivel de atributo, tenga en cuenta los siguientes puntos:

- CA Identity Manager no puede buscar los atributos cifrados en una búsqueda.

  Suponga que un atributo cifrado se agrega a una política de identidad, miembros o propietarios. CA Identity Manager no puede resolver la política correctamente debido a que no se puede buscar el atributo.

  Se debe considerar la posibilidad de establecer el atributo en searchable="false" en el archivo directory.xml. Por ejemplo:

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Si CA Identity Manager utiliza un almacén de usuarios compartido y un directorio de aprovisionamiento, no cifre atributos del servidor de aprovisionamiento.
- No active AttributeLevelEncrypt para contraseñas de usuario en entornos que cumplen con los siguientes criterios:
  - Que incluye integración de CA SiteMinder
  - Que se almacenen usuarios en una base de datos relacional

  Cuando CA Identity Manager se integra con CA SiteMinder, las contraseñas cifradas producen problemas cuando los usuarios nuevos intentan iniciar sesión e introducir contraseñas en el texto no cifrado.
- Si se activa el cifrado de nivel de atributo para un almacén de usuarios que utilizan aplicaciones distintas de CA Identity Manager, el resto de las aplicaciones no pueden utilizar el atributo cifrado.

Cómo agregar cifrado de nivel de atributo

Suponga que ha agregado un cifrado de nivel de atributo a un directorio de CA Identity Manager. CA Identity Manager cifra automáticamente valores de atributo de texto no cifrado existentes al guardar el objeto que se asocia al atributo. Por ejemplo, al cifrar el atributo de contraseña se cifra la contraseña cuando se guarda el perfil del usuario.

Nota: Para cifrar el valor de atributo, la tarea que utiliza para guardar el objeto debe incluir el atributo. Para cifrar el atributo de contraseña en el ejemplo anterior, asegúrese de que el campo de contraseña se agrega a la tarea que utiliza para guardar el objeto, como la tarea Modificar usuario.

Todos los nuevos objetos se crean con valores cifrados en el almacén de usuarios.

Siga estos pasos:

1. Complete una de las siguientes tareas:
   - Cree un directorio de CA Identity Manager.
   - Actualice un directorio existente exportando la configuración del directorio.
2. Agregue los siguientes atributos de clasificación de datos al atributo que desea cifrar en el archivo directory.xml:

   AttributeLevelEncrypt

   Persiste el valor de atributo de forma cifrada en el almacén de usuarios.

   sensitive (opcional)

   Oculta el valor de atributo en pantallas de CA Identity Manager. Por ejemplo, una contraseña se muestra como asteriscos (*).

   Por ejemplo:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false"
multivalued="false" maxlength="0" searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Si ha creado un directorio de CA Identity Manager, asocie el directorio a un entorno.
4. Para obligar a que CA Identity Manager cifre todos los valores inmediatamente, modifique todos los objetos mediante el cargador masivo.

   Nota: Para obtener más información sobre el cargador masivo, consulte la *Guía de administración*.

Cómo eliminar cifrado de nivel de atributo

Si existe un atributo cifrado en el directorio de CA Identity Manager y se almacena con el valor de ese atributo como un texto no cifrado, a continuación se puede eliminar la clasificación de datos de AttributeLevelEncrypt.

Una vez que la clasificación de datos se haya eliminado, CA Identity Manager dejará de cifrar los valores de nuevos atributo. Los valores existentes se descifran cuando se guarda el objeto que se asocia al atributo.

Nota: Para descifrar el valor de atributo, la tarea que utiliza para guardar el objeto debe incluir el atributo. Por ejemplo, para descifrar una contraseña para un usuario existente, guarde el objeto de usuario con una tarea que incluya el campo de contraseña, como la tarea Modificar usuario.

Para obligar a que CA Identity Manager detecte y descifre algunos valores cifrados que permanecen en el almacén de usuarios para el atributo, se puede especificar otra clasificación de datos: PreviouslyEncrypted. El valor de texto no cifrado se guarda en el almacén de usuarios cuando se guarda el objeto.

Nota: Al agregar la clasificación de los datos de PreviouslyEncrypted agrega procesamiento adicional en la carga de cada objeto. Para impedir que se produzcan incidencias de rendimiento, se debe considerar la posibilidad de agregar la clasificación de datos de PreviouslyEncrypted, cargar y guardar cada objeto que se asocia a ese atributo, y eliminar después la clasificación de datos. Este método convierte automáticamente todos los valores cifrados almacenados en texto no cifrado almacenado.

Siga estos pasos:

1. Exporte la configuración del directorio para el directorio de CA Identity Manager adecuado.
2. En el archivo directory.xml, elimine la clasificación de datos, AttributeLevelEncrypt, de los atributos que desea descifrar.
3. Si desea obligar a que CA Identity Manager elimine previamente los valores cifrados, agregue el atributo de clasificación de datos de PreviouslyEncrypted.

   Por ejemplo:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Para obligar a que CA Identity Manager descifre todos los valores inmediatamente, modifique todos los objetos mediante el cargador masivo.

   Nota: Para obtener más información sobre el cargador masivo, consulte la *Guía de administración*.

Consideraciones sobre CA Directory

Cuando se describen atributos para un almacén de usuarios de CA Directory, tenga en cuenta los siguientes puntos:

- Los nombres de atributo distinguen mayúsculas de minúsculas.
- Al utilizar el atributo seeAlso como atributo que indica un grupo autosuscriptor, se pueden producir errores cuando los administradores creen grupos.

Al utilizar el atributo photo como atributo que indica el estado de una cuenta de usuario (activada o desactivada), se pueden producir errores cuando un administrador crea un usuario.

Nota: Para obtener información adicional sobre los requisitos de CA Directory, consulte la documentación de CA Directory.

Consideraciones sobre Microsoft Active Directory

Al describir atributos para Active Directory, tenga en cuenta los puntos siguientes:

- Las mayúsculas y minúsculas de los atributos especificados en las descripciones de atributo deben coincidir con las de los atributos en Active Directory. Por ejemplo, cuando se selecciona el atributo unicodePwd como atributo para almacenar contraseñas de usuarios, especifique unicodePwd (con una letra mayúscula P) en el archivo de configuración del directorio.
- Para objetos de usuario y grupo, asegúrese de que incluye el atributo sAMAccountName.

Consideraciones sobre el servidor de directorios de IBM

Cuando se describen atributos para un directorio de usuarios de servidor de directorios de IBM, consulte las secciones siguientes:

- Grupos en directorios de servidor de directorio (en la página 78)
- El Objectclass "Top" en la descripción de objeto de organización (en la página 79)

Grupos en directorios de servidor de directorio

El servidor de directorios de IBM requiere grupos que contengan como mínimo un miembro. Para abordar este requisito, CA Identity Manager agrega un *usuario ficticio* como miembro de un grupo nuevo cuando se crea el grupo.

Configuración de usuarios ficticios

Siga estos pasos:

1. En la sección de objeto de grupo del archivo de configuración del directorio, busque los elementos siguientes:

   ```
   <PropertyDict name="DUMMY_USER">
       <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
   </PropertyDict>
   ```

   Nota: Si estos elementos no se encuentren en el archivo de configuración del directorio, agréguelos exactamente tal y como se muestra aquí.

2. Sustituya ##DUMMY_USER_DN por un nombre destacado. CA Identity Manager agrega este nombre destacado como miembro de todos los grupos nuevos.

   Nota: Si se especifica el nombre destacado de un usuario existente; a continuación, ese usuario se muestra como un miembro de todos los grupos de CA Identity Manager. Para evitar que el *usuario ficticio* se muestre como un miembro del grupo, especifique un nombre destacado que no exista en el directorio.

3. Guarde el archivo de configuración del directorio.

El Objectclass "Top" en la descripción de objeto de organización

Importante: En la descripción del objeto de organización en el archivo de configuración del directorio, no incluya top de objectclass.

Por ejemplo, cuando el objectclass del objeto de organización es top, organizationalUnit, especifique el objectclass tal y como se muestra a continuación:

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

Al incluir top, los resultados de la búsqueda se pueden volver impredecibles.

Consideraciones de directorio de Internet de Oracle

Cuando se describen atributos para un almacén de usuarios del directorio de Internet de Oracle (OID), especifique los atributos de LDAP utilizando solamente letras en minúscula.

Atributos conocidos para un almacén de usuarios de LDAP

Los atributos conocidos tienen un significado especial en CA Identity Manager. Se identifican tal y como se muestra en la siguiente sintaxis:

%ATTRIBUTENAME%

En esta sintaxis, *ATTRIBUTENAME* debe estar en mayúscula.

Un atributo conocido se asigna a un atributo físico mediante una descripción del atributo (en la página 122).

En la descripción del atributo siguiente, el atributo userpassword está asignado al atributo conocido %PASSWORD% para que CA Identity Manager trate el valor de tblUsers.password como una contraseña:

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Algunos atributos conocidos son obligatorios y otros son opcionales.

Atributos conocidos de usuarios

Una lista de atributos conocidos de usuario y los elementos a los cuales se asignan puede ser la siguiente:

%ADMIN_ROLE_CONSTRAINT%

Asigna a la lista de roles de administrador de un administrador.

El atributo físico que se asigna a %ADMIN_ROLE_CONSTRAINT% debe tener varios valores para incluir varios roles.

Se recomienda la indexación del atributo LDAP que esté asignado a %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

Se asigna al estado de la certificación de un usuario.

Este atributo es obligatorio para utilizar la función de certificación de usuario.

Nota: Para obtener más información sobre la certificación de usuarios, consulte la *Guía de administración*.

%DELEGATORS%

Se asigna a una lista de usuarios quiénes han delegado elementos de trabajo al usuario actual.

Este atributo es obligatorio para utilizar la delegación. El atributo físico que se ha asignado a %DELEGATORS% debe tener varios valores y poder contener cadenas.

Importante: Si se edita este campo utilizando directamente tareas de CA Identity Manager o una herramienta externa, se pueden provocar implicaciones de seguridad importantes.

%EMAIL%

Se asigna a una dirección de correo electrónico de un usuario.

Se requiere para utilizar la función de notificación de correo electrónico.

%ENABLED_STATE%

(Obligatorio)

Se asigna al estado de un usuario.

Nota: Este atributo debe coincidir con el atributo de directorio de usuarios Disabled Flag en el directorio de usuarios de SiteMinder.

%FIRST_NAME%

Se asigna al nombre de un usuario.

%FULL_NAME%

Se asigna al nombre y los apellidos de un usuario.

%IDENTITY_POLICY%

Especifica la lista de políticas de identidad que se han aplicado a una cuenta de usuario y una lista de ID de política de la política exprés única que han realizado acciones de adición o eliminación en el objeto de usuario.

CA Identity Manager utiliza este atributo para determinar si es obligatorio aplicar una política de identidad a un usuario. Por ejemplo, la política tiene activado el parámetro Aplicar una vez activada y la política se muestra en el atributo %IDENTITY_POLICY%. CA Identity Manager no aplica los cambios en la política del usuario.

Nota: Para obtener más información sobre las políticas de identidad, consulte la *Guía de administración*.

%LAST_CERTIFIED_DATE%

Se asigna a la fecha en que los roles se certifican a un usuario.

Se requiere para utilizar la función de certificación de usuario.

Nota: Para obtener más información sobre la certificación de usuarios, consulte la *Guía de administración*.

%LAST_NAME%

Se asigna a los apellidos de un usuario.

%MEMBER_OF%

Se asigna a la lista de grupos de los cuales el usuario es miembro.

El atributo físico que se ha asignado a %MEMBER_OF% debe tener varios valores con objeto de incluir varios grupos.

Al utilizar este atributo, se mejora tiempo de respuesta al buscar grupos de un usuario.

Se puede utilizar este atributo con Active Directory o cualquier esquema de directorio que mantenga la pertenencia a grupo de un usuario en el objeto de usuario.

%ORG_MEMBERSHIP%

(Obligatorio)

Se asigna al nombre destacado de la organización a la cual pertenece el usuario.

CA Identity Manager utiliza este atributo conocido para determinar la estructura de un directorio (en la página 86).

Este atributo no es obligatorio cuando el directorio de usuarios no incluye organizaciones.

%ORG_MEMBERSHIP_NAME%

(Obligatorio)

Se asigna al nombre sencillo de la organización en el que se encuentra el perfil del usuario.

Este atributo no es obligatorio cuando el directorio de usuarios no incluye organizaciones.

%PASSWORD%

Se asigna a la contraseña de un usuario.

Este atributo debe coincidir con el atributo **de contraseña** en la conexión con el directorio de usuarios de SiteMinder.

Nota: El valor del atributo %PASSWORD% se muestra siempre como una serie de caracteres de asterisco (*) en las pantallas de CA Identity Manager, incluso cuando el atributo o el campo no estén establecidos para ocultar contraseñas.

%PASSWORD_DATA%

(Requerido para la compatibilidad con la política de contraseñas).

Especifica el atributo que realiza el seguimiento de la información de la política de contraseñas.

Nota: El valor del atributo %PASSWORD_DATA% se muestra siempre como una serie de caracteres de asterisco (*) en las pantallas de CA Identity Manager, incluso cuando el atributo o el campo no estén establecidos para ocultar contraseñas.

%PASSWORD_HINT%

(Obligatorio)

Se asigna a un par de pregunta y respuesta que ha especificado el usuario. El par de pregunta y la respuesta se utilizan cuando los usuarios olvidan sus contraseñas.

Para que sean compatibles con pares de varias preguntas y respuestas, asegúrese de que el atributo %PASSWORD_HINT% tiene varios valores.

Si se está utilizando la función de servicios de contraseña de SiteMinder para gestionar contraseñas, el atributo de sugerencia de contraseña debe coincidir con el atributo de respuesta o pista en el directorio de usuarios de SiteMinder.

Nota: El valor del atributo %PASSWORD% se muestra siempre como una serie de caracteres de asterisco (*) en las pantallas de CA Identity Manager, incluso cuando el atributo o el campo no estén establecidos para ocultar contraseñas.

%USER_ID%

(Obligatorio)

Se asigna al ID de un usuario.

Atributos conocidos de grupos

Los elementos siguientes son la lista de atributos conocidos de grupos:

%GROUP_ADMIN_GROUP%

Indica qué atributo almacena una lista de grupos que son administradores del grupo. Por ejemplo, cuando el grupo 1 un administrador del grupo A, el grupo 1 se almacena en el atributo %GROUP_ADMIN_GROUP%.

Nota: Si no se especifica un atributo %GROUP_ADMIN_GROUP%, CA Identity Manager almacena grupos de administradores en el atributo %GROUP_ADMIN%.

Nota: Para agregar un grupo como un administrador de otro grupo, consulte la *Guía de administración*.

%GROUP_ADMIN%

Indica qué atributo contiene los nombres destacados de administradores de un grupo.

El atributo físico que se asigna a %GROUP_ADMIN% debe tener varios valores.

%GROUP_DESC%

Indica qué atributo contiene la descripción de un grupo.

%GROUP_MEMBERSHIP%

(Obligatorio)

Indica qué atributo contiene una lista del miembro de un grupo.

El atributo físico que asigna a %GROUP_MEMBERSHIP% debe tener varios valores.

El atributo conocido %GROUP_MEMBERSHIP% no es obligatorio para los directorios de usuario de aprovisionamiento.

%GROUP_NAME%

(Obligatorio)

Indica qué atributo almacena un nombre de grupo.

%ORG_MEMBERSHIP%

(Obligatorio)

Indica qué atributo contiene el nombre destacado de la organización a la cual pertenece el grupo.

CA Identity Manager utiliza este atributo conocido para determinar la estructura del directorio (en la página 86).

Este atributo no es obligatorio cuando el directorio de usuarios no incluye organizaciones.

%ORG_MEMBERSHIP_NAME%

Indica qué atributo contiene el nombre sencillo de la organización en la que se encuentra el grupo.

Este atributo no es válido para directorios de usuarios que no incluyen organizaciones.

%SELF_SUBSCRIBING%

Indica qué atributo determina si los usuarios se pueden suscribir a un grupo (en la página 86).

%NESTED_GROUP_MEMBERSHIP%

Indica qué atributo almacena una lista de grupos que son miembros del grupo. Por ejemplo, cuando el grupo 1 es miembro del grupo A, el grupo 1 se almacena en el atributo %NESTED_GROUP_MEMBERSHIP%.

Si no se especifica un atributo %NESTED_GROUP_MEMBERSHIP%, CA Identity Manager almacena grupos anidados en el atributo %GROUP_MEMBERSHIP%.

Para incluir grupos como miembros de otros grupos, configure la compatibilidad con grupos anidados tal y como se describe en la sección de configuración de grupos anidados y dinámicos.

%DYNAMIC_GROUP_MEMBERSHIP%

Indica qué atributo almacena la consulta de LDAP que genera un grupo dinámico (en la página 148).

Nota: Para extender los atributos disponibles para que el objeto de grupo incluya los atributos %NESTED_GROUP_MEMBERSHIP% y %DYNAMIC_GROUP_MEMBERSHIP%, se pueden utilizar clases de objeto auxiliares.

Organización de atributos conocidos

Los siguientes atributos conocidos se aplican solamente a entornos que son compatibles con organizaciones:

%ORG_DESCR%

Indica qué atributo contiene la descripción de una organización.

%ORG_MEMBERSHIP%

(Obligatorio)

Indica qué atributo contiene el nombre destacado de la organización principal de una organización.

%ORG_MEMBERSHIP_NAME%

Indica qué atributo contiene el nombre sencillo de la organización principal de una organización.

%ORG_NAME%

(Requerido)

Indica qué atributo contiene el nombre de la organización.

Atributo %ADMIN_ROLE_CONSTRAINT%

Cuando se crea un rol de administrador, se especifican una o varias reglas para la pertenencia a roles. Los usuarios que cumplen las reglas de pertenencia obtienen el rol. Por ejemplo, cuando la regla de pertenencia para el rol Gestor de usuarios es title=Gestor de usuarios, los usuarios que tengan el cargo Gestor de usuarios, poseerán el rol Gestor de usuarios.

Nota: Para obtener más información sobre reglas, consulte la *Guía de administración*.

%ADMIN_ROLE_CONSTRAINT% permite designar un atributo de perfil para almacenar los roles de administrador de un administrador.

Cómo utilizar el atributo %ADMIN_ROLE_CONSTRAINT%

Para utilizar %ADMIN_ROLE_CONSTRAINT% como restricción para todos los roles de administrador, lleve a cabo las tareas siguientes:

- Empareje el atributo conocido %ADMIN_ROLE_CONSTRAINT% con un atributo de perfil con varios valores para incluir varios roles.
- Cuando se configura un rol de administrador en la Consola de usuario, es necesario asegurarse de la restricción siguiente:

  `Admin Roles equals` *`role name`*

  role name

  Define el nombre del rol para el que se está proporcionando la restricción, como en el siguiente ejemplo:

  `Admin Roles equals User Manager`

Note: Admin Roles es el nombre para mostrar predeterminado del atributo %ADMIN_ROLE_CONSTRAINT%.

Configuración de atributos conocidos

Realice el procedimiento siguiente para configurar atributos conocidos.

Siga estos pasos:

1. En el archivo de configuración del directorio, busque el signo siguiente:

   ##
2. Sustituya el valor que empiece por ## con el atributo LDAP adecuado.
3. Repita los pasos 1 y 2 hasta que haya sustituido todos los valores obligatorios.
4. Asigne atributos conocidos opcionales a atributos físicos, según sea necesario.
5. Guarde el archivo de configuración del directorio.

Descripción de la estructura del directorio de usuarios

CA Identity Manager utiliza el atributo conocido %ORG_MEMBERSHIP% para determinar la estructura de un directorio de usuarios.

El procedimiento para describir la estructura del directorio de usuarios depende del tipo de estructura de directorios.

Cómo describir una estructura de directorios jerárquica

El archivo de configuración del directorio ya está configurado para una estructura de directorios jerárquica. Como resultado, no es necesario modificar la descripción del atributo %ORG_MEMBERSHIP%.

Cómo describir una estructura del directorio de usuarios plana

Siga estos pasos:

1. Busque la descripción del atributo %ORG_MEMBERSHIP% en la sección del objeto de usuario del archivo directory.xml.
2. En el parámetro physicalname, sustituya %ORG_MEMBERSHIP% por el nombre del atributo que almacene la organización a la cual pertenece el usuario.

Cómo describir una estructura del directorio plana

Siga estos pasos:

1. Busque la descripción del atributo %ORG_MEMBERSHIP% en la sección del objeto de usuario del archivo directory.xml.
2. En el parámetro physicalname, sustituya %ORG_MEMBERSHIP% por el nombre del atributo que almacene la organización a la cual pertenece el usuario.
3. Repita el paso 1 en la sección de objeto de grupo.
4. En el parámetro physicalname, sustituya %ORG_MEMBERSHIP% por el nombre del atributo que almacene la organización a la cual pertenece el grupo.

Cómo describir un directorio de usuarios que no es compatible con organizaciones

Se debe verificar que no se han definido descripciones de objetos o atributos conocidos para organizaciones en directory.xml.

Cómo configurar grupos

En el caso de la configuración, los grupos se pueden dividir del siguiente modo:

- Grupos autosuscriptores
- Grupos anidados y dinámicos

Configuración del grupos autosuscriptores

Se puede permitir que los usuarios de autoservicio se unan a grupos configurando la compatibilidad para grupos autosuscriptores en el archivo de configuración del directorio.

Cuando un usuario se autorregistra, CA Identity Manager busca grupos en las organizaciones especificadas y, a continuación, muestra los grupos autosuscriptores al usuario.

Siga estos pasos:

1. En la sección de grupos autosuscriptores, agregue un elemento SelfSubscribingGroups de la siguiente manera:

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. Agregue valores para los siguientes parámetros:

   type

   Indica dónde busca CA Identity Manager grupos autosuscriptores de la siguiente manera:

   - NONE: CA Identity Manager no busca grupos. Especifique NONE para evitar que los usuarios se autosuscriban a grupos.
   - ALL: CA Identity Manager empieza a buscar grupos en la raíz. Especifique ALL cuando los usuarios se puedan suscribir a grupos de toda la jerarquía del directorio.
   - INDICATEDORG: CA Identity Manager busca grupos autosuscriptores en la organización de un usuario y sus suborganizaciones. Por ejemplo, cuando el perfil de un usuario está en la organización Marketing, CA Identity Manager busca grupos autosuscriptores en la organización Marketing y en todas las suborganizaciones.
   - SPECIFICORG: CA Identity Manager busca en una organización específica. Se debe proporcionar el nombre destacado (DN) de la organización específica en el parámetro org.

   org

   Especifica el identificador único de la organización en la que CA Identity Manager busca los grupos autosuscriptores.

   Nota: Es necesario asegurarse de que se especifica el parámetro org cuando type=SPECIFICORG.

Cuando se haya configurado la compatibilidad con grupos autosuscriptores en el directorio de CA Identity Manager, los administradores de CA Identity Manager pueden especificar qué grupos se autosuscriben en la Consola de usuario.

Nota: Para obtener más información sobre la gestión de grupos, consulte la *Guía de administración*.

Configuración de grupos anidados y dinámicos

Si se está gestionando un almacén de usuarios LDAP, se puede configurar la compatibilidad para los siguientes tipos de grupos en el archivo de configuración del directorio:

Grupos dinámicos

Permite definir la pertenencia a grupos especificando una consulta de filtro de LDAP en la Consola de usuario de forma dinámica. Con los grupos dinámicos, los administradores no tienen que buscar y agregar los miembros del grupo de forma individual.

Grupos anidados

Permite agregar grupos como miembros de otros grupos.

Se pueden activar los grupos dinámicos y anidados utilizando el archivo de configuración del directorio.

Siga estos pasos:

1. Asigne los siguientes atributos conocidos (en la página 83) a un atributo físico para el objeto gestionado del grupo, según sea necesario:
   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   Nota: El atributo físico que se seleccione debe ser compatible con varios valores.
2. En la sección de comportamiento de los grupos del directorio, agregue el siguiente elemento GroupTypes:

   ```
   <GroupTypes type=group>
   ```

   Nota: GroupTypes distingue entre mayúsculas y minúsculas.

3. Escriba un valor para el siguiente parámetro:

   group

   Permite la compatibilidad con grupos dinámicos y anidados. Los valores válidos son los siguientes:

   - NONE: CA Identity Manager no es compatible con grupos dinámicos y anidados.
   - ALL: CA Identity Manager es compatible con grupos dinámicos y anidados.
   - DYNAMIC: CA Identity Manager es compatible con grupos dinámicos solamente.
   - NESTED: CA Identity Manager es compatible con grupos anidados solamente.

Cuando se configure la compatibilidad con grupos dinámicos y anidados en el directorio de CA Identity Manager, los administradores de CA Identity Manager pueden especificar qué grupos son dinámicos y cuáles son anidados en la Consola de usuario.

Nota: Es posible que se establezca el tipo de grupo como NESTED o ALL *sin* establecer el parámetro conocido %NESTED_GROUP_MEMBERSHIP%. En tal caso, CA Identity Manager almacena tanto los grupos anidados como los usuarios en el parámetro conocido %GROUP_MEMBERSHIP%. El procesamiento de la pertenencia a grupos puede ser un poco más lento.

Adición de compatibilidad para grupos como administradores de grupos

Si se está gestionando un almacén de usuario LDAP, se pueden activar grupos para que actúen de administradores de otros grupos. Cuando se asigna un grupo como administrador, solamente los administradores de ese grupo son administradores del grupo especificado. Los miembros del grupo del administrador que se especifique no tendrán ningún privilegio para gestionar el grupo.

Siga estos pasos:

1. Asigne el atributo conocido %GROUP_ADMIN_GROUP% a un atributo físico que almacene la lista de grupos que actúan de administradores.

   Nota: El atributo físico que se seleccione debe ser compatible con varios valores.

   En Atributos conocidos de grupos (en la página 83) se proporciona más información acerca del atributo %GROUP_ADMIN_GROUP%.

   Nota: Si se establece el tipo de grupo de administrador como ALL sin establecer el atributo conocido %GROUP_ADMIN_GROUP%, CA Identity Manager almacena los grupos de administrador en el atributo %GROUP_ADMIN%.

2. En la sección de comportamiento de grupos de administradores del directorio, configure el elemento AdminGroupTypes como se muestra a continuación:

   <AdminGroupTypes type="ALL">

   El valor predeterminado de AdminGroupTypes es NONE.

   Nota: AdminGroupTypes distingue entre mayúsculas y minúsculas.

Cuando se haga configurado la compatibilidad con grupos como administradores en el directorio de CA Identity Manager, los administradores de CA Identity Manager podrán especificar grupos como administradores de otros grupos en la Consola de usuario.

Reglas de validación

Una regla de validación impone requisitos sobre los datos que un usuario escribe en un campo de pantalla de tarea. Los requisitos pueden imponer un formato o tipo de datos. De modo que, es necesario asegurarse de que los datos son válidos en el contexto de otros datos en la pantalla de tarea.

Las reglas de validación están asociadas con los atributos del perfil. CA Identity Manager garantiza que los datos introducidos para un atributo de perfil cumplen todas las reglas de validación asociadas antes de procesar una tarea.

Se pueden definir reglas de validación y se pueden asociar con atributos de perfil en el archivo de configuración del directorio.

Propiedades del directorio de CA Identity Manager adicionales

Se pueden configurar las siguientes propiedades adicionales:

- Orden de clasificación de los resultados de búsquedas.
- Búsqueda en las clases de objeto para verificar que un usuario nuevo no existe.
- Tiempo de espera para evitar que CA Identity Manager agote el tiempo de espera antes de que se complete la replicación de datos, del directorio LDAP principal al directorio LDAP esclavo.

Configuración del orden de clasificación

Se puede especificar un atributo de clasificación para cada objeto gestionado, como usuarios, grupos u organizaciones. CA Identity Manager utiliza este atributo para ordenar los resultados de búsquedas con una lógica empresarial personalizada, que se crea con las API de CA Identity Manager.

Nota: El atributo de clasificación no afecta a la forma en que se muestran los resultados en la Consola de usuario.

Por ejemplo, cuando se especifica el atributo cn para el objeto de usuario, CA Identity Manager ordena los resultados de una búsqueda de usuarios alfabéticamente por el atributo cn.

Siga estos pasos:

1. Después del último elemento IMSManagedObjectAttr de la sección para el objeto gestionado al cual se aplica el orden de clasificación, agregue las siguientes instrucciones:

   ```
   <PropertyDict name="SORT_ORDER">
       <Property name="ATTR">su_atributo_clasificación
       </Property>
   </PropertyDict>
   ```

2. Sustituya *su_atributo_clasificación* con el atributo por el cual CA Identity Manager clasificará los resultados de la búsqueda.

Nota: Se debe especificar solamente un atributo físico. No se debe especificar un atributo conocido.

Por ejemplo, quizá se necesite clasificar los resultados de la búsqueda de usuarios en función del valor del atributo cn. En ese caso, se deben agregar los siguientes elementos después del último elemento IMSManagedObjectAttr de la sección del objeto de usuario del archivo de configuración del directorio:

```
<!-- ******************* User Object ******************* -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

Búsqueda en objectclass

CA Identity Manager busca en el almacén de usuarios para comprobar si el usuario existe o no cuando éste se crea. Esta búsqueda se limita a usuarios que tienen objectclass especificados en la definición de objeto de usuario en el archivo de configuración del directorio (directory.xml). Si no se encuentra ningún usuario existente en esos objectclass, CA Identity Manager intentará crear el usuario.

Si existe un usuario con el mismo identificador único (ID de usuario) pero con un objectclass diferente, el servidor LDAP no podrá crear el usuario. Se informa del error en el servidor LDAP, pero CA Identity Manager no lo reconoce. CA Identity Manager parece crear el usuario correctamente.

Para evitar esta incidencia, se puede configurar una propiedad SEARCH_ACROSS_CLASSES, que hace que CA Identity Manager busque usuarios en todas las definiciones de objectclass al comprobar si hay usuarios existentes.

Nota: Esta propiedad afecta solamente a búsquedas de usuarios duplicados al realizar tareas como la creación de usuarios. Para todas las demás búsquedas, se aplican las restricciones de objectclass.

Siga estos pasos:

1. En el archivo de configuración del directorio (directory.xml), busque el elemento ImsManagedObject que describe el objeto de usuario.

2. Agregue el siguiente elemento PropertyDict:

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Nota: El elemento PropertyDict debe ser el último elemento en el elemento ImsManagedObject, como en el siguiente ejemplo:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
description="Department" valuetype="String" required="true"
multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Especificación del tiempo de espera de la replicación

En una implementación que incluya la replicación entre los directorios LDAP principal y esclavo, se puede configurar el servidor de políticas de SiteMinder para que se comunique con un directorio esclavo. En esta configuración, el servidor de políticas detecta automáticamente referencias que apunten al directorio principal durante las operaciones que escriban datos en el directorio LDAP. Los datos se almacenan en el directorio LDAP principal y se replican en el directorio LDAP esclavo según el esquema de replicación de los recursos de red.

En esta configuración, cuando se crea un objeto en CA Identity Manager, el objeto se crea en el directorio principal y se replica también al directorio esclavo. Puede que se produzca un retraso durante el proceso de replicación que provoque un error en la acción de creación en CA Identity Manager.

Para evitar que ocurra esta incidencia, se puede especificar la cantidad de tiempo (en segundos) que CA Identity Manager espera antes de que se agote el tiempo de espera en la propiedad REPLICATION_WAIT_TIME.

Siga estos pasos:

1. En el archivo de configuración del directorio (directory.xml), busque el elemento ImsManagedObject que describe el objeto de usuario.
2. Agregue el siguiente elemento PropertyDict:

   ```
   <PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
   for LDAP provider to allow replication to propagate from master to slave">
   <Property name=REPLICATION_WAIT_TIME><time in seconds></Property>
   </PropertyDict>
   ```

   Nota: El elemento PropertyDict debe ser el último elemento en el elemento ImsManagedObject, como en el siguiente ejemplo:

   ```
   <ImsManagedObject name="User" description="My Users"
   objectclass="top,person,organizationalperson,inetorgperson,customClass"
   objecttype="USER">
   <ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
   description="Department" valuetype="String" required="true"
   multivalued="false" maxlength="0" />
   .
   .
   .
   <PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
   for LDAP provider to allow replication to propagate from master to slave">
   <Property name=REPLICATION_WAIT_TIME>800</Property>
   </PropertyDict>
   ```

Cuando no se define el tiempo de espera de la replicación, se utiliza el valor predeterminado 0.

Cómo especificar la configuración de la conexión LDAP

Para mejorar el rendimiento, se pueden especificar los siguientes parámetros en el archivo de configuración del directorio (directory.xml):

Tiempo de espera de conexión

Especifica el número máximo de milisegundos que CA Identity Manager busca en un directorio antes de terminar la búsqueda.

Esta propiedad se especifica en el archivo de configuración del directorio como se muestra a continuación:

com.sun.jndi.ldap.connect.timeout

Tamaño máximo de la agrupación de conexiones

Especifica el número máximo de conexiones que CA Identity Manager puede realizar al directorio LDAP.

Esta propiedad se especifica en el archivo de configuración del directorio como se muestra a continuación:

com.sun.jndi.ldap.connect.pool.maxsize

Tamaño predeterminado de la agrupación de conexiones

Especifica el número predeterminado de conexiones entre CA Identity Manager y el directorio LDAP.

Esta propiedad se especifica en el archivo de configuración del directorio como se muestra a continuación:

com.sun.jndi.ldap.connect.pool.prefsize

Siga estos pasos:

1. En el archivo de configuración del directorio (directory.xml), busque el elemento ImsManagedObject que describe el objeto de usuario.
2. Agregue el siguiente elemento PropertyDict:

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection
Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. Guarde el archivo directory.xml.

   CA Identity Manager configura estos parámetros de configuración cuando se crea el directorio de CA Identity Manager con este archivo.

Cómo mejorar el rendimiento de las búsquedas en directorios

Para mejorar el rendimiento de las búsquedas en directorios de usuarios, organizaciones y grupos, se deben llevar a cabo las siguientes acciones:

- Indexar los atributos que los administradores pueden especificar en las consultas de búsqueda.

  Nota: En el caso del directorio de Internet de Oracle, una búsqueda puede producir un error cuando un atributo de una consulta de búsqueda no está indexado.

- Configurar los parámetros de configuración de máximo de filas y de tamaño de la página (en la página 97) para determinar cómo manejará CA Identity Manager las búsquedas grandes.

- Ajustar el directorio de usuarios. Consulte la documentación del directorio de usuarios que esté utilizando.

Cómo mejorar el rendimiento de las búsquedas grandes

Cuando CA Identity Manager gestiona un almacén de usuarios muy grande, las búsquedas que devuelven muchos resultados pueden hacer que el sistema se quede sin memoria. Para ayudar a evitar incidencias con la memoria, se pueden definir límites para las búsquedas grandes.

Los dos parámetros de configuración siguientes determinan cómo manejará CA Identity Manager las búsquedas grandes:

- Número máximo de filas

  Especifica el número máximo de resultados que CA Identity Manager puede devolver al buscar un directorio de usuarios. Cuando el número de resultados supera el límite, se muestra un error.

- Tamaño de la página

  Especifica el número de objetos que se pueden devolver en una búsqueda única. Si el número de objetos supera el tamaño de la página, CA Identity Manager realizará varias búsquedas.

  Se deben tener en cuenta los siguientes aspectos al especificar el tamaño de la página:

  - Para utilizar la opción Search Page Size (Tamaño de la página de búsqueda), el almacén de usuarios que gestiona CA Identity Manager debe ser compatible con la paginación. Algunos tipos de almacén de usuarios requieren configuración adicional para ser compatibles con la paginación. Si desea obtener más información, consulte los siguientes temas:

    Configuración de la compatibilidad con la paginación de servidor de directorios del sistema Sun Java (en la página 99)

    Configuración de la compatibilidad con la paginación de Active Directory

  - Si el almacén de usuarios no es compatible con la paginación y se especifica un valor para maxrows, CA Identity Manager utilizará solamente el valor de maxrows para controlar el tamaño de la búsqueda.

Se pueden configurar límites de máximo de filas y de tamaño de la página en los siguientes lugares:

- Almacén de usuarios

  En la mayor parte de los almacenes de usuarios y bases de datos, se pueden configurar límites de búsqueda.

  Nota: Para obtener más información, consulte la documentación del almacén de usuarios o la base de datos que esté utilizando.

- Directorio de CA Identity Manager

  Se puede configurar el elemento DirectorySearch (en la página 59) en el archivo de configuración del directorio (directory.xml) que se utiliza para crear el directorio de CA Identity Manager.

  De forma predeterminada, el valor máximo para las filas y el tamaño de la página es ilimitado para los directorios existentes. Para los directorios nuevos, el valor máximo para las filas es ilimitado y el valor para el tamaño de la página es 2000.

- Definición de objeto gestionado

  Para establecer los límites de máximo de filas y los tamaños de página que se aplican a un tipo de objeto en lugar de a un directorio completo, se configura la *definición del objeto gestionado* (en la página 61) en el archivo directory.xml que se utiliza para crear el directorio de CA Identity Manager.

  El establecimiento de límites para un tipo de objeto gestionado permite hacer ajustes basados en las necesidades empresariales. Por ejemplo, la mayor parte de las compañías tienen más usuarios que grupos. Esas compañías pueden establecer límites para las búsquedas de objetos de usuario solamente.

- Pantallas de búsqueda de tarea

  Se puede controlar el número de resultados de la búsqueda que los usuarios ven en las pantallas de búsqueda y lista en la Consola de usuario. Si el número de resultados supera el número de resultados por página definidos para la tarea, los usuarios verán vínculos a páginas de resultados adicionales.

  Esta configuración no afecta al número de resultados que devuelve una búsqueda.

  Nota: Para obtener información acerca de la configuración del tamaño de la página en pantallas de búsqueda y lista, consulte la *Guía de administración*.

Si los límites de máximo de fila y de tamaños de la página están definidos en varios lugares, se aplicará la configuración más específica. Por ejemplo, los parámetros de configuración de los objetos gestionados tienen prioridad sobre los de nivel de directorio.

Configuración de la compatibilidad con la paginación de servidor de directorios del sistema Sun Java

Los servidores de directorios del sistema Sun Java son compatibles con la vista de lista virtual (VLV), un método para proporcionar resultados de búsqueda en un orden o en subconjuntos determinados. Este método difiere de los resultados en páginas simples, que se esperan CA Identity Manager.

Para utilizar VLV, se establecen permisos y se crean índices. CA Identity Manager incluye los siguientes archivos en los que se debe configurar la compatibilidad con la paginación:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Estos archivos se incluyen como parte del ejemplo de NeteAuto, en samples\NeteAuto en las herramientas administrativas.

Las herramientas administrativas están instaladas en las siguientes ubicaciones predeterminadas:

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

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

Siga estos pasos:

1. Agregue el siguiente parámetro al elemento DirectorySearch (en la página 59) en el archivo directory.xml para el directorio de CA Identity Manager como se muestra a continuación:

   ```
   minsortrules="1"
   ```

   Nota: Si se modifica un directorio de CA Identity Manager existente, consulte Cómo actualizar la configuración de un directorio de CA Identity Manager (en la página 187).

2. Establezca los permisos para el archivo vlvcntrl.ldif como se muestra a continuación:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. Importe las definiciones de indexación y búsqueda VLV como se muestra a continuación:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. Detenga el directorio como se muestra a continuación:
   ```
   stop-slapd
   ```

5. Cree los índices mediante runvlvindex.
6. Inicie el directorio como se muestra a continuación:
   `start-slapd`

Configuración de la compatibilidad con la paginación de Active Directory

Para configurar la compatibilidad con la paginación en Active Directory, complete los siguientes pasos de alto nivel:

- Configuración de la compatibilidad con la vista de lista virtual (en la página 100).
- Configuración de MaxPageSize para Active Directory (en la página 101). (**Para directorios creados con una versión anterior a CA Identity Manager r12.5 SP7 solamente**).

Configuración de la compatibilidad con la vista de lista virtual (VLV)

Active Directory es compatible con la vista de lista virtual (VLV), un método para proporcionar resultados de búsqueda en un orden o en subconjuntos determinados. Este método difiere de los resultados en páginas simples, que se esperan CA Identity Manager.

Para utilizar VLV, se establecen permisos y se crean índices. CA Identity Manager incluye los siguientes archivos en los que se debe configurar la compatibilidad con la paginación:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Estos archivos se incluyen como parte del ejemplo de NeteAuto, en samples\NeteAuto en las herramientas administrativas.

Las herramientas administrativas están instaladas en las siguientes ubicaciones predeterminadas:

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

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

Siga estos pasos:

1. Agregue el siguiente parámetro al elemento DirectorySearch (en la página 59) en el archivo directory.xml para el directorio de CA Identity Manager como se muestra a continuación:

   ```
   minsortrules="1"
   ```

   Nota: Si se modifica un directorio de CA Identity Manager existente, consulte Cómo actualizar la configuración de un directorio de CA Identity Manager (en la página 187).

2. Establezca los permisos para el archivo vlvcntrl.ldif como se muestra a continuación:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. Importe las definiciones de indexación y búsqueda VLV como se muestra a continuación:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. Detenga el directorio como se muestra a continuación:
   ```
   stop-slapd
   ```

5. Cree los índices mediante runvlvindex.

6. Inicie el directorio como se muestra a continuación:
   ```
   start-slapd
   ```

Configuración de MaxPageSize en Active Directory

El valor predeterminado de MaxPageSize en Active Directory es 1000. Puede que el valor del atributo maxpagesize en directory.xml sea mayor o igual a 1000. Si esto es así, CA Identity Manager no mostrará una advertencia cuando el número de resultados de la búsqueda supere el valor de maxrows en directory.xml. En ese caso, los administradores que realicen la búsqueda no sabrán que se han omitido algunos resultados de la búsqueda.

Para evitar esta incidencia, se debe verificar que el valor del atributo maxpagesize del directorio y de cada objeto gestionado es menor que MaxPageSize en Active Directory.

Puede que se esté creando un directorio de CA Identity Manager mediante el archivo directory.xml de plantilla que está instalado con CA Identity Manager 12.5 SP7 o superior. En este caso, no es necesario llevar a cabo pasos adicionales para admitir la paginación. El atributo maxpagesize de directory.xml está establecido de forma predeterminada.

Si se agrega la compatibilidad con la paginación a un directorio de CA Identity Manager existente, el atributo maxpagesize de directory.xml deberá ser menor que 1000.

Además, si MaxPageSize de Active Directory es igual a 1000, es necesario asegurarse de establecer el atributo maxpagesize de forma adecuada en el directorio de CA Identity Manager y todos los objetos gestionados.

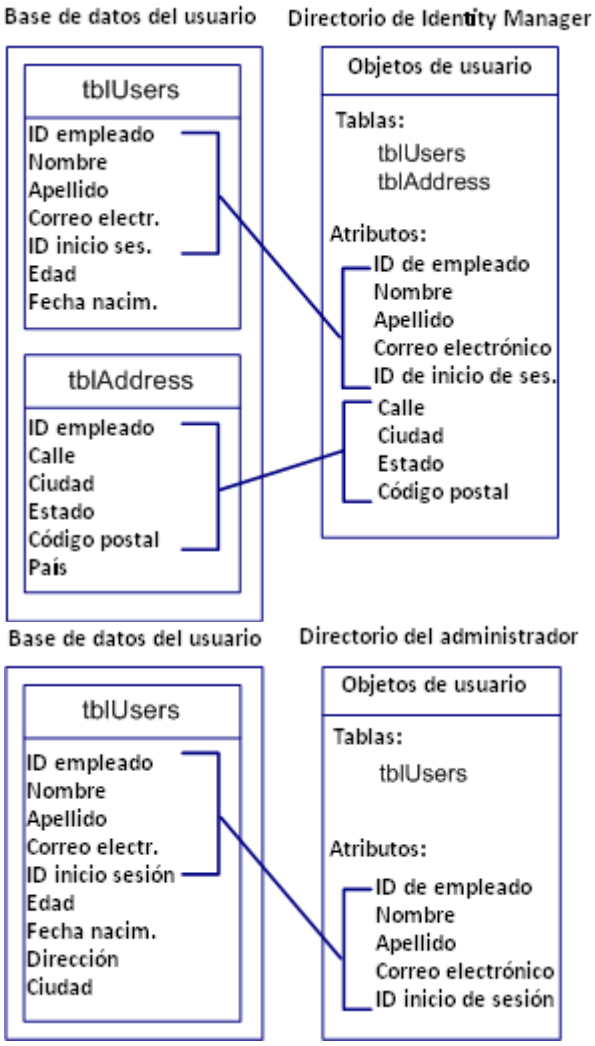
Capítulo 4: Gestión de bases de datos relacionales

Esta sección contiene los siguientes temas:

Directorios de CA Identity Manager

En un *directorio de CA Identity Manager* se describe cómo se almacenan objetos, como usuarios, grupos y (de forma opcional) organizaciones, en el almacén de usuarios y cómo se representan en CA Identity Manager. Un directorio de CA Identity Manager se asocia con uno o varios entornos de CA Identity Manager.

En la siguiente ilustración se muestra cómo se relaciona un directorio de CA Identity Manager con un almacén de usuarios:



Nota: Algunos atributos de usuario de la base de datos no forman parte del directorio de CA Identity Manager. Por lo tanto, CA Identity Manager no los gestiona.

Notas importantes sobre la configuración de CA Identity Manager para bases de datos relacionales

Antes de configurar CA Identity Manager para la gestión de una base de datos relacional, se debe garantizar que la base de datos cumple los siguientes requisitos:

- Debe poder accederse a la base de datos mediante un controlador JDBC o un controlador de conectividad abierta de bases de datos (ODBC) (cuando CA Identity Manager se integra con SiteMinder). El controlador debe ser compatible con las combinaciones externas. Si se utilizan más de dos tablas para representar un objeto gestionado, el controlador también debe ser compatible con las combinaciones externas anidadas.

  Nota: Si el controlador no es compatible con las combinaciones externas, CA Identity Manager utilizará combinaciones internas al consultar la base de datos. Esto puede provocar resultados de consulta inesperados.

- Se debe identificar de forma exclusiva cada objeto que CA Identity Manager gestione, como usuarios, grupos u organizaciones (cuando sean compatibles). Por ejemplo, el identificador único de los usuarios puede ser un ID de inicio de sesión.

  Nota: Es necesario asegurarse de que el identificador único se almacena en una sola columna.

- CA Identity Manager requiere que algunos atributos tengan varios valores, que se pueden almacenar como una lista delimitada en una sola celda o en varias filas en una tabla separada. Por ejemplo, la siguiente tabla tblGroupMembers almacena los miembros de un grupo:

ID	Miembros
Investigación	dmason
Investigación	rsavory
Marketing	dmason
Marketing	awelch

La columna ID contiene el identificador único de cada grupo y la columna Miembros contiene el identificador único de cada miembro del grupo. Por ejemplo, dmason y rsavory son miembros del grupo Investigación. Cuando se agrega un miembro nuevo a ese grupo, se agrega otra fila a tblGroupMembers.

- Cuando el entorno incluye organizaciones, se debe llevar a cabo lo siguiente:
  - Editar y ejecutar un script de SQL, incluido con CA Identity Manager, con respecto a la base de datos para configurar la compatibilidad con organizaciones (en la página 150).
  - CA Identity Manager requiere una organización de nivel superior, denominada raíz. Todas las demás organizaciones están relacionadas con la organización raíz.

    Para obtener más información sobre los requisitos de las organizaciones, consulte Gestión de organizaciones (en la página 149).

Creación de un origen de datos de Oracle para WebSphere

Siga estos pasos:

1. En la Consola de administración de WebSphere, navegue al proveedor de JDBC que se creó al configurar el controlador JDBC.
2. Cree un origen de datos con las siguientes propiedades y haga clic en Aplicar:

   Nombre: User Store Data Source

   Nombre de JNDI: userstore

   Dirección URL: jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*
3. Configure una nueva entrada de datos de autenticación J2C para el origen de datos del almacén de usuarios:
   a. Introduzca las siguientes propiedades:

      Alias: User Store

      ID de usuario: *username*

      Contraseña: *password*

      donde *username* y *password* son el nombre del usuario y la contraseña de la cuenta que se especificó cuando se creó la base de datos.

   b. Haga clic en Aceptar y, a continuación, utilice los vínculos de navegación de la parte superior de la pantalla para volver al origen de datos que está creando.
4. Seleccione la entrada de datos de autenticación J2C del almacén de usuarios que ha creado en el cuadro de lista en los campos siguientes:
   - Alias de autenticación de componente gestionado
   - Alias de autenticación de contenedor gestionado
5. Haga clic en Aceptar y guarde la configuración.

   Nota: Para verificar que el origen de datos se configura correctamente, haga clic en Probar conexión en la pantalla de configuración del origen de datos. Si se produce un error la conexión de prueba, reinicie WebSphere y vuelva a probar la conexión.

Cómo crear un directorio de CA Identity Manager

Siga estos pasos:

1. Si está utilizando SiteMinder, aplique el esquema del almacén de políticas antes de crear un directorio de CA Identity Manager.

   Nota: Para obtener más información sobre esquemas de almacén de políticas específicos y cómo aplicarlos, consulte la *Guía de instalación*.

2. Si está utilizando SiteMinder, cree un origen de datos ODBC para utilizarlo con SiteMinder (en la página 113).

3. Cree un origen de datos para la base de datos de usuarios que gestiona CA Identity Manager.

4. Describa la base de datos para CA Identity Manager modificando un archivo de configuración del directorio (directory.xml). Para obtener más información, consulte Cómo describir una base de datos en un archivo de configuración del directorio.

5. En la Consola de gestión, importe el archivo de configuración del directorio y cree el directorio.

Cómo crear un origen de datos JDBC

CA Identity Manager requiere un origen de datos JDBC en el servidor de aplicaciones donde esté instalado CA Identity Manager para conectarse al almacén de usuarios. Las instrucciones para crear un origen de datos son diferentes para cada servidor de aplicaciones.

Creación de un origen de datos JDBC para servidores de aplicaciones JBoss

Siga estos pasos:

1. Cree una copia del siguiente archivo:

   jboss_home\server\default\deploy\objectstore-ds.xml

   jboss home

   La ubicación de la instalación del servidor de aplicaciones Jboss donde se instala CA Identity Manager.

   El archivo nuevo debe existir en la misma ubicación.

2. Cambie el nombre del archivo a userstore-ds.xml.

3. Edite userstore-ds.xml como se muestra a continuación:
   a. Busque el elemento <jndi-name>.
   b. Cambiar el valor del elemento <jndi-name> de jdbc/objectstore a userstore como se muestra a continuación:

      <jndi-name>userstore</jndi-name>

   c. En el elemento <connection-url>, cambie el parámetro DatabaseName al nombre de la base de datos que actúa como almacén de usuarios, como se muestra a continuación:

      <connection-url>

      jdbc:sqlserver://*ipaddress:port*;selectMethod=cursor;DatabaseName=*userstore_name*

      </connection-url>

      ipaddress

      Especifica la dirección IP del equipo donde está instalado el almacén de usuarios.

      puerto

      Especifica el número de puerto de la base de datos.

      userstore_name

      Especifica el nombre de la base de datos que actúa como almacén de usuarios.

4. Lleve a cabo los siguientes pasos si planea crear un territorio de seguridad de JBoss, que se requiere para la compatibilidad con FIPS:
   a. Cambie el nombre de security-domain a <security-domain>imuserstoredb</security-domain>.
   b. Guarde el archivo.
   c. Omita los pasos restantes. En cambio, complete los pasos para crear un territorio de seguridad de JBoss para el origen de datos JDBC (en la página 109).
5. Realice los siguientes cambios adicionales en userstore-ds.xml:
   a. Cambie el valor del elemento <user-name> al nombre de usuario de una cuenta que tenga acceso de lectura y escritura al almacén de usuarios.
   b. Cambie el valor del elemento <password> a la contraseña de la cuenta especificada en el elemento <user-name>.

   Nota: El nombre de usuario y la contraseña aparecen en texto no cifrado en este archivo. Por lo tanto, es posible decidir crear un territorio de seguridad de JBoss en lugar de editar userstore-ds.xml.
6. Guarde el archivo.

Uso de un territorio de seguridad de JBoss para el origen de datos JDBC

Es necesario asegurarse de que se está creando un origen de datos JDBC en un servidor de aplicaciones JBoss. Se puede configurar el origen de datos para que utilice un nombre de usuario y una contraseña o para que utilice un dominio de seguridad.

Importante: Es necesario asegurarse de que se utiliza la opción de territorio de seguridad de JBoss si se está utilizando FIPS.

Siga estos pasos:

1. Complete los pasos de Creación de un origen de datos JDBC para servidores de aplicaciones JBoss (en la página 107).

   No especifique un nombre de usuario y una contraseña en userstore-ds.xml como se describe en el paso 4.

2. Abra login-cfg.xml en *jboss_home*\server\default\conf.

3. Busque la siguiente entrada en el archivo:

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option
name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=N
oTxCM</module-option>
    </login-module>
  </authentication>
</application-policy>
```

4. Copie toda la entrada y péguela dentro de las etiquetas <policy> y </policy> del archivo login-cfg.xml.

5. En la entrada que se ha pegado en el archivo, realice los siguientes cambios:

   a. Cambie el valor de atributo de nombre de imobjectstoredb a imuserstoredb como se muestra a continuación:

      ```
      <application-policy name="imuserstoredb">
      ```

   b. Especifique el nombre del usuario que se usa para autenticar con respecto al almacén de usuarios como se muestra a continuación:

      ```
      <module-option name="userName">user_store_user</module-option>
      ```

   c. Especifique la contraseña para el usuario del paso anterior como se muestra a continuación:

      ```
      <module-option name="password">user_store_user_password</module-option>
      ```

Nota: Para cifrar la contraseña del almacén de usuarios, se debe usar la herramienta de contraseñas (pwdtools) que se instala con CA Identity Manager.

d. En el elemento <module-option name="managedConnectionFactoryName">, proporcione el jdbc.jca:name correcto, como se muestra a continuación:

```
<module-option name="managedConnectionFactoryName">
   jboss.jca:name=userstore,service=NoTxCM
</module-option>
```

6. Guarde el archivo.
7. Reinicie el servidor de aplicaciones.

Creación un origen de datos JDBC para WebLogic

Un origen de datos se crea en la Consola de administración de WebLogic.

Nota: Consulte la documentación de Oracle WebLogic 11 para obtener información completa acerca de las agrupaciones de conexiones de WebLogic.

Siga estos pasos:

1. Cree un origen de datos JDBC con los siguientes parámetros en la Consola de administración de WebLogic:

   Nombre: User Store Data Source

   Nombre de JNDI: userstore

2. Cree la agrupación de conexiones para el origen de datos con la siguiente información:

- Para las bases de datos SQL Server 2005, utilice los siguientes valores:

  URL: jdbc:sqlserver://*db_systemName*:1433

  Nombre de la clase de controlador: com.microsoft.sqlserver.jdbc.SQLServerDriver

  Propiedades: user=*username*

  databaseName=*user store name*

  selectMethod=cursor

  Contraseña: *password*

- En el caso de bases de datos de Oracle, utilice los siguientes valores:

  Dirección URL: jdbc:oracle:thin:@*tp_db_systemname*:1521:*oracle_SID*

  Nombre de la clase de controlador: oracle.jdbc.driver.OracleDriver

  Propiedades: user=*username*

  Contraseña: *password*

3. Después de la configuración, establezca el destino de la agrupación en la instancia del servidor *wl_server_name*.

   Después de implementar la agrupación, compruebe la consola para ver si se ha producido algún error.

   Nota: Puede que obtenga un error que diga que no se puede crear el origen de datos con una agrupación inexistente. Para resolver este error, reinicie WebLogic.

Orígenes de datos de WebSphere

Las siguientes secciones describen cómo crear un origen de datos de SQL u Oracle para servidores de aplicaciones WebSphere.

Creación de un origen de datos de SQL Server para WebSphere

Siga estos pasos:

1. En la Consola de administración de WebSphere, navegue al proveedor de JDBC que se creó al configurar el controlador JDBC.
2. Seleccione Orígenes de datos en la sección de propiedades adicionales.
3. Cree un origen de datos con las siguientes propiedades y haga clic en Aplicar:

   Nombre: User Store Data Source

   Nombre de JNDI: userstore

   databaseName: *userstore_name*

   serverName: *db_systemname*

4. Configure la propiedad selectMethod como se muestra a continuación:
   a. Seleccione Propiedades personalizadas en la sección de propiedades adicionales.
   b. Haga clic en la propiedad personalizada selectMethod.
   c. Introduzca el siguiente texto en el campo Valor:

      cursor

   d. Haga clic en Aceptar y, a continuación, utilice los vínculos de navegación de la parte superior de la pantalla para volver al origen de datos que está creando.
5. Configure una nueva entrada de datos de autenticación J2C para el origen de datos del almacén de usuarios:
   a. Seleccione entradas de datos de autenticación de arquitectura de conectores J2EE (J2C) en la sección de elementos relacionados.
   b. Haga clic en Nuevo.
   c. Introduzca las siguientes propiedades:

      Alias: User Store

      ID de usuario: *username*

      Contraseña: *password*

      donde *username* y *password* son el nombre del usuario y la contraseña de la cuenta que se especificó cuando se creó la base de datos.

   d. Haga clic en Aceptar y, a continuación, utilice los vínculos de navegación de la parte superior de la pantalla para volver al origen de datos que está creando.
6. Seleccione la entrada de datos de autenticación J2C del almacén de usuarios que ha creado en el cuadro de lista en el campo Component-managed Authentication Alias (Alias de autenticación de componente gestionado).
7. Haga clic en Aceptar y guarde la configuración.

   Nota: Para verificar que el origen de datos se configura correctamente, haga clic en Probar conexión en la pantalla de configuración del origen de datos. Si se produce un error la conexión de prueba, reinicie WebSphere y vuelva a probar la conexión.

Creación de un origen de datos de Oracle para WebSphere

Siga estos pasos:

1. En la Consola de administración de WebSphere, navegue al proveedor de JDBC que se creó al configurar el controlador JDBC.

2. Cree un origen de datos con las siguientes propiedades y haga clic en Aplicar:

   Nombre: User Store Data Source

   Nombre de JNDI: userstore

   Dirección URL: jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. Configure una nueva entrada de datos de autenticación J2C para el origen de datos del almacén de usuarios:

   a. Introduzca las siguientes propiedades:

      Alias: User Store

      ID de usuario: *username*

      Contraseña: *password*

      donde *username* y *password* son el nombre del usuario y la contraseña de la cuenta que se especificó cuando se creó la base de datos.

   b. Haga clic en Aceptar y, a continuación, utilice los vínculos de navegación de la parte superior de la pantalla para volver al origen de datos que está creando.

4. Seleccione la entrada de datos de autenticación J2C del almacén de usuarios que ha creado en el cuadro de lista en los campos siguientes:

   - Alias de autenticación de componente gestionado
   - Alias de autenticación de contenedor gestionado

5. Haga clic en Aceptar y guarde la configuración.

   Nota: Para verificar que el origen de datos se configura correctamente, haga clic en Probar conexión en la pantalla de configuración del origen de datos. Si se produce un error la conexión de prueba, reinicie WebSphere y vuelva a probar la conexión.

Cómo crear un origen de datos ODBC para su uso con SiteMinder

Si CA Identity Manager se integra con SiteMinder, se debe definir un origen de datos ODBC en el equipo de SiteMinder que apunte a la base de datos. Se debe tener en cuenta el nombre del origen de datos para su uso posterior. Continúe de la siguiente manera:

- **Windows:** Configure el origen de datos ODBC como nombre distintivo del sistema. Consulte la documentación del sistema operativo Windows para obtener instrucciones.
- **UNIX:** Agregue una entrada que especifique los parámetros del origen de datos ODBC en el archivo system_odbc.ini que se encuentra en *policy_server_installation*/db.

Cómo describir una base de datos en un archivo de configuración del directorio

Para gestionar una base de datos, CA Identity Manager debe entender la estructura y el contenido de la base de datos. Para describir la base de datos para CA Identity Manager cree un archivo de configuración del directorio (directory.xml).

El archivo de configuración del directorio contiene una o varias de las secciones siguientes:

Información del directorio de CA Identity Manager

Contiene información acerca del directorio de CA Identity Manager que utiliza CA Identity Manager.

Validación del atributo

Define las reglas de validación que se aplican al directorio de CA Identity Manager.

Información del proveedor

Describe el almacén de usuarios que gestiona CA Identity Manager.

Información de búsqueda de directorios

Permite especificar cómo busca CA Identity Manager en el almacén de usuarios.

Objeto de usuario **(en la página 116)**

Describe cómo se almacenan los usuarios en el almacén de usuarios y cómo se representan en CA Identity Manager.

Objeto de grupo **(en la página 116)**

Describe cómo se almacenan los grupos en el almacén de usuarios y cómo se representan en CA Identity Manager.

Objeto de organización **(en la página 116)**

Describe cómo se almacenan las organizaciones y cómo se representan en CA Identity Manager.

Grupos autosuscriptores

Configura la compatibilidad con grupos a los que se pueden unir los usuarios de autoservicio.

El directorio en el que se instalaron las herramientas administrativas para CA Identity Manager incluye la siguiente plantilla del archivo de configuración del directorio para bases de datos relacionales:

admin_tools\directoryTemplates\RelationalDatabase\directory.xml

admin_tools

Define la ubicación de la instalación de herramientas administrativas de CA Identity Manager, como en los siguientes ejemplos:

- **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Nota: La plantilla del archivo de configuración del directorio en directoryTemplates\RelationalDatabase está configurada para entornos compatibles con organizaciones. Para ver un archivo de configuración del directorio para un entorno que no incluya organizaciones, se puede mirar el archivo directory.xml para el ejemplo de NeteAuto que se encuentra en *admin_tools*\samples\NeteAutoRDB\NoOrganization

Se debe copiar la plantilla de configuración en un directorio nuevo o guardarlo con un nombre diferente para evitar que se sobrescriba. Entonces se podrá modificar la plantilla para reflejar la estructura de la base de datos.

El archivo de configuración del directorio tiene dos convenciones importantes:

- ##: indica valores requeridos.

  Para proporcionar toda la información obligatoria, busque todos los signos dobles de almohadilla (##) y sustitúyalos por los valores adecuados. Por ejemplo, ##PASSWORD_HINT indica que se debe proporcionar un atributo para almacenar una pregunta a la que un usuario responde para recibir una contraseña temporal en caso de olvidar la contraseña.

- @: indica valores que rellena CA Identity Manager. No se deben modificar estos valores en el archivo de configuración del directorio. CA Identity Manager pide que se proporcionen los valores cuando se importa el archivo de configuración del directorio.

Antes de modificar el archivo de configuración del directorio, se necesita la información siguiente:

- Nombres de tabla del usuario, el grupo y los objetos de organización (cuando la estructura incluye organizaciones).
- Una lista de atributos de perfiles de usuario, grupo y organización (cuando la estructura incluye organizaciones).

Modificación del archivo de configuración del directorio

Realice el siguiente procedimiento para modificar el archivo de configuración del directorio.

Siga estos pasos:

1. Configure una conexión a la base de datos.
2. Especifique la cantidad de tiempo que CA Identity Manager dedica a buscar en un directorio antes de finalizar la búsqueda.
3. Defina los objetos gestionados que CA Identity Manager gestiona (en la página 116) de usuario y grupo.
4. Modifique los atributos conocidos.

   Los atributos conocidos identifican atributos especiales, como el atributo de contraseña, en CA Identity Manager.
5. Configure la compatibilidad con grupos autosuscriptores.
6. Si el entorno incluye organizaciones, configure la compatibilidad con organizaciones.

Más información:

Descripciones de objetos gestionados (en la página 116)
Gestión de organizaciones (en la página 149)
Cómo configurar grupos autosuscriptores (en la página 148)
Atributos conocidos para una base de datos relacional (en la página 142)

Descripciones de objetos gestionados

En CA Identity Manager, se gestionan los siguientes tipos de objetos, que corresponden a entradas en un almacén de usuarios:

- Usuarios: representan los usuarios de una empresa.
- Grupos: representan asociaciones de usuarios que tienen algo en común.
- Organizaciones (organizaciones): representan unidades de negocio. Las organizaciones pueden contener usuarios, grupos y otras organizaciones.

  Nota: En Gestión de organizaciones (en la página 149) se proporciona información acerca de la configuración de organizaciones.

Una descripción de objeto contiene la siguiente información:

- Información acerca del objeto (en la página 117), como las tablas en las cuales se almacena el objeto.
- Los atributos que almacenan información acerca de una entrada (en la página 122). Por ejemplo, el atributo de buscapersonas almacena un número de buscapersonas.

Importante: Un entorno de CA Identity Manager es compatible solamente con un tipo de objeto de organización, usuario y grupo.

Cómo describir un objeto gestionado

Un objeto gestionado se describe especificando la información del objeto en las secciones de objeto de usuario, objeto de grupo y objeto de organización (cuando la base de datos incluye organizaciones) del archivo de configuración del directorio.

Cada una de estas secciones contiene un elemento ImsManagedObject, como el siguiente código:

```
<ImsManagedObject name="User" description="My Users">
```

El elemento ImsManagedObject puede incluir los siguientes elementos:

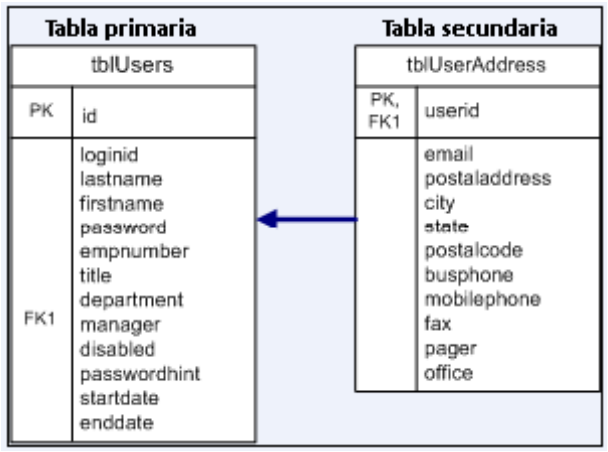
- Table (obligatorio)
- UniqueIdentifier (obligatorio)
- ImsManagedObjectAttr (obligatorio)
- RootOrg (para objetos de organización solamente)

Tablas de la base de datos

El elemento de tabla en el archivo de configuración del directorio se utiliza para definir las tablas que almacenan información acerca de un objeto gestionado.

Cada objeto gestionado debe tener una tabla primaria que contenga el identificador único del objeto. La información adicional se puede almacenar en tablas secundarias.

En la siguiente ilustración se muestra una base de datos que almacena la información de usuario en una tabla primaria y una secundaria:



Si la información de un objeto se almacena en varias tablas, cree un elemento Table para cada tabla. Utilice el elemento Reference del elemento Table para definir la relación entre una tabla secundaria y una primaria.

Por ejemplo, si la información básica de un usuario está almacenada en tblUsers y la información de dirección está almacenada en tblUserAddress, las definiciones de tabla para el objeto gestionado del usuario se parecerían a las entradas siguientes:

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

Elementos de tabla

Los parámetros de un elemento de tabla son los siguientes:

name

(Requerido)

Especifica el nombre de la tabla que almacena algunos o todos los atributos de un perfil gestionado de un objeto.

primary

Indica si la tabla es la primaria para el objeto gestionado. La tabla primaria contiene el identificador único del objeto, como se muestra a continuación:

- Verdadero: la tabla es la tabla primaria.
- Falso: la tabla es una tabla secundaria (valor predeterminado).

Si no se especifica el parámetro primary, CA Identity Manager da por hecho que la tabla es una tabla secundaria.

Nota: Solamente puede haber una tabla primaria.

filtro

Identifica un subconjunto de las entradas de la tabla que se aplica al objeto gestionado.

El parámetro opcional de filtro se puede parecer al siguiente ejemplo:

```
filter="ORG=2"
```

Nota: El filtro se aplica solamente a consultas que genere CA Identity Manager. Si se sobrescribe una consulta generada con una consulta personalizada, se debe especificar el filtro en la consulta personalizada.

fullouterjoin

Indica si la combinación externa es una combinación externa completa.

- Verdadero: la combinación externa es una combinación externa completa. En este caso, la condición que se requiere para devolver una fila válida se encuentra en las dos tablas en la combinación para devolver una fila.
- Falso: La combinación externa es una combinación externa izquierda relativa a la tabla primaria. En este caso, solamente deben cumplir la condición las filas de una tabla de la consulta (valor predeterminado).

Nota: Los parámetros son opcionales a menos que se especifique lo contrario.

El parámetro Table puede contener uno o varios elementos Reference para vincular una tabla primaria con tablas secundarias.

Elemento de referencia

Los parámetros del elemento Reference son los siguientes:

childcol

Indica la columna de la tabla secundaria (especificada en el elemento de tabla correspondiente) que se asigna a la columna de la tabla primaria.

primarycol

Indica la columna de la tabla primaria que se asigna a la columna de la tabla secundaria.

Nota: Los parámetros son opcionales a menos que se especifique lo contrario.

Especificación de la información del objeto

La información del objeto se especifica proporcionando valores para diversos parámetros.

Siga estos pasos:

1. Busque el elemento ImsManagedObject en la sección de objeto de usuario, objeto de grupo u objeto de organización.
2. Proporcione valores para los siguientes parámetros:

   name

   (Requerido)

   Proporciona un nombre único para el objeto gestionado.

   descripción

   Proporciona la descripción del objeto gestionado.

   objecttype

   (Requerido)

   Especifica el tipo de objeto gestionado. Los valores válidos son los siguientes:

   - USER
   - GROUP
   - ORGANIZATION

   El elemento ImsManagedObject se debe parecer al siguiente código:

   ```
   <ImsManagedObject name="User" description="My  Users" objecttype="USER">
   ```

3. Proporcionar la información de la tabla, como se describe en Tablas de la base de datos (en la página 117).
4. Especifique la columna que contiene el identificador único para el objeto (en la página 121).
5. Describa los atributos que constituyen el perfil del objeto (en la página 122).
6. Si se está configurando un objeto de organización, vaya a Gestión de organizaciones (en la página 149).

Cómo especificar el identificador único para un objeto gestionado

Cada objeto que gestiona CA Identity Manager debe tener un identificador único. Es necesario asegurarse de que el identificador único se almacena en una columna única en la tabla primaria del objeto gestionado. Las tablas primarias están descritas en Tablas de la base de datos (en la página 117).

Utilice los elementos UniqueIdentifier y UniqueIdentifierAttr para definir el identificador único como se muestra a continuación:

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="tablename.columnname" />
</UniqueIdentifier>
```

El elemento UniqueIdentifierAttr requiere el parámetro de nombre. El valor del parámetro de nombre es el atributo en el que se almacena el identificador único. El valor puede ser un atributo físico o un atributo conocido (en la página 79).

Cuando se especifica un atributo físico, se deben tener en cuenta los siguientes puntos:

- Asegúrese de que el atributo especificado existe en la base de datos y está definido en el archivo de configuración del directorio, como se describe en Cómo modificar descripciones de atributos (en la página 122). En la descripción del atributo, asegúrese de especificar un permiso de sólo lectura o de una sola escritura para evitar que el identificador único cambie durante una sesión.
- Utilice la siguiente sintaxis para especificar un atributo físico:

  nombretabla.nombrecolumna

  nombretabla

  Define el nombre de la tabla en la que se encuentra el atributo. La tabla que se especifica debe ser la tabla primaria.

  nombrecolumna

  Define el nombre de la columna que almacena el atributo.

- Si la base de datos genera el identificador único, especifique una operación personalizada para el atributo (en la página 133). Por ejemplo, puede tener que especificar una operación que busque el último identificador generado de la base de datos.

Cómo modificar descripciones de atributos

Un atributo almacena información acerca de una entidad de organización, usuario o grupo, como un número de teléfono o dirección. Los atributos de una entidad determinan su perfil.

En el archivo de configuración del directorio, los atributos están descritos en los elementos ImsManagedObjectAttr. En las secciones de objeto de usuario, objeto de grupo y objeto de organización del archivo de configuración del directorio:

- Modifique las descripciones predeterminadas de los atributos para describir los atributos de la base de datos.
- Cree nuevas descripciones de atributos copiando una descripción existente y modificando los valores según sea necesario.

Para cada atributo de los perfiles de usuario, grupo y organización, solamente hay un elemento ImsManagedObjectAttr. Por ejemplo, un elemento ImsManagedObjectAttr puede describir un ID de usuario.

Un elemento ImsManagedObjectAttr tiene el aspecto del siguiente código:

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

Nota: Cuando se está utilizando una base de datos de Oracle, se deben tener en cuenta los siguientes puntos durante la configuración de atributos de objetos gestionados:

- Las bases de datos de Oracle distinguen entre mayúsculas y minúsculas de forma predeterminada. Las mayúsculas y minúsculas de los atributos y los nombres de tabla del archivo de configuración del directorio deben coincidir con las de los atributos de Oracle.

  Es necesario asegurarse de especificar una longitud máxima para los tipos de datos de cadenas para evitar los truncamientos. Para limitar la longitud de las cadenas, se puede crear una regla de validación para que muestre un error cuando un usuario escriba una cadena que supere la longitud máxima.

Los parámetros de ImsManagedObjectAttr son los siguientes:

Nota: Los parámetros son opcionales a menos que se especifique lo contrario.

physicalname

(Requerido)

Especifica el nombre físico del atributo y debe contener uno de los siguientes detalles:

- El nombre y la ubicación donde se almacena el valor.

  Formato: *nombretabla.nombrecolumna*

  Por ejemplo, cuando un atributo se almacena en la columna de ID de la tabla tblUsers, el nombre físico de ese atributo es el siguiente:

  tblUsers.id

  Es necesario definir cada tabla que contenga un atributo en un elemento Table (en la página 117).

- Un atributo conocido.

  Un atributo conocido puede representar un valor calculado. Por ejemplo, se puede utilizar un atributo conocido para hacer referencia a un atributo calculado mediante una operación personalizada (en la página 133).

displayname

(Requerido)

Especifica un nombre único para el atributo.

En la Consola de usuario, el nombre para mostrar aparece en la lista de atributos que están disponibles para agregar a una pantalla de tarea.

Nota: No se debe modificar el displayname de un atributo en el archivo de configuración del directorio (directory.xml). Para cambiar el nombre de un atributo en una pantalla de tarea, se puede especificar una etiqueta para el atributo en la definición de pantalla de tarea. Para obtener más información, consulte la *Guía de administración*.

descripción

Proporciona la descripción del atributo.

valuetype

Especifica el tipo de datos del atributo. Los valores válidos son los siguientes:

STRING

El valor puede ser cualquier cadena.

Éste es el valor predeterminado.

Entero

El valor debe ser un número entero.

Nota: Entero no admite números decimales.

Número

El valor debe ser un número entero. La opción de número admite números decimales.

Fecha

El valor debe analizar una fecha válida mediante el patrón:

DD/MM/AAAA

ISODate

El valor debe analizar una fecha válida mediante el patrón aaaa-MM-dd.

UnicenterDate

El valor debe analizar una fecha válida mediante el patrón YYYYYYYDDD, donde:

YYYYYYY es una representación del año de siete números que empieza con tres ceros. Por ejemplo: 0002008

DDD es una representación del día de tres números que empieza con ceros, según sea necesario. Los valores válidos incluyen de 001 a 366.

Si el valuetype de un atributo es incorrecto, puede que se produzca un error con las consultas de CA Identity Manager.

Para asegurarse de que un atributo se almacena correctamente en la base de datos, se puede asociar con una regla de validación.

required

Indica si es obligatorio especificar un valor para el atributo, como se muestra a continuación:

- Verdadero: obligatorio
- Falso: opcional (valor predeterminado)

multi-valued

Indica si el atributo puede tener varios valores, como se muestra a continuación:

- Verdadero: un atributo puede tener varios valores.
- Falso: un atributo puede tener solamente un valor único (valor predeterminado).

Por ejemplo, el atributo de pertenencia a un grupo en un perfil de usuario tiene varios valores para almacenar los grupos a los cuales pertenece un usuario.

Para almacenar atributos con varios valores en una lista delimitada en lugar de en una tabla de varias filas, es necesario definir el carácter delimitador en el parámetro delimiter.

Es necesario asegurarse de que el número de posibles valores y la longitud de cada valor que permite la columna son suficientes.

Importante: Es necesario asegurarse de que el atributo de pertenencia a grupo de la definición del objeto de usuario tiene varios valores.

wellknown

Proporciona el nombre del atributo conocido.

Los atributos conocidos tienen un significado específico en CA Identity Manager.

Formato: %*ATTRIBUTENAME*%

Nota: Cuando una operación personalizada se asocia con un atributo, se debe especificar un atributo conocido (en la página 79).

maxlength

Determina el tamaño máximo de la columna.

permission

Indica si el valor de un atributo se puede modificar en una pantalla de tarea, como se muestra a continuación:

READONLY

El valor se muestra pero no se puede modificar.

WRITEONCE

No se puede modificar el valor una vez que el objeto se haya creado. Por ejemplo, no se puede cambiar un ID de usuario después de que el usuario se haya creado.

READWRITE

El valor se puede modificar (valor predeterminado).

hidden

Indica si un atributo aparece en las pantallas de tarea CA Identity Manager, como se muestra a continuación:

- True: el atributo no se muestra a usuarios.
- False: el atributo se muestra a usuarios (valor predeterminado).

Los atributos lógicos utilizan atributos ocultos.

Nota: Para obtener más información sobre los atributos lógicos, consulte la *Guía de programación para Java*.

system

Indica que solamente CA Identity Manager utiliza los atributos. Los usuarios no deben modificar los atributos en la Consola de usuario, como se muestra a continuación:

- True: los usuarios no pueden modificar el atributo. El atributo no aparecerá en la Consola de usuario.
- Falso: los usuarios pueden modificar este atributo y se encuentra disponible para agregarse a pantallas de tarea en la Consola de usuario (valor predeterminado).

validationruleset

Asocia un conjunto de reglas de validación con el atributo.

Es necesario asegurarse de que el conjunto de reglas de validación que se especifica está definido en un elemento ValidationRuleSet en el archivo de configuración del directorio.

delimiter

Define el carácter que separa los valores cuando se almacenan varios en una sola columna.

Importante: Es necesario asegurarse de que el parámetro de varios valores está establecido en verdadero para que se aplique el parámetro de delimitador.

Nota: Para evitar que se muestre información confidencial, como contraseñas o salarios, en la Consola de usuario se pueden especificar los parámetros de clasificación de datos (en la página 74).

Gestión de atributos confidenciales

CA Identity Manager proporciona los siguientes métodos para gestionar atributos confidenciales:

- Clasificaciones de datos para atributos

  Las clasificaciones de los datos permiten especificar las propiedades de visualización y cifrado para los atributos en el archivo de configuración del directorio (directory.xml).

  Se pueden definir clasificaciones de datos que gestionan atributos confidenciales de la siguiente forma:

  - En pantallas de tarea de CA Identity Manager, se muestra el valor de un atributo como una serie de asteriscos.

    Por ejemplo, se pueden mostrar contraseñas como asteriscos en lugar de mostrarlas en texto no cifrado.

  - En las pantallas Ver tareas enviadas, oculte el valor de atributo.

    Esta opción permite ocultar atributos de administradores. Por ejemplo, ocultar detalles de salario como el salario de los administradores que ven el estado de las tareas en CA Identity Manager pero no deben consultar detalles de salario.

  - Ignore determinados atributos al crear una copia de un objeto existente.

  - Cifre un atributo.

- Estilos del campo en pantallas de perfil de tarea

  Si no se desea modificar un atributo en el archivo directory.xml, establezca la propiedad de visualización para el atributo en las definiciones de la pantalla donde se muestra el atributo confidencial.

  El estilo del campo permite mostrar atributos, como las contraseñas, como una serie de asteriscos en vez de texto no cifrado.

  Nota: Para obtener más información sobre el estilo del campo de atributos confidenciales, busque "estilos de campo" en la ayuda de la Consola de usuario.

Atributos de clasificación de datos

El elemento de clasificación de datos proporciona una forma de asociar propiedades adicionales con una descripción del atributo. Los valores de este elemento determinan cómo CA Identity Manager gestiona el atributo. Este elemento es compatible con los siguientes parámetros:

- sensitive

  Hace que CA Identity Manager muestre el atributo como una serie de asteriscos (*) en las pantallas Ver tareas enviadas. Este parámetro impide que los atributos antiguos y nuevos del atributo se muestren en texto no cifrado en las pantallas Ver tareas enviadas.

  Además, si se crea una copia de un usuario existente en la Consola de usuario, este parámetro impide que el atributo se copie en el usuario nuevo.

- vst_hide

  Oculta el atributo en la pantalla Detalles del evento para la ficha Ver tareas enviadas. A diferencia de los atributos confidenciales, que se muestran como asteriscos, los atributos vst_hidden no se mostrarán.

  Se puede utilizar este parámetro para impedir que se muestren cambios en un atributo, como el salario, que en la pantalla Ver tareas enviadas.

- ignore_on_copy

  Hace que CA Identity Manager ignore un atributo cuando un administrador crea una copia de un objeto en la Consola de usuario. Por ejemplo, suponga que se ha especificado ignore_on_copy para el atributo de contraseña en un objeto de usuario. Al copiar un perfil de usuario, CA Identity Manager no aplica la contraseña del usuario actual al nuevo perfil de usuario.

- AttributeLevelEncrypt

  Cifra valores de atributo cuando se almacenan en el almacén de usuarios. Si se ha activado FIPS 140-2 para CA Identity Manager, este utilizará el cifrado RC2 o FIPS 140-2.

  Para obtener más información sobre la compatibilidad de FIPS 140-2 en CA Identity Manager, consulte la *Guía de configuración*.

  Los atributos se muestran en texto no cifrado durante el tiempo de ejecución.

  Nota: Para impedir que los atributos se muestren en texto no cifrado en las pantallas, se puede agregar también un elemento de clasificación de datos confidenciales en atributos cifrados. Para obtener más información, consulte Cómo agregar cifrado de nivel de atributo (en la página 75).

- PreviouslyEncrypted

  Hace que CA Identity Manager detecte y descifre algunos valores cifrados en el atributo cuando accede al objeto en el almacén de usuarios.

  Utilice esta clasificación de datos para descifrar algunos valores previamente cifrados.

  El valor de texto no cifrado se guarda en el almacén cuando se guarda el objeto.

Configuración de atributos de clasificación de datos

Siga estos pasos:

1. Busque el atributo en el archivo de configuración del directorio.
2. Después de la descripción del atributo, agregue el siguiente atributo:

   <DataClassification name="*parameter*">

   parameter

   Representa uno de los parámetros siguientes:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Por ejemplo, una descripción del atributo que incluye el atributo de clasificación de los datos de vst_hide se parece al siguiente código:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Cifrado de nivel de atributo

Se puede cifrar un atributo en el almacén de usuarios especificando una clasificación de los datos de AttributeLevelEncypt para ese atributo en el archivo de configuración del directorio (directory.xml). Cuando el cifrado de nivel de atributo se activa, CA Identity Manager cifra el valor de ese atributo antes de almacenarlo en el almacén de usuarios. El atributo se muestra como texto no cifrado en la Consola de usuario.

Nota: Para impedir que los atributos se muestren en texto no cifrado en las pantallas, se puede agregar también un elemento de clasificación de datos confidenciales en atributos cifrados. Para obtener más información, consulte Cómo agregar cifrado de nivel de atributo (en la página 75).

Si se ha activado el soporte de FIPS 140-2, el atributo se cifra mediante el cifrado RC2 o FIPS 140-2.

Antes de que se implemente el cifrado de nivel de atributo, tenga en cuenta los siguientes puntos:

- CA Identity Manager no puede buscar los atributos cifrados en una búsqueda.

  Suponga que un atributo cifrado se agrega a una política de identidad, miembros o propietarios. CA Identity Manager no puede resolver la política correctamente debido a que no se puede buscar el atributo.

  Se debe considerar la posibilidad de establecer el atributo en searchable="false" en el archivo directory.xml. Por ejemplo:

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Si CA Identity Manager utiliza un almacén de usuarios compartido y un directorio de aprovisionamiento, no cifre atributos del servidor de aprovisionamiento.
- No active AttributeLevelEncrypt para contraseñas de usuario en entornos que cumplen con los siguientes criterios:
  - Que incluye integración de CA SiteMinder
  - Que se almacenen usuarios en una base de datos relacional

  Cuando CA Identity Manager se integra con CA SiteMinder, las contraseñas cifradas producen problemas cuando los usuarios nuevos intentan iniciar sesión e introducir contraseñas en el texto no cifrado.
- Si se activa el cifrado de nivel de atributo para un almacén de usuarios que utilizan aplicaciones distintas de CA Identity Manager, el resto de las aplicaciones no pueden utilizar el atributo cifrado.

Cómo agregar cifrado de nivel de atributo

Suponga que ha agregado un cifrado de nivel de atributo a un directorio de CA Identity Manager. CA Identity Manager cifra automáticamente valores de atributo de texto no cifrado existentes al guardar el objeto que se asocia al atributo. Por ejemplo, al cifrar el atributo de contraseña se cifra la contraseña cuando se guarda el perfil del usuario.

Nota: Para cifrar el valor de atributo, la tarea que utiliza para guardar el objeto debe incluir el atributo. Para cifrar el atributo de contraseña en el ejemplo anterior, asegúrese de que el campo de contraseña se agrega a la tarea que utiliza para guardar el objeto, como la tarea Modificar usuario.

Todos los nuevos objetos se crean con valores cifrados en el almacén de usuarios.

Siga estos pasos:

1. Complete una de las siguientes tareas:
   - Cree un directorio de CA Identity Manager.
   - Actualice un directorio existente exportando la configuración del directorio.
2. Agregue los siguientes atributos de clasificación de datos al atributo que desea cifrar en el archivo directory.xml:

   AttributeLevelEncrypt

   Persiste el valor de atributo de forma cifrada en el almacén de usuarios.

   sensitive (opcional)

   Oculta el valor de atributo en pantallas de CA Identity Manager. Por ejemplo, una contraseña se muestra como asteriscos (*).

   Por ejemplo:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false"
multivalued="false" maxlength="0" searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Si ha creado un directorio de CA Identity Manager, asocie el directorio a un entorno.
4. Para obligar a que CA Identity Manager cifre todos los valores inmediatamente, modifique todos los objetos mediante el cargador masivo.

   Nota: Para obtener más información sobre el cargador masivo, consulte la *Guía de administración*.

Cómo eliminar cifrado de nivel de atributo

Si existe un atributo cifrado en el directorio de CA Identity Manager y se almacena con el valor de ese atributo como un texto no cifrado, a continuación se puede eliminar la clasificación de datos de AttributeLevelEncrypt.

Una vez que la clasificación de datos se haya eliminado, CA Identity Manager dejará de cifrar los valores de nuevos atributo. Los valores existentes se descifran cuando se guarda el objeto que se asocia al atributo.

Nota: Para descifrar el valor de atributo, la tarea que utiliza para guardar el objeto debe incluir el atributo. Por ejemplo, para descifrar una contraseña para un usuario existente, guarde el objeto de usuario con una tarea que incluya el campo de contraseña, como la tarea Modificar usuario.

Para obligar a que CA Identity Manager detecte y descifre algunos valores cifrados que permanecen en el almacén de usuarios para el atributo, se puede especificar otra clasificación de datos: PreviouslyEncrypted. El valor de texto no cifrado se guarda en el almacén de usuarios cuando se guarda el objeto.

Nota: Al agregar la clasificación de los datos de PreviouslyEncrypted agrega procesamiento adicional en la carga de cada objeto. Para impedir que se produzcan incidencias de rendimiento, se debe considerar la posibilidad de agregar la clasificación de datos de PreviouslyEncrypted, cargar y guardar cada objeto que se asocia a ese atributo, y eliminar después la clasificación de datos. Este método convierte automáticamente todos los valores cifrados almacenados en texto no cifrado almacenado.

Siga estos pasos:

1. Exporte la configuración del directorio para el directorio de CA Identity Manager adecuado.
2. En el archivo directory.xml, elimine la clasificación de datos, AttributeLevelEncrypt, de los atributos que desea descifrar.
3. Si desea obligar a que CA Identity Manager elimine previamente los valores cifrados, agregue el atributo de clasificación de datos de PreviouslyEncrypted.

   Por ejemplo:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Para obligar a que CA Identity Manager descifre todos los valores inmediatamente, modifique todos los objetos mediante el cargador masivo.

   Nota: Para obtener más información sobre el cargador masivo, consulte la *Guía de administración*.

Operaciones personalizadas

Se pueden definir operaciones personalizadas para que ciertos objetos gestionados realicen las tareas siguientes:

- Utilizar procedimientos almacenados
- Optimizar las consultas para su estructura de base de datos
- Recuperar un identificador único generado por la base de datos

Las operaciones personalizadas se aplican solamente a los atributos.

Al especificar operaciones personalizadas, se deben recordar los siguientes puntos:

- Los usuarios que especifiquen operaciones personalizadas deberán estar familiarizados con SQL.
- CA Identity Manager no valida las operaciones personalizadas. Hasta el momento de la ejecución, no se informa de los errores de sintaxis y las consultas no válidas.

- Si se especifica una operación personalizada para un atributo, dicho atributo no se podrá utilizar en los filtros de búsqueda en tareas de CA Identity Manager.
- Las operaciones personalizadas se deben ajustar a los estándares de XML. Los caracteres especiales se representan mediante sintaxis de XML. Por ejemplo, se especifica un signo de comillas simples (') como '

Para especificar una operación personalizada, se utiliza el elemento de operación.

Elemento de operación

El elemento Operation define una instrucción de SQL que puede ejecutar una consulta personalizada o llama un procedimiento almacenado para la creación, recuperación, modificación o supresión de un atributo. Operation es un subelemento del elemento IMSManagedObjectAttr, como se muestra en el siguiente ejemplo:

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

Los parámetros de elemento de operación son los siguientes:

name

Especifica un nombre predefinido para una operación. Las operaciones válidas son las siguientes:

- Creación
- Obtener
- Establecer
- Supresión
- GetDB

  La operación GetDB recupera un identificador único de la base de datos durante una tarea Crear cuando el identificador único se genera mediante la base de datos o de un procedimiento almacenado.

value

Define la instrucción de SQL o el procedimiento almacenado que se debe ejecutar. Los valores válidos son los siguientes:

- INSERT
- SELECT

- UPDATE
- DELETE
- CALL (para procedimientos almacenados)

Nota: Los parámetros son opcionales a menos que se especifique lo contrario.

El elemento de operación puede contener uno o varios elementos de parámetro.

Elemento de parámetro

Un elemento de parámetro especifica los valores que se transfieren a la consulta. Cuando se definen varios elementos de parámetro, los valores se transfieren a la consulta en el orden proporcionado.

Un elemento de parámetro requiere el parámetro de nombre. El valor del parámetro de nombre puede ser un atributo físico o un atributo conocido (en la página 79).

Nota: CA Identity Manager debe entender los valores que se transfieren a una consulta en el elemento Parameter. Por ejemplo, el valor puede ser un nombre físico o un atributo conocido definido en los atributos ImsManagedObjectAttr.

Cuando se especifica un atributo físico, se deben tener en cuenta los siguientes puntos:

- Utilice la siguiente sintaxis para especificar un atributo físico:

  nombretabla.nombrecolumna

  - *nombretabla*

    Proporciona el nombre de la tabla en la que se encuentra el atributo. La tabla que se especifica debe ser la tabla primaria.

  - *nombrecolumna*

    Proporciona el nombre de la columna que almacena el atributo.

- El atributo que se especifica debe existir en la base de datos y está definido en el archivo de configuración del directorio, como se describe en Cómo modificar descripciones de atributos (en la página 122).

Ejemplo: operaciones personalizadas para el atributo de número de negocio

En el siguiente ejemplo, el atributo de número de negocio se genera llamando un procedimiento almacenado; no es un atributo físico en la base de datos.

```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

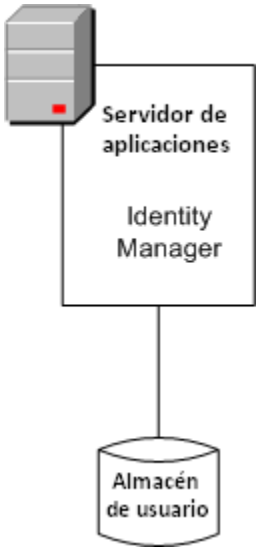
```
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

Tenga en cuenta los siguientes puntos:

- sp_getbusinessnumber, sp_setbusinessnumber y sp_deletebusinessnumber son procedimientos almacenados definidos por el usuario.
- El valor que se devuelve de la operación Obtener se asigna al atributo %BUSINESS_NUMBER%.
- La interrogación (?) indica sustituciones que se hacen en el tiempo de ejecución antes de que la consulta se ejecute. Por ejemplo, en la operación Obtener, el atributo conocido %USER_ID% se transfiere al procedimiento almacenado sp_getbusinessnumber.

Conexión al directorio de usuarios

CA Identity Manager se conecta a un directorio de usuarios para almacenar información de usuarios, grupos y organizaciones tal y como se muestra en la siguiente ilustración:



No se requiere nuevos directorios o bases de datos. Sin embargo, el directorio o la base de datos existentes deben estar en un sistema que tenga un nombre de dominio completo (FQDN).

Para consultar una lista de directorios y tipos de bases de datos compatibles, consulte el cuadro de compatibilidad de CA Identity Manager en el sitio de Soporte de CA.

Configure una conexión al almacén de usuarios al crear un directorio de CA Identity Manager en la Consola de gestión.

Si se exporta la configuración del directorio después de haber creado un directorio de CA Identity Manager, la información de conexión con el directorio de usuarios se muestra en el elemento de proveedor del archivo de configuración del directorio.

Descripción de una conexión de base de datos

Para describir una conexión de base de datos, utilice el elemento de proveedor y sus subelementos en el archivo directory.xml.

Nota: Si se está creando un directorio de CA Identity Manager, no es necesario proporcionar información de conexión del directorio en el archivo directory.xml. La información de conexión se proporciona en el asistente del directorio de CA Identity Manager en la Consola de gestión.

Modifique el elemento de proveedor solamente para realizar actualizaciones.

Elemento de proveedor

El elemento de proveedor incluye los subelementos siguientes:

JDBC (obligatorio)

Identifica el origen de datos JDBC que se debe utilizar al realizar la conexión con el almacén de usuarios. Se debe especificar el nombre de JNDI que se ha proporcionado al crear el origen de datos JDBC (en la página 107).

Credenciales (obligatorio)

Proporciona el nombre del usuario y la contraseña para acceder a la base de datos.

DSN

Identifica el origen de datos ODBC que se debe utilizar al realizar la conexión con el almacén de usuarios.

Nota: Este subelemento solamente se aplica cuando CA Identity Manager se integra con SiteMinder. En los entornos de CA Identity Manager que no incluyan SiteMinder, este subelemento se ignora.

SiteMinderQuery

Especifica esquemas de consulta personalizados para buscar información de usuario en una base de datos relacional.

Nota: Este subelemento solamente se aplica cuando CA Identity Manager se integra con SiteMinder. En los entornos de CA Identity Manager que no incluyan SiteMinder, este subelemento se ignora.

Una conexión de base de datos completada tiene el aspecto del ejemplo siguiente:

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Los atributos del elemento Provider son los siguientes:

type

Especifica el tipo de base de datos. Para las bases de datos de Microsoft SQL Server y de Oracle, se debe especificar la base de datos de recursos (valor predeterminado).

userdirectory

Especifica el nombre de la conexión del directorio de usuarios. Este parámetro corresponde al nombre del objeto de conexión que se proporciona durante la creación del directorio.

Si CA Identity Manager se integra con SiteMinder para la autenticación, crea una conexión con el directorio de usuarios en SiteMinder con el nombre que se especifique para el objeto de conexión durante la instalación. Si se desea realizar la conexión con un directorio de usuarios de SiteMinder existente, se debe introducir el nombre de ese directorio de usuarios cuando se solicite el objeto de conexión. CA Identity Manager rellena el parámetro userdirectory con el nombre que se especifique.

Si CA Identity Manager no se integra con SiteMinder, el valor del parámetro userdirectory es el nombre que se otorgue a la conexión JDBC para el almacén de usuarios.

Nota: No se debe especificar un nombre para la conexión con el directorio de usuarios en el archivo directory.xml. CA Identity Manager solicita el nombre durante la creación del directorio.

Credenciales de la base de datos

Para conectarse a la base de datos, CA Identity Manager debe proporcionar credenciales válidas al origen de datos. Las credenciales se definen en el elemento Credentials, que tiene el aspecto siguiente:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Si no se especifica una contraseña en el elemento Credentials y se intenta crear el directorio de CA Identity Manager en la Consola de gestión, ésta solicitará las credenciales de contraseña.

Nota: Se recomienda que se especifique la contraseña en la Consola de gestión.

Si se especifica la contraseña en la Consola de gestión, CA Identity Manager cifrará la contraseña. En caso contrario, si no se desea que la contraseña aparezca en texto no cifrado, la contraseña se cifra mediante la herramienta de contraseñas que se instala con CA Identity Manager. En la sección sobre contraseñas de SiteMinder hay instrucciones acerca del uso de la herramienta de contraseñas.

Nota: Se puede especificar solamente un conjunto de credenciales. Cuando se definen varios orígenes de datos, las credenciales que se especifiquen se deben aplicar a todos los orígenes de datos.

Los parámetros de las credenciales son los siguientes:

usuario

Define el ID de inicio de sesión de una cuenta que puede acceder al origen de datos.

No se debe especificar un valor para el parámetro de usuario en el archivo directory.xml. CA Identity Manager pide que se proporcione el ID de inicio de sesión al crear el directorio de CA Identity Manager en la Consola de gestión.

cleartext

Determina si la contraseña se muestra en texto no cifrado en el archivo directory.xml:

- True: la contraseña se muestra en texto no cifrado.
- False: la contraseña se cifra (valor predeterminado).

Nota: Estos parámetros son opcionales.

Nombre del origen de datos (DSN)

El elemento DSN en el archivo directory.xml tiene un parámetro: el nombre del origen de datos ODBC que CA Identity Manager utiliza para conectarse a la base de datos. El valor del parámetro de nombre debe coincidir con el nombre de un origen de datos existente.

Nota: Este elemento solamente se aplica cuando CA Identity Manager se integra con SiteMinder. Si CA Identity Manager no se integra con SiteMinder, este elemento se ignora.

Si el valor del parámetro de nombre es @SmDirDSN, no deberá especificar un nombre DSN en el archivo directory.xml. CA Identity Manager pide que se proporcione el nombre DSN cuando se importa el archivo directory.xml.

Para configurar una conmutación por error, se deben definir varios elementos DSN. Si el origen de datos principal no responde a una solicitud, el siguiente origen de datos que se defina responderá a la solicitud.

Por ejemplo, si se ha configurado la conmutación por error de la siguiente manera:

```
<DSN name="DSN1">
<DSN name="DSN2">
```

CA Identity Manager utiliza el origen de datos DSN1 para conectarse a la base de datos. Si hay un problema con DSN1, CA Identity Manager intentará conectarse a la base de datos mediante DSN2.

Nota: Las credenciales que se especifican en el elemento de credenciales (en la página 139) se deben aplicar a todos los DSN que se definan.

Esquemas de la consulta SQL

CA Identity Manager utiliza esquemas de consulta para buscar información de usuarios y grupos en una base de datos relacional.

Nota: Este elemento solamente se aplica cuando CA Identity Manager se integra con SiteMinder. En los entornos que no incluyan SiteMinder, este parámetro se ignora.

Cuando se crea un directorio de CA Identity Manager en la Consola de gestión, CA Identity Manager genera un conjunto de esquemas de consulta basados en los esquemas de consulta requeridos en SiteMinder. (Para obtener información completa acerca de los esquemas de consulta de SiteMinder, consulte la *Guía de configuración del servidor de políticas del gestor de acceso Web de CA SiteMinder*). Los nombres de tabla y de columna de los esquemas de consulta de SiteMinder se sustituyen por los datos que se especifiquen en el archivo de configuración del directorio.

Cómo definir esquemas de consulta personalizados

Los esquemas de consulta se definen en los elementos SiteMinderQuery en el archivo de configuración del directorio. Un elemento SiteMinderQuery presenta el siguiente aspecto:

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

Nota: En la consulta de ejemplo, ' es la sintaxis de XML para las comillas simples (').

El elemento SiteMinderQuery solamente se aplica cuando CA Identity Manager se integra con SiteMinder.

Los parámetros de esquema de consulta son los siguientes:

name

Especifica el nombre redefinido de un esquema de consulta de SiteMinder.

Este valor no se debe modificar.

consulta

Especifica el procedimiento almacenado o la instrucción de SQL que se debe ejecutar. Los valores válidos son los siguientes:

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (para procedimientos almacenados)

Nota: Estos parámetros son obligatorios para el elemento SiteMinderQuery.

Antes de personalizar los esquemas de consulta, se deben llevar a cabo los puntos siguientes:

- Familiarizarse con los esquemas de consulta predeterminados.

  Nota: Para obtener más información sobre los esquemas de la consulta SQL, consulte la *Guía de configuración del servidor de políticas del gestor de acceso Web de CA SiteMinder*.

- Adquirir una experiencia amplia en el desarrollo de consultas SQL.

Modificación de los esquemas de consulta predeterminados

Se debe realizar el siguiente procedimiento para modificar los esquemas de consulta predeterminados.

Siga estos pasos:

1. Exporte el archivo de configuración del directorio.

   CA Identity Manager genera un archivo de configuración del directorio que contiene todos los parámetros de configuración actuales para el directorio de CA Identity Manager, incluidos los esquemas de consulta generados.

2. Guarde el archivo de configuración del directorio.

   Nota: Si se desea crear una copia de seguridad del archivo de configuración del directorio original, guarde el archivo con un nombre diferente o en una ubicación diferente antes de guardar el archivo exportado.

3. Busque el esquema de consulta generado por CA Identity Manager que desee modificar.

4. Introduzca el esquema de consulta o el procedimiento almacenado que se ejecutará en el parámetro de la consulta.

   Nota: No se debe modificar el nombre de la consulta.

5. Después de realizar los cambios necesarios, guarde el archivo de configuración del directorio.

   Importe el archivo para actualizar el directorio de CA Identity Manager (en la página 187).

Atributos conocidos para una base de datos relacional

Los atributos conocidos tienen un significado especial en CA Identity Manager. Se identifican mediante la siguiente sintaxis:

%ATTRIBUTENAME%

En esta sintaxis, *ATTRIBUTENAME* debe estar en mayúscula.

Un atributo conocido se asigna a un atributo físico mediante una descripción del atributo (en la página 122).

En la descripción del atributo siguiente, el atributo tblUsers.password está asignado al atributo conocido %PASSWORD% para que CA Identity Manager trate el valor de tblUsers.password como una contraseña:

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Algunos atributos conocidos son obligatorios y otros son opcionales.

Atributos conocidos de usuarios

A continuación, se incluye una lista de atributos conocidos de usuarios:

%ADMIN_ROLE_CONSTRAINT%

Contiene la lista de roles de administrador (en la página 146) que se asignan al administrador (en la página 146).

El atributo físico que se asigne a %ADMIN_ROLE_CONSTRAINT% deberá tener varios valores para incluir varios roles.

Se recomienda la indexación del atributo que esté asignado a %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

(Requerido para poder utilizar la función de certificación de usuario).

Contiene el estado de certificación de un usuario.

Nota: Para obtener más información sobre la certificación de usuarios, consulte la *Guía de administración*.

%DELEGATORS%

Se asigna a una lista de usuarios quiénes han delegado elementos de trabajo al usuario actual.

Este atributo es obligatorio para utilizar la delegación. El atributo físico que se ha asignado a %DELEGATORS% debe tener varios valores y poder contener cadenas.

Importante: Si se edita este campo utilizando directamente tareas de CA Identity Manager o una herramienta externa, se pueden provocar implicaciones de seguridad importantes.

%EMAIL%

(Requerido para activar la función de notificación de correo electrónico).

Almacena la dirección de correo electrónico de un usuario.

%ENABLED_STATE%

(Requerido)

Realiza un seguimiento del estado de un usuario.

Nota: El tipo de datos del atributo físico que se asigne a %ENABLED_STATE% debe ser Cadena.

%FIRST_NAME%

Contiene el nombre de un usuario.

%FULL_NAME%

(Requerido)

Contiene el nombre y los apellidos de un usuario.

%IDENTITY_POLICY%

Contiene la lista de políticas de identidad que se han aplicado a una cuenta de usuario.

CA Identity Manager utiliza este atributo para determinar si una política de identidad se debe aplicar a un usuario. Si la política tiene activado el parámetro Aplicar una vez y la política se encuentra en el atributo %IDENTITY_POLICY%, CA Identity Manager no aplicará los cambios de la política al usuario.

Nota: Para obtener más información sobre las políticas de identidad, consulte la *Guía de administración*.

%LAST_CERTIFIED_DATE%

(Requerido para poder utilizar la función de certificación de usuario).

Contiene la fecha en la que se certificó el rol de un usuario.

Nota: Para obtener más información sobre la certificación de usuarios, consulte la *Guía de administración*.

%LAST_NAME%

Contiene los apellidos de un usuario.

%ORG_MEMBERSHIP%

(Requerido cuando se admiten organizaciones).

Contiene el identificador único de la organización a la que pertenece el usuario.

%ORG_MEMBERSHIP_NAME%

(Requerido cuando se admiten organizaciones).

Contiene el nombre sencillo de la organización a la cual pertenece el usuario.

%PASSWORD%

Contiene la contraseña de un usuario.

Nota: El valor del atributo %PASSWORD% se muestra siempre como una serie de caracteres de asterisco (*) en las pantallas de CA Identity Manager, incluso cuando el atributo o el campo no estén establecidos para ocultar contraseñas.

%PASSWORD_DATA%

(Requerido para la compatibilidad con la política de contraseñas).

Especifica el atributo que realiza el seguimiento de la información de la política de contraseñas.

Nota: El valor del atributo %PASSWORD_DATA% se muestra siempre como una serie de caracteres de asterisco (*) en las pantallas de CA Identity Manager, incluso cuando el atributo o el campo no estén establecidos para ocultar contraseñas.

%PASSWORD_HINT%

(Requerido)

Contiene los pares de pregunta y respuesta que haya especificado el usuario. Los pares de pregunta y respuesta se utilizan en el caso de que se olvide la contraseña.

Nota: El valor del atributo %PASSWORD_HINT% se muestra siempre como una serie de caracteres de asterisco (*) en las pantallas de CA Identity Manager, incluso cuando el atributo o el campo no estén establecidos para ocultar contraseñas.

%USER_ID%

(Requerido)

Almacena el ID de inicio de sesión de un usuario.

Atributos conocidos de grupos

A continuación, se incluye una lista de atributos conocidos de grupos:

%GROUP_ADMIN%

Contiene los administradores de un grupo.

Nota: El atributo %GROUP_ADMIN% deberá tener varios valores.

%GROUP_DESC%

Contiene la descripción de un grupo.

%GROUP_ID%

Contiene el identificador único de un grupo.

%GROUP_MEMBERSHIP%

(Requerido)

Contiene una lista de los miembros de un grupo.

Nota: El atributo %GROUP_MEMBERSHIP% deberá tener varios valores.

%GROUP_NAME%

(Requerido)

Almacena el nombre de un grupo.

%ORG_MEMBERSHIP%

(Requerido cuando se admiten organizaciones).

Contiene el identificador único de la organización a la que pertenece el grupo.

%ORG_MEMBERSHIP_NAME%

(Requerido cuando se admiten organizaciones).

Contiene el nombre sencillo de la organización a la cual pertenece el grupo.

%SELF_SUBSCRIBING%

Determina si los usuarios se pueden suscribir a un grupo.

Atributo %Admin_Role_Constraint%

Cuando se crea un rol de administrador, se especifican una o varias reglas para la pertenencia a roles. Los usuarios que cumplan las reglas de pertenencia tendrán el rol. Por ejemplo, si la regla de pertenencia para el rol Gestor de usuarios es title=Gestor de usuarios, los usuarios que tengan el cargo Gestor de usuarios, poseerán el rol Gestor de usuarios.

Nota: Para obtener más información sobre reglas, consulte la *Guía de administración*.

%ADMIN_ROLE_CONSTRAINT% permite designar un atributo de perfil para almacenar todos los roles de administrador de un administrador.

Cómo utilizar el atributo %ADMIN_ROLE_CONSTRAINT%

Para utilizar %ADMIN_ROLE_CONSTRAINT% como restricción para todos los roles de administrador, lleve a cabo las tareas siguientes:

- Empareje el atributo conocido %ADMIN_ROLE_CONSTRAINT% con un atributo de perfil con varios valores para incluir varios roles.

- Cuando se configura un rol de administrador en la interfaz de usuario de CA Identity Manager, el siguiente escenario puede ser una restricción:

  Admin Roles equals *role name*

  role name

  Define el nombre del rol para el cual se proporciona la restricción.

  Por ejemplo, Admin Roles equals Gestor de usuarios

Note: Admin Roles es el nombre para mostrar predeterminado del atributo %ADMIN_ROLE_CONSTRAINT%.

Configuración de atributos conocidos

Realice el procedimiento siguiente para configurar atributos conocidos.

Siga estos pasos:

1. En el archivo de configuración del directorio, busque el signo siguiente:

   ##

   Los valores obligatorios se identifican mediante dos signos de almohadilla (##).

2. Sustituya el valor que empiece por ## con el nombre del atributo físico que desee que exista en la base de datos. Proporcione el nombre del atributo mediante el formato siguiente:

   nombretabla.nombrecolumna

   Por ejemplo, si el atributo de contraseña se almacena en la columna de contraseña de la tabla de tblUsers, se debe especificar de la manera siguiente:

   `tblUsers.password`

3. Repita los pasos 1 y 2 hasta que haya sustituido todos los valores obligatorios y los valores opcionales incluidos que desee.
4. Asigne atributos conocidos opcionales a atributos físicos, según sea necesario.
5. Guarde el archivo de configuración del directorio.

Cómo configurar grupos autosuscriptores

Se puede permitir que los usuarios de autoservicio se unan a grupos configurando la compatibilidad para grupos autosuscriptores en el archivo de configuración del directorio.

Siga estos pasos:

1. En la sección de grupos autosuscriptores, agregue un elemento SelfSubscribingGroups de la siguiente manera:

   `<SelfSubscribingGroups type=`*`search_type`* `org=`*`org_dn`*`>`

2. Escriba valores para los siguientes parámetros:

   type

   Indica dónde busca CA Identity Manager grupos autosuscriptores. Los valores válidos son los siguientes:

   - NONE: CA Identity Manager no busca grupos. Especifique NONE para evitar que los usuarios se suscriban a grupos.
   - ALL: CA Identity Manager busca en todos los grupos del almacén de usuarios. Especifique ALL cuando los usuarios se puedan suscribir a todos los grupos.
   - INDICATEDORG (*para entornos compatibles con organizaciones solamente*): CA Identity Manager busca grupos autosuscriptores en la organización de un usuario y sus suborganizaciones. Por ejemplo, cuando el perfil de un usuario está en la organización Marketing, CA Identity Manager busca grupos autosuscriptores en la organización Marketing y en todas las suborganizaciones.
   - SPECIFICORG (*para entornos compatibles con organizaciones solamente*): CA Identity Manager busca en una organización específica. Se debe proporcionar el identificador único de la organización específica en el parámetro org.

   org

   Define el identificador único de la organización en la que CA Identity Manager busca los grupos autosuscriptores.

   Nota: Es necesario asegurarse de que se especifica el parámetro org si type=SPECIFICORG.

3. Reinicie el servidor de políticas de SiteMinder si se cambió alguno de los siguientes elementos:

   - El parámetro de tipo a o de SPECIFICORG
   - El valor del parámetro org

Cuando se haya configurado la compatibilidad con grupos autosuscriptores en el directorio de CA Identity Manager, los administradores de CA Identity Manager pueden especificar qué grupos se autosuscriben en la Consola de usuario.

Cuando un usuario se autorregistra, CA Identity Manager busca grupos en las organizaciones especificadas y muestra los grupos autosuscriptores al usuario.

Reglas de validación

Una regla de validación impone requisitos sobre los datos que un usuario escribe en un campo de pantalla de tarea. Los requisitos pueden imponer un formato o tipo de datos o se pueden asegurar de que los datos son válidos en el contexto de otros datos en la pantalla de tarea.

Las reglas de validación están asociadas con los atributos del perfil. Antes de que una tarea se procese, CA Identity Manager se asegura de que los datos introducidos para un atributo de perfil cumplen todas las reglas de validación asociadas.

Se pueden definir reglas de validación y se pueden asociar con atributos de perfil en el archivo de configuración del directorio.

Gestión de organizaciones

En el caso de las bases de datos relacionales, CA Identity Manager incluye la opción de gestionar organizaciones. Cuando la base de datos es compatible con organizaciones, los siguientes puntos se cumplen:

- Las organizaciones tienen una estructura jerárquica.
- Todos los objetos gestionados, como los usuarios, los grupos y otras organizaciones, pertenecen a una organización.
- Cuando se suprime una organización, los objetos que pertenecen a esa organización también se suprimen.

Un objeto de organización se configura de la misma manera en que configuran los objetos de grupo y de usuario, con algunos pasos adicionales.

Cómo configurar la compatibilidad con organizaciones

Implemente los siguientes pasos para configurar la compatibilidad con una organización:

1. Configure la compatibilidad con la organización en la base de datos (en la página 150).
2. Describa el objeto de organización en ImsManagedObject (en la página 117).

   Asegúrese de configurar los subelementos Table y UniqueIdentifier.
3. Configure la organización de nivel superior (en la página 150).
4. Describa los atributos (en la página 122) que constituyen una organización.
5. Defina los atributos conocidos del objeto de organización (en la página 151).

Configuración de la compatibilidad con la organización en la base de datos

Siga estos pasos:

1. Abrir uno de los siguientes scripts de SQL en un editor:
   - Bases de datos de Microsoft SQL Server:

     ims_mssql_rdb.sql
   - Bases de datos de Oracle:

     ims_oracle_rdb.sql

     Estos archivos se encuentran en la siguiente ubicación:

     admin_tools\directoryTemplates\RelationalDatabase

     admin_tools hace referencia a la ubicación de la instalación de las herramientas administrativas, que se instalan de forma predeterminada en una de las siguientes ubicaciones:

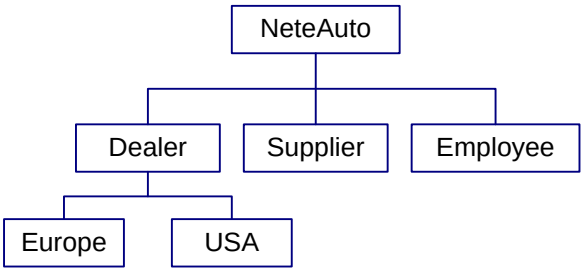
     Windows: C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools

     UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
2. En el script de SQL, busque y sustituya <@primary organization table@> por el nombre de la tabla primaria del objeto de organización. Guarde el script de SQL.
3. Ejecute el script de SQL con respecto a la base de datos.

Especificación de la organización raíz

La organización raíz actúa como la organización de nivel superior o principal en el directorio. Todas las organizaciones están relacionadas con la organización raíz.

En la siguiente ilustración, NeteAuto es la organización raíz. Las demás organizaciones son suborganizaciones de NeteAuto:



Una definición de organización raíz completa se parece al ejemplo siguiente:

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
      <Result name="%ORG_ID%" />
   </RootOrg>
```

Después de definir la información básica para el objeto de organización, incluidas las tablas que constituyen el perfil de la organización y el identificador único del objeto de organización, especifique la organización raíz en el archivo directory.xml:

- En el parámetro de valor del elemento RootOrg, defina la consulta que CA Identity Manager utiliza para recuperar la organización raíz, como en el siguiente ejemplo:

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- En el parámetro de nombre del elemento de resultado, escriba el identificador único de la organización, como en el siguiente ejemplo:

  ```
  <Result name="%ORG_ID%" />
  ```

  Nota: El valor del parámetro de nombre deberá ser el identificador único del objeto de organización.

Atributos conocidos para organizaciones

Los atributos conocidos para los atributos del perfil de una organización se definen como está descrito en la sección de atributos conocidos (en la página 79).

Los atributos conocidos de organización obligatorios y opcionales son los siguientes:

%ORG_DESCR%

Contiene la descripción de una organización.

%ORG_MEMBERSHIP%

(Requerido)

Contiene la organización principal de una organización.

Nota: Consulte Defining the Organizational Hierarchy para obtener más información sobre el atributo %ORG_MEMBERSHIP%.

%ORG_MEMBERSHIP_NAME%

(Requerido)

Contiene el nombre sencillo de la organización principal (en la página 152) de una organización.

%ORG_NAME%

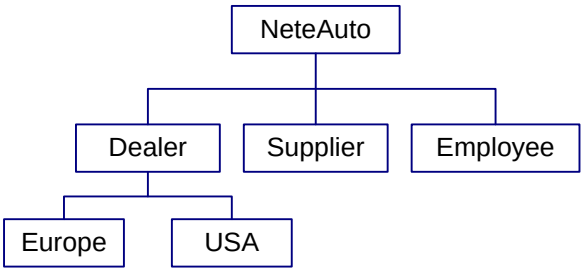
(Requerido)

Contiene el nombre de la organización.

Cómo definir la jerarquía en la organización

En CA Identity Manager, las organizaciones tienen una estructura jerárquica que incluye una organización raíz y suborganizaciones. Las suborganizaciones también pueden tener otras suborganizaciones.

Cada organización, excepto la organización raíz, tiene una organización principal. Por ejemplo, en la siguiente ilustración, Dealer es la organización principal para las organizaciones de Europa y EE. UU.:



El identificador único de la organización principal se almacena en un atributo en el perfil de una organización. Mediante la información de este atributo, CA Identity Manager puede crear la jerarquía de la organización.

Para especificar el atributo que almacena la organización principal, se utilizan los atributos conocidos %ORG_MEMBERSHIP% y %ORG_MEMBERSHIP_NAME% con el atributo físico que almacena el nombre de la organización principal en una descripción del atributo como se muestra a continuación:

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0" />
```

Cómo mejorar el rendimiento de las búsquedas en directorios

Para mejorar el rendimiento de las búsquedas en directorios de usuarios, organizaciones y grupos, se deben llevar a cabo las siguientes tareas:

- Indexar los atributos que los administradores pueden especificar en las consultas de búsqueda.
- Reemplazar el parámetro de tiempo de espera del directorio predeterminado especificando valores para los parámetros de búsqueda de tiempo de espera en el archivo de configuración de un directorio (directory.xml).
- Ajustar el directorio de usuarios. Consulte la documentación de la base de datos que esté utilizando.

Las opciones específicas de base de datos se configuran en el origen de datos ODBC. Para obtener más información, consulte la documentación del origen de datos.

Cómo mejorar el rendimiento de las búsquedas grandes

Cuando CA Identity Manager gestiona un almacén de usuarios muy grande, las búsquedas que devuelven muchos resultados pueden hacer que el sistema se quede sin memoria.

Los dos parámetros de configuración siguientes determinan cómo manejará CA Identity Manager las búsquedas grandes:

- Número máximo de filas

  Especifica el número máximo de resultados que CA Identity Manager puede devolver al buscar un directorio de usuarios. Cuando el número de resultados supera el límite, se muestra un error.

- Tamaño de la página

  Especifica el número de objetos que se pueden devolver en una búsqueda única. Si el número de objetos supera el tamaño de la página, CA Identity Manager realizará varias búsquedas.

  Nota: Si el almacén de usuarios no es compatible con la paginación y se especifica un valor para maxrows, CA Identity Manager utilizará solamente el valor de maxrows para controlar el tamaño de la búsqueda.

Se pueden configurar límites de máximo de filas y de tamaño de la página en los siguientes lugares:

- Almacén de usuarios

  En la mayor parte de los almacenes de usuarios y bases de datos, se pueden configurar límites de búsqueda.

  Nota: Para obtener más información, consulte la documentación del almacén de usuarios o la base de datos que esté utilizando.

- Directorio de CA Identity Manager

  Se puede configurar el elemento DirectorySearch (en la página 59) en el archivo de configuración del directorio (directory.xml) que se utiliza para crear el directorio de CA Identity Manager.

  De forma predeterminada, el valor máximo para las filas y el tamaño de la página es ilimitado para los directorios existentes. Para los directorios nuevos, el valor máximo para las filas es ilimitado y el valor para el tamaño de la página es 2000.

- Definición de objeto gestionado

  Para establecer los límites de máximo de filas y los tamaños de página que se aplican a un tipo de objeto en lugar de a un directorio completo, configure la *definición de objeto gestionado* (en la página 61) en el archivo directory.xml que utilice para crear el directorio de CA Identity Manager.

  El establecimiento de límites para un tipo de objeto gestionado permite hacer ajustes basados en las necesidades empresariales. Por ejemplo, la mayor parte de las compañías tienen más usuarios que grupos. Esas compañías pueden establecer límites para las búsquedas de objetos de usuario solamente.

- Pantallas de búsqueda de tarea

  Se puede controlar el número de resultados de la búsqueda que los usuarios ven en las pantallas de búsqueda y lista en la Consola de usuario. Si el número de resultados supera el número de resultados por página definido para la tarea, los usuarios verán vínculos a páginas de resultados adicionales.

  Esta configuración no afecta al número de resultados que devuelve una búsqueda.

  Nota: Para obtener información acerca de la configuración del tamaño de la página en pantallas de búsqueda y lista, consulte la *Guía de administración*.

Si los límites de máximo de fila y de tamaños de la página están definidos en varios lugares, se aplicará la configuración más específica. Por ejemplo, los parámetros de configuración de los objetos gestionados tienen prioridad sobre los de nivel de directorio.

Capítulo 5: Directorios de CA Identity Manager

Un directorio de CA Identity Manager proporciona información acerca de un directorio de usuarios que gestiona CA Identity Manager. Esta información describe cómo se almacenan objetos, como usuarios, grupos y organizaciones, en el almacén de usuarios y se muestran en CA Identity Manager.

Se pueden crear, consultar, exportar, actualizar y suprimir los directorios de CA Identity Manager en la sección del directorio de CA Identity Manager de la Consola de gestión.

Nota: Si CA Identity Manager utiliza un clúster de servidores de políticas de SiteMinder, se deben detener todos los servidores de políticas excepto uno antes de crear o actualizar los directorios de CA Identity Manager.

Esta sección contiene los siguientes temas:

Requisitos previos para crear un directorio de CA Identity Manager

Antes de crear un directorio de CA Identity Manager, se debe realizar el siguiente procedimiento:

- Detener todos los nodos de CA Identity Manager excepto uno antes de crear o modificar un directorio de CA Identity Manager.

  Nota: Cuando se tiene un clúster de nodos de CA Identity Manager, solamente se puede activar un nodo de CA Identity Manager cuando se hacen cambios en la Consola de gestión.

- Detener todos los servidores de políticas excepto uno antes de crear o actualizar directorios de CA Identity Manager.

  Nota: Cuando se tiene un clúster de servidores de políticas de SiteMinder, solamente se puede activar un servidor de políticas de SiteMinder cuando se hacen cambios en la Consola de gestión.

Cómo crear un directorio

En la Consola de gestión, se crea un directorio de CA Identity Manager, que describe la estructura y el contenido del almacén de usuarios y el directorio de aprovisionamiento, que almacena información necesaria para el servidor de aprovisionamiento. Estos directorios están asociados con el entorno de CA Identity Manager.

Se puede utilizar uno de los métodos siguientes para crear directorios:

- Uso del asistente de configuración de directorios

  Guía a los administradores por todo el proceso de creación de un directorio para el almacén de usuarios. Este método ayuda a reducir posibles errores de configuración.

  Nota: El asistente de configuración de directorios se utiliza para crear directorios nuevos para los almacenes de usuario LDAP solamente. Para crear un directorio para una base de datos relacional o actualizar un directorio existente,se debe importar directamente un archivo directory.xml.

- Uso de un archivo de configuración XML

  Permite a los administradores seleccionar un archivo XML completamente configurado para crear o modificar el almacén de usuarios o el servidor de aprovisionamiento.

  Este método se selecciona si se está creando un directorio para una base de datos relacional o si se está actualizando un directorio existente.

Más información:

Creación de un directorio con un archivo de configuración XML (en la página 171)
Creación de directorios mediante el asistente de configuración de directorios (en la página 159)

Creación de directorios mediante el asistente de configuración de directorios

El asistente de configuración de directorios guía a los administradores durante todo el proceso de creación de directorios para el almacén de sus usuarios; además, ayuda a reducir errores de configuración. Antes de que inicie al asistente, se debe cargar primero la plantilla de configuración del directorio LDAP de CA Identity Manager. Estas plantillas están preconfiguradas con los atributos conocidos y obligatorios. Después de introducir los detalles de conexión del almacén de usuarios LDAP o directorio de aprovisionamiento, puede seleccionar los atributos de LDAP, asignar los atributos conocidos e introducir los metadatos de los atributos. Cuando haya terminado de asignar los atributos, haga clic en Finalizar para crear el directorio.

Inicio del asistente de configuración de directorios

El asistente de configuración de directorios permite a un administrador seleccionar una plantilla de CA Identity Manager y modificar esa plantilla para utilizarla en el entorno.

Siga estos pasos:

1. En la Consola de gestión, haga clic en Directories (Directorios) y seleccione Create from Wizard (Crear a partir del asistente).

   Se le pide que seleccione un archivo de configuración del directorio para configurar el almacén de usuarios.

2. Haga clic en Browse (Examinar) para seleccionar el archivo de configuración con el que se configurará el almacén de usuarios o el servidor de aprovisionamiento de la siguiente ubicación predeterminada. A continuación, haga clic en Next (Siguiente).

   ```
   admin_tools\directoryTemplates\directory\
   ```

   Nota: admin_tools especifica el directorio donde las herramientas administrativas se instalan; el directorio especifica el nombre del distribuidor de LDAP.

   Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

   - Windows: <rutainstalación>\tools
   - UNIX: <rutainstalación2>/tools

3. En la pantalla Detalles de la conexión, especifique la información de conexión para el directorio LDAP o servidor de aprovisionamiento, los parámetros de búsqueda de directorios y la información sobre las conexiones de conmutación por error. A continuación, haga clic en Siguiente.

4. En la pantalla de configuración de objetos gestionados, especifique los objetos para configurarlos y haga clic en Siguiente. Puede elegir entre los siguientes objetos:

   - Configure User Managed Object (Configuración de objeto gestionado del usuario)
   - Configure Group Managed Object (Configuración de objeto gestionado del grupo)
   - Configure Organization Object (Configuración de objeto de organización)
   - Show summary and deploy directory (Mostrar resumen e implementar el directorio)

     Nota: Elija el resumen e implemente el directorio solamente cuando se haya finalizado la configuración del directorio.

   a. En la pantalla Seleccionar atributo, vea y modifique las clases estructurales y auxiliares según sea necesario y haga clic en Siguiente.

   b. En Select Attributes: Mapping Well-Knowns (Seleccionar atributos: asignación de elementos conocidos), asigne los alias conocidos de CA Identity Manager a los atributos de LDAP seleccionados. A continuación, haga clic en Siguiente.

   c. (Opcional) En la pantalla de descripción de atributos de usuario, haga clic en Siguiente. Se puede modificar el nombre para mostrar y la descripción.

   d. (Opcional) En la pantalla de detalles de atributo de usuario, defina los metadatos para cada atributo seleccionado con objeto de gestionarlo. A continuación, haga clic en Siguiente.

      Se mostrará la pantalla de selección de objetos gestionados.

      Para configurar grupos u organizaciones, seleccione el objeto gestionado y haga clic en Siguiente para que se le oriente por las pantallas de atributos de estos objetos.

5. Seleccione Show summary and deploy directory (Mostrar resumen e implementar el directorio) de la lista y haga clic en Siguiente.

   Se abrirá la pantalla Confirmación.

6. Vea los detalles del directorio.

   Si hay errores, hacer clic en el botón Atrás para realizar modificaciones en las pantallas pertinentes. Haga clic en Finalizar para aplicar los cambios.

   CA Identity Manager valida la configuración y crea el directorio. Se le redirige a continuación a la pantalla de listado de directorios, donde se puede ver el nuevo directorio.

Pantalla de selección de plantillas de directorio

Utilice esta pantalla para seleccionar un archivo XML del directorio para LDAP con objeto de configurar un almacén de usuarios o un servidor de aprovisionamiento.

Haga clic en Examinar para seleccionar el archivo de configuración con el que se configurará el almacén de usuarios o el servidor de aprovisionamiento de la siguiente ubicación predeterminada:

```
admin_tools\directoryTemplates\directory\
```

Nota: admin_tools especifica el directorio donde las herramientas administrativas se instalan; el directorio especifica el nombre del distribuidor de LDAP.

Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

- Windows: <rutainstalación>\tools
- UNIX: <rutainstalación2>/tools

Una vez seleccionado el archivo XML del directorio, haga clic Siguiente para continuar a la pantalla Detalles de la conexión.

Pantalla Detalles de la conexión

Utilice esta pantalla para introducir las credenciales de configuración para el almacén de usuarios. Se pueden introducir también los parámetros de búsqueda de directorios, así como agregar conexiones de conmutación por error. Una vez que se introduzca la información de conexión, hacer clic Siguiente para seleccionar los objetos que se gestionarán.

Nota: Los campos que se muestran en esta pantalla dependen del tipo de almacén de usuarios, así como si está utilizando la conexión mediante el asistente de configuración de directorios o importando directamente un archivo XML.

Los siguientes campos están disponibles en esta pantalla:

Nombre

Especifica el nombre del directorio de usuarios al cual se va a conectar.

Descripción

Especifica una descripción del directorio del usuario.

Host

Especifica el nombre de host para el equipo donde se encuentra el almacén de usuarios.

Puerto

Especifica el puerto para el equipo donde se encuentra el almacén de usuarios.

DN de usuario

Especifica el nombre de dominio de usuario para acceder al almacén de usuario de LDAP.

Nombre de JNDI de orígenes de datos de JDBC

Especifica el nombre de un origen de datos de JDBC existente que CA Identity Manager utiliza para conectarse a la base de datos.

Nombre de usuario

Especifica el nombre del usuario para acceder al servidor de aprovisionamiento.

Nota: Solamente para servidores de aprovisionamiento.

Dominio

Especifica el nombre de dominio para acceder al servidor de aprovisionamiento.

Nota: Solamente para servidores de aprovisionamiento.

Contraseña

Especifica la contraseña para acceder al almacén de usuario de LDAP/servidor de aprovisionamiento.

Confirmar contraseña

Confirma la contraseña para acceder al almacén de usuario de LDAP/servidor de aprovisionamiento.

Conexión segura

Al activarse, se obliga a utilizar una conexión de Secure Sockets Layer (SSL) en el directorio de usuarios de LDAP.

Raíz de búsqueda

Especifica la ubicación en un directorio LDAP que sirve del punto de partida para el directorio, normalmente, una organización (o) o una unidad organizativa (ou).

Nota: Solamente para los almacenes de usuario de LDAP.

Search Maximum Rows (Número máximo de filas de búsqueda)

Especifica el número máximo de resultados que CA Identity Manager puede devolver al buscar un directorio de usuarios. Cuando el número de resultados supera el límite, se muestra un error.

Al establecer el número máximo de filas, se puede reemplazar la configuración en el directorio LDAP que limita los resultados de la búsqueda. Al aplicar una configuración que entre en conflicto, el servidor de LDAP utiliza la configuración de menor nivel.

Search Page Size (Tamaño de la página de búsqueda)

Especifica el número de objetos que se pueden devolver en una búsqueda única. Si el número de objetos supera el tamaño de la página, CA Identity Manager realizará varias búsquedas.

Se deben tener en cuenta los siguientes aspectos al especificar el tamaño de la página de búsqueda:

- Para utilizar la opción Search Page Size (Tamaño de la página de búsqueda), el almacén de usuarios que gestiona CA Identity Manager debe ser compatible con la paginación. Algunos tipos de almacén de usuarios pueden requerir configuración adicional para ser compatibles con la paginación. Para obtener más información, consulte la *Guía de configuración*.
- Si el almacén de usuarios no es compatible con la paginación y un valor para el Máximo de Búsqueda Filas se especifica, CA Identity Manager utiliza solamente el valor de Filas Máximas de Búsqueda para controlar tamaño de búsqueda.

Search Timeout (Tiempo de espera de búsqueda)

Especifica el número máximo de segundos que CA Identity Manager busca un directorio antes de finalizar la búsqueda.

Failover Host (Host de conmutación por error)

Especifica el nombre de host del sistema en el que hay un almacén de usuarios redundante o un servidor de aprovisionamiento, en caso de que el sistema primario no esté disponible. Si se muestran varios servidores, CA Identity Manager intentará conectarse a los sistemas en el mismo orden que se proporciona.

Failover Port (Puerto de conmutación por error)

Especifica el puerto del sistema en el que hay un almacén de usuarios redundante o un servidor de aprovisionamiento, en caso de que el sistema primario no esté disponible. Si se muestran varios servidores, CA Identity Manager intentará conectarse a los sistemas en el mismo orden que se proporciona.

Botón Agregar

Haga clic para agregar el nombre de host de conmutación por error adicional y los números de puerto.

Pantalla Configure Managed Objects (Configuración de objetos gestionados)

Utilice esta pantalla para seleccionar un objeto que se vaya a configurar.

La siguiente lista muestra los campos de esta pantalla:

Configure User Managed Object (Configuración de objeto gestionado del usuario)

Describe cómo se almacenan los usuarios en el almacén de usuarios y cómo se representan en CA Identity Manager.

Configure Group Managed Object (Configuración de objeto gestionado del grupo)

Describe cómo se almacenan los grupos en el almacén de usuarios y cómo se representan en CA Identity Manager.

Configure Organization Managed Object (Configuración de objeto gestionado de organización)

Si el almacén de usuarios incluye organizaciones, describa cómo se almacenan y representan las organizaciones en CA Identity Manager.

Show Summary and Deploy Directory (Mostrar resumen e implementar el directorio)

Especifica que todos los objetos gestionados se hayan definido y que desea implementar el directorio. Una vez que se seleccione Show summary and deploy directory (Mostrar resumen e implementar el directorio), haga clic en Siguiente para que se le redirija a una página de resumen.

Botón Guardar

Haga clic para guardar el archivo XML.

Botón Atrás

Haga clic para volver a la pantalla Detalles de la conexión y realizar las modificaciones.

Botón Siguiente

Haga clic para continuar a la pantalla de selección de atributos con objeto de seleccionar el usuario, el grupo o los atributos de la organización para su configuración.

Pantalla Select Attributes (Selección de atributos)

Utilice esta pantalla para cambiar o agregar clases estructurales y auxiliares para objetos de usuario, grupo u organización. Esta pantalla se ha preconfigurado con valores basados en los esquemas de directorio comunes y las recomendaciones para el tipo de directorio que se vaya a utilizar. Un administrador puede cambiar la clase estructural seleccionando una nueva clase en el menú desplegable. Al seleccionar una clase, se actualiza esta con los atributos que pertenecen a la nueva clase estructural.

Una clase auxiliar se puede agregar seleccionando una en el menú desplegable. Al seleccionar una clase, se actualiza esta con los atributos que pertenecen a la nueva clase auxiliar.

La siguiente lista muestra los campos que aparecen en esta pantalla:

Structural Class Name (Nombre de clase estructural)

Especifica la clase estructural del atributo para su configuración.

Botón Cambiar

Haga clic para cambiar la clase estructural.

Auxiliary Class Name (Nombre de clase auxiliar)

Especifica la clase auxiliar del atributo para su configuración.

Botón Agregar

Haga clic para agregar una clase auxiliar que se vaya a configurar.

Clase de objeto

Especifica la clase de objeto del contenedor.

ID

Especifica el ID del contenedor.

Nombre

Especifica el nombre del contenedor.

Attributes Table (Tabla de atributos)

Especifica el nombre físico, la clase de objeto, si el atributo contiene varios valores, así como el tipo de datos de los atributos seleccionados. Los atributos de esta tabla se pueden ordenar por Seleccionado, Clase de objeto, Con varios valores y Tipo de datos.

Botón Atrás

Haga clic para volver a la pantalla Configure Managed Objects (Configuración de objetos gestionados).

Siguiente

Haga clic para continuar a la pantalla Well-Known Mapping (Asignación de elementos conocidos) para asignar los alias conocidos obligatorios y opcionales.

Pantalla Well-Known Mapping (Asignación de elementos conocidos)

Utilice esta pantalla para asignar atributos conocidos de CA Identity Manager a atributos de LDAP seleccionados. Un administrador puede agregar a la lista de atributos conocidos (si se requieren para el código personalizado) escribiendo un atributo conocido nuevo en el campo de texto y haciendo clic en el botón Agregar. La pantalla se actualiza para que pueda continuar agregando tantos atributos conocidos como sea necesario.

La siguiente lista muestra los campos que aparecen en esta pantalla:

Required Well-Knowns (Elementos conocidos obligatorios)

Especifica los atributos conocidos para usuarios, grupos u organizaciones (si procede) que se requieren para que se asignen a atributos de LDAP.

Optional Well-Knowns (Elementos conocidos opcionales)

Especifica los atributos conocidos para usuarios, grupos u organizaciones (si procede) que se pueden asignar de forma opcional.

Nueva Well-Known

Especifica un atributo conocido tal y como se hace referencia en el código personalizado.

Botón Agregar

Haga clic para agregar un atributo conocido nuevo a la tabla Optional Well-Knowns (Elementos conocidos opcionales).

Botón Atrás

Haga clic para volver a la pantalla Select Attributes (Selección de atributos) para seleccionar más atributos. Las asignaciones que se hayan realizado se guardarán y estarán disponibles cuando vuelva a esta pantalla.

Botón Siguiente

Haga clic para continuar a la pantalla Basic Object Attribute Definition (definición de los atributos de objetos básicos) para especificar las definiciones de los atributos básicos.

Más información

Atributos conocidos para un almacén de usuarios de LDAP (en la página 79)
Atributos conocidos de grupos (en la página 83)
Atributos conocidos de usuarios (en la página 80)
Organización de atributos conocidos (en la página 85)

Pantalla Basic Object Attribute Definition (Definición de los atributos de objetos básicos)

Utilice esta pantalla para ver y modificar las definiciones que se definen habitualmente: Nombre para mostrar y Descripción.

La siguiente lista muestra los campos que aparecen en esta pantalla:

Tabla Managed Object (Objeto gestionado)

Especifica el nombre para mostrar, el nombre físico, el nombre conocido y la descripción del objeto gestionado. Utilice el menú desplegable para cambiar la descripción, si procede. Una vez que se hayan realizado los cambios, haga clic en Siguiente para continuar.

Botón Atrás

Haga clic para volver a la pantalla Well-Known Mapping (Asignación de elementos conocidos) para modificar los detalles de las asignaciones.

Botón Siguiente

Haga clic para continuar a la pantalla Basic Object Attribute Definition (definición de los atributos de objetos básicos), donde puede especificar definiciones de atributos adicionales.

Pantalla Detailed Object Attribute Definition (Definición de los atributos de objetos detallados)

Utilice esta pantalla para especificar otras definiciones de atributos. Un administrador puede definir los metadatos de cada atributo seleccionado modificando el nombre para mostrar, gestionando el atributo en las pantallas de la Consola de usuario, el tipo de datos del valor, la longitud máxima y el conjunto de reglas de validación. Una vez que se hayan especificado las definiciones de atributos, haga clic en Siguiente para continuar.

Los campos de esta pantalla se muestran a continuación:

Nombre para mostrar

Especifica el nombre único para el atributo del objeto gestionado. Se trata del nombre que se muestra en la Consola de usuario.

Etiquetas

Especifica las etiquetas de clasificación de datos para el valor de atributo del objeto gestionado. Las etiquetas son opcionales y tienen el valor false de forma predeterminada, excepto para Se puede buscar. Se pueden seleccionar las siguientes etiquetas:

Requerido

Indica que el atributo es obligatorio al crear objetos.

Multiple Values (Varios valores)

Indica que el atributo se muestra con varios valores.

Oculto

Indica que el atributo está oculto.

Sistema

Indica que el atributo es un atributo del sistema y no se agrega a las pantallas de tarea.

Searchable (Se puede buscar)

Indica que el atributo se agrega a los filtros de búsqueda. El valor predeterminado es verdadero.

Sensitive Encrypt (Cifrado de datos confidenciales)

Indica que el atributo es confidencial y se muestra con una serie de asteriscos (*).

Hide in VST (Ocultar en VST)

Indica que el atributo se oculta en la pantalla Detalles del evento para Ver tareas enviadas.

Do not copy (No copiar)

Indica que el atributo se debe ignorar cuando un administrador crea una copia de un objeto.

Previously encrypted (Previamente cifrado)

Indica que el atributo al cual se accede en el almacén de usuarios se ha cifrado previamente y se requiere que se descifre. El valor de texto no cifrado se guarda en el almacén de usuarios cuando se guarda el objeto.

Untagged encrypted (Cifrado sin etiquetar)

Indica que el atributo se ha cifrado previamente en el almacén de usuarios y no contiene un nombre de etiqueta de algoritmo de cifrado al comienzo del texto de cifrado.

Tipo de datos

Especifica el tipo de datos del valor para el atributo del objeto gestionado en la Consola de usuario. Puede elegir uno de la siguiente lista:

- READONLY
- WRITEONCE
- READWRITE

Longitud máxima

Especifica la longitud máxima del valor para el atributo del objeto gestionado.

Predeterminado: 0

Validation Rule Set (Conjunto de reglas de validación)

Especifica los conjuntos de reglas de validación para validar el valor del atributo del objeto gestionado. Puede elegir uno de la siguiente lista:

- User Validation (Validación de usuarios)
- Phone Format (Formato de teléfono)
- International Phone Format (Formato de teléfono internacional)

Botón Atrás

Haga clic en este botón para volver a la pantalla Basic Object Attribute Definition (Definición de los atributos de objetos básicos).

Botón Siguiente

Haga clic en este botón para continuar a la pantalla Configure Managed Objects (Configuración de objetos gestionados). En esta pantalla, se puede seleccionar el siguiente objeto gestionado para su configuración. Una vez configurados los objetos gestionados, seleccione Show summary and deploy directory (Mostrar resumen e implementar el directorio) para ver la información del directorio e implementar el directorio.

Más información

Gestión de atributos confidenciales (en la página 71)

Pantalla Confirmación

Esta pantalla muestra un resumen de los detalles del directorio.

La siguiente lista muestra los campos que aparecen en esta pantalla:

Detalles de la conexión

Especifica los detalles de la conexión para el directorio de usuarios.

User/Group/Organization Details (Detalles de usuario, grupo u organización)

Especifica los cambios que se hayan realizado en directory.xml.

Botón Atrás

Haga clic para modificar algunos detalles en el asistente.

Botón Guardar

Haga clic para guardar sus selecciones.

Botón Finalizar

Haga clic si todos los detalles del directorio son correctos para salir del asistente.

La configuración se valida y el directorio se crea. A continuación, se le redirige a la página de listado de directorios, donde se muestra el nuevo directorio. Para editar o exportar el nuevo directorio, selecciónelo de la lista de directorios.

Creación de un directorio con un archivo de configuración XML

Se puede crear o actualizar un directorio de CA Identity Manager importando un archivo directory.xml completado en la Consola de gestión.

Nota: Si se está creando un directorio con un archivo directory.xml en lugar de con el asistente de configuración de directorios, es necesario asegurarse de que se ha modificado la plantilla de configuración predeterminada. Para obtener más información, consulte la *Guía de configuración*.

Siga estos pasos:

1. Abra la Consola de gestión de escribiendo la siguiente URL en un explorador:

   http://*nombre de host*:*puerto*/iam/immanage

   nombre de host

   Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager.

   puerto

   Define el número de puerto de servidor de aplicaciones.

2. Haga clic en Directorios.

   Se mostrará la ventana de directorios de CA Identity Manager.

3. Haga clic en Create (Crear) o Update from XML (Actualizar de XML).

4. Escriba la ruta y el nombre de archivo del archivo XML de configuración del directorio para crear el directorio de CA Identity Manager o navegue hasta el archivo. Haga clic en Siguiente.

5. Proporcione valores para los campos de esta ventana como se muestra a continuación:

   Nota: Los campos que aparecen en esta ventana dependen del tipo de almacén de usuarios y la información proporcionada en el archivo de configuración del directorio en el paso 4. Si se han proporcionado valores para alguno de estos campos en el archivo de configuración del directorio, CA Identity Manager no solicita que se vuelvan a proporcionar estos valores.

   Nombre

   Determina el nombre del directorio de CA Identity Manager que se está creando.

   Descripción

   (Opcional). Describe el directorio de CA Identity Manager.

   Connection Object Name (Nombre del objeto de conexión)

   Especifica el nombre del directorio de usuarios que describe el directorio de CA Identity Manager. Introduzca *uno* de los detalles siguientes:

   - Si CA Identity Manager no se integra con SiteMinder, especifique cualquier nombre significativo para que el objeto que CA Identity Manager utiliza se conecte al almacén de usuarios.
   - Si CA Identity Manager se integra con SiteMinder y se desea crear un objeto de conexión con el directorio de usuarios en SiteMinder, especifique cualquier nombre significativo. CA Identity Manager crea el objeto de conexión con el directorio de usuarios en SiteMinder con el nombre que se especifique.
   - Si CA Identity Manager se integra con SiteMinder y se desea conectarse a un directorio de usuarios de SiteMinder existente, especifique el nombre del objeto de conexión con el directorio de usuarios de SiteMinder exactamente tal como aparece en la interfaz de usuario del servidor de políticas.

Nombre de JNDI de orígenes de datos de JBDC (para directorios relacionales solamente)

Especifica el nombre de un origen de datos de JDBC existente que CA Identity Manager utiliza para conectarse a la base de datos.

Host (para directorios LDAP solamente)

Especifica el nombre de host o la dirección IP del sistema en el que se ha instalado el servidor de usuarios.

Para los almacenes de usuarios de CA Directory, se debe utilizar el nombre completo de dominio del sistema de host. No se debe utilizar localhost.

Para almacenes de usuarios de Active Directory, se debe especificar el nombre de dominio, no la dirección IP.

Puerto (para directorios LDAP solamente)

Especifica el número de puerto del directorio de usuarios.

Dominio de aprovisionamiento

Dominio de aprovisionamiento que gestiona CA Identity Manager.

Nota: El nombre de dominio de aprovisionamiento distingue entre mayúsculas y minúsculas.

Nombre de usuario/DN de usuario

Especifica el nombre de usuario para una cuenta que puede acceder al almacén de usuarios.

Para almacenes de usuario de aprovisionamiento, la cuenta de usuario que se especifique debe tener el perfil de administrador de dominio o un conjunto equivalente de privilegios para el dominio de aprovisionamiento.

Contraseña

Especifica la contraseña para la cuenta de usuario especificada en el campo Nombre de usuario (para bases de datos relacionales) o DN de usuario (para directorios LDAP).

Confirmar contraseña

Se debe volver a introducir la contraseña escrita en el campo Contraseña para confirmarse.

Conexión segura (para directorios LDAP solamente)

Indica si CA Identity Manager utiliza una conexión segura.

Asegúrese de seleccionar esta opción para almacenes de usuarios de Active Directory.

Haga clic en Siguiente.

6. Revise la configuración del directorio de CA Identity Manager. Haga clic en Finalizar para crear el directorio de CA Identity Manager con la configuración actual o haga clic en Anterior para modificarlo.

   La información de estado se muestra en la ventana de salida de configuración de directorios.

7. Haga clic en Continuar para salir.

   CA Identity Manager crea el directorio.

Activación del acceso al servidor de aprovisionamiento

Se activa el acceso al servidor de aprovisionamiento mediante el vínculo de directorios de la Consola de gestión.

Nota: Un requisito previo a este procedimiento es instalar el directorio de aprovisionamiento en CA Directory. Para obtener más información, consulte la *Guía de instalación*.

Siga estos pasos:

1. Abra la Consola de gestión de escribiendo la siguiente URL en un explorador:

   `http://`*`nombre de host`*`:`*`puerto`*`/iam/immanage`

   nombre de host

   Define el nombre de host completamente cualificado del sistema donde está instalado el servidor de CA Identity Manager.

   puerto

   Define el número de puerto de servidor de aplicaciones.

2. Haga clic en Directorios.

   Se mostrará la ventana de directorios de CA Identity Manager.

3. Haga clic en Create from Wizard (Crear a partir del asistente).

4. Escriba la ruta y el nombre de archivo del archivo XML del directorio para configurar el directorio de aprovisionamiento. Se almacena en directoryTemplates\ProvisioningServer en la carpeta de herramientas administrativas. La ubicación predeterminada de esa carpeta es:

   - Windows: <rutainstalación>\tools
   - UNIX: <rutainstalación2>/tools

   Nota: Se puede utilizar este archivo de configuración del directorio como se instale sin realizar modificaciones.

5. Haga clic en Siguiente.

6. Proporcione valores para los campos de esta ventana como se muestra a continuación:

Nombre

Es un nombre para el directorio de aprovisionamiento asociado al servidor de aprovisionamiento que se está configurando.

- Si CA Identity Manager no se integra con SiteMinder, especifique cualquier nombre significativo para que el objeto que CA Identity Manager utiliza se conecte al directorio de usuarios.
- Si CA Identity Manager se integra con SiteMinder, existen dos opciones:

  Si se desea crear un objeto de conexión con el directorio de usuarios en SiteMinder, se debe especificar cualquier nombre significativo. CA Identity Manager crea este objeto en SiteMinder con el nombre especificado.

  Si desea conectarse a un directorio de usuarios de SiteMinder existente, especifique el nombre del objeto de conexión con el directorio de usuarios de SiteMinder exactamente tal como aparece en la interfaz de usuario del servidor de políticas.

Descripción

(Opcional). Describe el directorio de CA Identity Manager.

Host

Especifica el nombre de host o la dirección IP del sistema en el que se ha instalado el servidor de usuarios.

Puerto

Especifica el número de puerto del directorio de usuarios.

Dominio

Especifica el nombre del dominio de aprovisionamiento que gestiona CA Identity Manager.

Importante: Al crear un directorio de aprovisionamiento mediante la Consola de gestión con los caracteres de idioma extranjero como nombre de dominio, se produce un error en la creación del directorio de aprovisionamiento.

El nombre debe coincidir con el nombre del dominio de aprovisionamiento especificado durante la instalación.

Nota: el nombre de dominio distingue entre mayúsculas y minúsculas.

Nombre de usuario

Especifica un usuario que puede iniciar sesión en el gestor de aprovisionamiento.

El usuario debe tener el perfil de administrador de dominios o un conjunto equivalente de privilegios para el dominio de aprovisionamiento.

Contraseña

Especifica la contraseña para el usuario global especificado en el campo Nombre de usuario.

Confirmar contraseña

Se debe volver a introducir la contraseña escrita en el campo Contraseña para confirmarse.

Conexión segura

Indica si CA Identity Manager utiliza una conexión segura.

Asegúrese de seleccionar esta opción para almacenes de usuarios de Active Directory.

Parámetros de búsqueda de directorios

maxrows define el número máximo de resultados que CA Identity Manager puede devolver al buscar un directorio de usuarios. Este valor anula cualquier límite establecido en el directorio LDAP. Al aplicar una configuración que entre en conflicto, el servidor de LDAP utiliza la configuración de menor nivel.

Nota: El parámetro maxrows no limita el número de resultados que se muestran en la pantalla de tarea de CA Identity Manager. Para configurar la configuración de visualización, modifique la definición de la pantalla de lista en la Consola de usuario de CA Identity Manager. Para obtener instrucciones, consulte la *Guía de diseño de la Consola de usuario*.

timeout determina el número máximo de segundos que CA Identity Manager busca en un directorio antes de terminar la búsqueda.

Conexiones de conmutación por error

El nombre de host y el número de puerto de uno o varios sistemas opcionales que son servidores de aprovisionamiento alternativos. Si se muestran varios servidores, CA Identity Manager intenta conectarse a los sistemas en el orden en el que se clasifican.

Los servidores de aprovisionamiento alternativos se usan si se produce un error con el servidor de aprovisionamiento principal. Cuando el servidor de aprovisionamiento principal esté disponible de nuevo, se continuará utilizando el servidor de aprovisionamiento alternativo. Si se desea volver a usar el servidor de aprovisionamiento, reinicie los servidores de aprovisionamiento alternativos.

7. Haga clic en Siguiente.
8. Seleccione los objetos que se desean gestionar, como Usuarios o Grupos.
9. Después de haber configurado los objetos según sea necesario, haga clic en Show Summary and Deploy Directory (Mostrar resumen e implementar el directorio) y revise la configuración del directorio de aprovisionamiento.
10. Haga clic en una de estas acciones:
    a. Haga clic en Atrás para modificar.
    b. Haga clic en Guardar para guardar la información del directorio si se desea volver más tarde para realizar la implementación.
    c. Haga clic en Finalizar para completar este procedimiento y empezar a configurar un entorno con aprovisionamiento (en la página 197).

Vista de un directorio de CA Identity Manager

Realice el procedimiento siguiente para ver un directorio de CA Identity Manager.

Siga estos pasos:

1. En la Consola de gestión de CA Identity Manager, haga clic en Directories (Directorios).
2. Haga clic en el nombre del directorio de CA Identity Manager que se va a ver. Aparecerá la ventana Directory Properties (Propiedades de directorio), mostrando las propiedades del directorio de CA Identity Manager.

Propiedades del directorio de CA Identity Manager

Las propiedades del directorio de CA Identity Manager son las siguientes:

Nota: Las propiedades mostradas dependen del tipo de base de datos o directorio que se asocia con el directorio de CA Identity Manager.

Nombre

Define el nombre único del directorio de CA Identity Manager.

Descripción

Proporciona una descripción del directorio de CA Identity Manager.

Tipo

Define el tipo de proveedor de directorios.

Connection Object Name (Nombre del objeto de conexión)

Muestra el nombre del directorio de usuarios que describe el directorio de CA Identity Manager.

Si CA Identity Manager se integra con SiteMinder, el nombre del objeto de conexión coincide con el nombre de la conexión con el directorio de usuarios de SiteMinder.

Organización raíz (para almacenes de usuarios que incluyen organizaciones)

Especifica el punto de entrada en el almacén de usuarios.

Para directorios LDAP, la organización raíz se especifica como nombre destacado. Para bases de datos relacionales, se muestra el identificador único para la organización raíz.

JDBC Data Source (Origen de datos de JDBC)

Especifica el nombre de un origen de datos de JDBC que CA Identity Manager utiliza para conectarse a la base de datos.

URL

Proporciona la dirección URL o dirección IP del almacén de usuarios.

Nombre de usuario

Especifica el nombre de usuario para una cuenta que puede acceder al almacén de usuarios.

Search Maximum Rows (Número máximo de filas de búsqueda)

Indica el número máximo de filas que se devuelven como resultado de una búsqueda.

Search Page Size (Tamaño de la página de búsqueda)

Especifica el número de objetos que se pueden devolver en una búsqueda única. Si el número de objetos supera el tamaño de la página, CA Identity Manager realizará varias búsquedas.

Nota: El almacén de usuarios que gestiona CA Identity Manager debe ser compatible con la paginación. Algunos tipos de almacén de usuarios pueden requerir configuración adicional para ser compatibles con la paginación. Para obtener más información, consulte la *Guía de configuración*.

Supports Paging (Compatible con paginación)

Indica que el directorio es compatible con la paginación.

Search Timeout (Tiempo de espera de búsqueda) (para directorios LDAP solamente)

Especifica el número máximo de segundos que CA Identity Manager busca en un almacén de usuarios antes de finalizar la búsqueda.

Provisioning Domain (Dominio de aprovisionamiento) (para directorios de servidor de aprovisionamiento solamente)

Dominio de aprovisionamiento que gestiona CA Identity Manager.

Ventana de propiedades del directorio de CA Identity Manager

La información general acerca de un directorio de CA Identity Manager se presenta en la ventana de propiedades para el directorio que se seleccione. La ventana Directory Properties (Propiedades de directorio) se divide en las secciones siguientes:

Directory Properties (Propiedades de directorio)

Muestra propiedades básicas para el directorio de CA Identity Manager incluido el dominio de aprovisionamiento asociado, si el aprovisionamiento está activado para el entorno.

Managed Objects (Objetos gestionados) (en la página 180)

Proporciona descripciones del tipo de objetos de almacén de usuarios que gestiona CA Identity Manager.

Validation Rule Sets (Conjuntos de reglas de validación) (en la página 185)

Conjuntos de reglas de validación de listas que se aplican al directorio de CA Identity Manager.

Entornos

Muestra los entornos asociados con el directorio de CA Identity Manager. Un directorio se puede asociar con varios entornos de CA Identity Manager.

Para consultar más información acerca de un entorno de CA Identity Manager, haga clic en el nombre del entorno.

Para modificar propiedades en un directorio de CA Identity Manager, se debe importar un archivo de configuración del directorio como se describe en Actualización de un directorio de CA Identity Manager (en la página 187).

Además de ver propiedades, también se pueden realizar las acciones siguientes:

Actualización de una autenticación

Permite a los administradores cambiar el directorio que CA Identity Manager usa para autenticar los administradores de Consola de gestión. Los administradores también pueden agregar administradores adicionales de la Consola de gestión al directorio de autenticación existente.

Nota: Las opciones de actualización de autenticación se aplican solamente cuando la seguridad de CA Identity Manager nativa protege la Consola de gestión. Para obtener información sobre la activación de seguridad nativa o el uso de un método de seguridad diferente, consulte la *Guía de configuración*.

Exportar (en la página 187)

Exporta la definición del directorio como archivo XML. Después de exportar la configuración del directorio, se puede modificar el archivo XML y, a continuación, volver a importarlo para actualizar el directorio. También se puede importar el archivo XML a otro directorio para configurar los mismos parámetros de configuración para ese directorio.

Actualización (en la página 187)

Permite a los administradores que agreguen o cambien las definiciones de objetos gestionados, como los atributos de un objeto, establecer los parámetros de búsqueda y cambiar las propiedades de directorio.

Cómo ver las propiedades y los atributos de objetos gestionados

Un objeto gestionado describe un tipo de entrada en el almacén de usuarios, como un usuario, grupo u organización. Las propiedades y los atributos que se aplican a un objeto gestionado se aplican a todas las entradas de ese tipo. Por ejemplo, un perfil de usuario está formado por todas las propiedades y los atributos del objeto gestionado Usuario.

Para ver los detalles de un objeto gestionado, haga clic en el nombre del objeto para abrir la ventana Managed Object Properties (Propiedades del objeto gestionado).

Managed Object Properties (Propiedades del objeto gestionado)

La ventana Managed Object Properties (Propiedades del objeto gestionado) describe las propiedades y los atributos de un tipo de objeto gestionado.

La información acerca de la ventana Managed Object Properties (Propiedades del objeto gestionado) depende del tipo de almacén de usuarios que se esté gestionando. Las propiedades del objeto gestionado son las siguientes:

Descripción

Proporciona una descripción del objeto gestionado.

Tipo

Indica el tipo de entrada que representa el objeto gestionado. Un tipo de objeto puede ser uno de los siguientes:

- Usuario
- Grupo
- Organización

Clase de objeto (para directorios LDAP solamente)

Especifica las clases de objeto del objeto gestionado. Un objeto gestionado puede tener varias clases de objetos.

Orden de clasificación (para directorios LDAP solamente)

Especifica el atributo que utiliza CA Identity Manager para ordenar los resultados de una búsqueda en la lógica del negocio personalizada. El orden de clasificación no afecta al orden de los resultados de la búsqueda en la Consola de usuario.

Por ejemplo, cuando se especifica el atributo cn para el objeto de usuario, CA Identity Manager ordena los resultados de una búsqueda de usuarios alfabéticamente por el atributo cn.

Primary Table (Tabla primaria) (para bases de datos relacionales solamente)

Especifica la tabla que contiene el identificador único para el objeto gestionado.

Número máximo de filas

Especifica el número máximo de resultados que CA Identity Manager puede devolver al buscar objetos de este tipo. Cuando el número de resultados supera el límite, se muestra un error.

Al establecer el número máximo de filas, se puede reemplazar la configuración en el directorio LDAP que limita los resultados de la búsqueda. Al aplicar una configuración que entre en conflicto, el servidor de LDAP utiliza la configuración de menor nivel.

Tamaño de la página

Especifica el número de objetos que se pueden devolver en una búsqueda única. Si el número de objetos supera el tamaño de la página, CA Identity Manager realizará varias búsquedas.

Nota: El almacén de usuarios que gestiona CA Identity Manager debe ser compatible con la paginación. Algunos tipos de almacén de usuarios pueden requerir configuración adicional para ser compatibles con la paginación. Para obtener más información, consulte la *Guía de configuración*.

Propiedades de contenedor (para directorios LDAP solamente)

En un directorio LDAP, los grupos de *contenedor* contienen objetos de un tipo específico. Cuando se especifica un contenedor, CA Identity Manager maneja solamente las entradas del contenedor. Por ejemplo, cuando se especifica el contenedor ou=Persona, CA Identity Manager maneja usuarios que existen en el contenedor People solamente.

Nota: Los usuarios y los grupos que existen en el directorio LDAP pero no en el contenedor definido pueden aparecer en la Consola de usuario. Puede que se experimenten problemas al gestionar esos usuarios y grupos.

Los contenedores agrupan usuarios y grupos solamente. No se puede especificar un contenedor para organizaciones.

Las propiedades de un contenedor son las siguientes:

objectclass

Especifica la clase de objeto de LDAP del contenedor donde se crean objetos de un tipo específico. Por ejemplo, el valor predeterminado para el contenedor de usuario es "top,organizationalUnit", lo que indica que se crean usuarios en unidades organizativas de LDAP (ou).

ID

Especifica el atributo que se almacena el nombre del contenedor, por ejemplo, ou. El atributo se empareja con el valor de nombre para formar el nombre destacado relativo del contenedor, como en el ejemplo siguiente:

ou=Persona

Nombre

Especifica el nombre del contenedor.

Propiedades de tablas secundarias (para bases de datos relacionales solamente)

Las tablas secundarias contienen atributos adicionales para un objeto gestionado. Por ejemplo, una tabla secundaria llamada tblUserAddress puede contener atributos de calle, ciudad, estado y código postal para el objeto gestionado del usuario.

Para las tablas secundarias se muestran las propiedades siguientes:

Tabla

Especifica el nombre de la tabla.

Referencia

Describe la asignación entre la tabla primaria y la tabla secundaria.

La referencia se muestra mediante el formato siguiente:

primarytable.attribute=secondarytable.attribute

Por ejemplo, tblUsers.id = tblUserAddress.userid indica que el atributo ID de la tabla primaria, tblUsers, se asigna al atributo userid en la tabla tblUserAddress.

Propiedades de atributo en la ventana de propiedades del objeto gestionado

Se muestran las propiedades siguientes para los atributos en la ventana de propiedades del objeto gestionado:

Nombre para mostrar

El nombre sencillo del atributo. Este nombre aparece en la lista de atributos disponibles cuando se diseña una ventana de tarea para una tarea determinada en la Consola de usuario.

Nombre físico

El nombre del atributo en el almacén de usuarios.

Nombre de Well-Known

Los nombres conocidos indican atributos que tienen un significado especial en CA Identity Manager, como el atributo que se utiliza para almacenar contraseñas de usuario.

Propiedades de atributos en las ventanas Attribute Properties (Propiedades de atributo)

Se pueden ver detalles adicionales sobre un atributo haciendo clic en su nombre para abrir la ventana Attribute Properties (Propiedades de atributo).

Las siguientes propiedades de atributo se muestran en la ventana Attribute Properties (Propiedades de atributo):

Descripción

Proporciona una descripción para el atributo.

Nombre físico

Especifica el nombre del atributo en el almacén de usuarios.

Clase de objeto (para atributos de usuario, grupo y organización en directorios LDAP solamente)

La clase auxiliar de LDAP para un atributo de usuario, cuando el atributo no forma parte de la clase de objeto primario que se especifica para el objeto de usuario.

Se puede especificar una clase de objeto auxiliar para los objetos de usuario y grupo solamente.

Nombre de Well-Known

Indica atributos que tienen un significado especial en CA Identity Manager, como el atributo que se utiliza para almacenar contraseñas de usuario.

Requerido

Indica si se requiere un valor para el atributo, como se muestra a continuación:

- True indica que el atributo debe tener un valor.
- False indica que la inclusión de un valor es opcional.

Sólo lectura

Indica el nivel de permisos de un atributo, como se muestra a continuación:

- True indica que no se puede modificar el atributo.
- False indica que el atributo se puede modificar.

Oculto

Indica si un atributo se puede mostrar en una ventana de tarea para una tarea particular.

Los atributos ocultos se utilizan a menudo en esquemas de atributos lógicos.

Nota: Para obtener más información, consulte la *Guía de programación para Java*.

Supports Multiple Values (Compatible con varios valores)

Indica si el atributo puede tener varios valores o no, como se muestra a continuación (por ejemplo, el atributo que se utiliza para almacenar los miembros de un grupo tiene varios valores):

- True indica que el atributo puede ser compatible con varios valores.
- False indica que el atributo puede tener solamente un valor.

Multiple Value Delimiter (Delimitador de varios valores) (para bases de datos relacionales solamente)

El carácter que separa los valores cuando se almacenan varios en una sola columna.

System Attribute (Atributo del sistema)

Indica si solamente CA Identity Manager utiliza el atributo o no, como se muestra a continuación:

- True indica que el atributo es un atributo del sistema. El atributo no está disponible para agregarse a las ventanas de tarea.
- False indica que los usuarios pueden utilizar este atributo. El atributo puede aparecer en las ventanas de tareas.

Tipo de datos

Especifica el tipo de datos del atributo. El valor predeterminado es String.

Longitud máxima

Especifica la longitud máxima que puede tener un valor de atributo. Si se establece como 0, no habrá ningún límite en la longitud del valor.

Validation Rule Set (Conjunto de reglas de validación)

Especifica el nombre de un conjunto de reglas de validación, cuando el atributo está asociado con uno.

Validation Rule Sets (Conjuntos de reglas de validación)

Una regla de validación impone requisitos sobre los datos que un usuario escribe en un campo de ventana de tarea. Los requisitos pueden imponer un formato o tipo de datos o se pueden asegurar de que los datos son válidos en el contexto de otros datos en la ventana de tarea.

Una o varias reglas de validación se agrupan en un conjunto de reglas de validación. Después, se asocia un conjunto de reglas de validación con un atributo de perfil. Por ejemplo, se puede crear un conjunto de reglas de validación que contenga una regla de validación del formato de fecha, que exija un formato de fecha dd-mm-aaaa. A continuación, se puede asociar el conjunto de reglas de validación con el atributo que almacena la fecha de inicio de un empleado.

Nota: Se crean reglas de validación y conjuntos de reglas en el archivo de configuración del directorio o en la Consola de usuario.

La ventana Managed Object Properties (Propiedades del objeto gestionado) muestra una lista de conjuntos de reglas de validación que se aplican al directorio de CA Identity Manager. Para consultar los detalles de un conjunto de reglas de validación, haga clic en el nombre del conjunto de reglas para abrir la ventana Validation Rule Set Properties (Propiedades del conjunto de reglas de validación).

Validation Rule Properties (Propiedades de reglas de validación)

La siguiente información se muestra en la ventana Validation Rule Properties (Propiedades de reglas de validación):

Nombre

Muestra el nombre de la regla de validación.

Descripción

Proporciona una descripción de la regla.

Clase

Proporciona el nombre de la clase de Java que implementa la regla de validación.

Este campo no aparece a menos que la regla de validación esté definida en una clase de Java.

Nombre de archivo

Proporciona el nombre del archivo que contiene la implementación en JavaScript de la regla de validación.

Este campo no aparece a menos que la regla de validación esté definida en un archivo.

Expresión regular

Proporciona la expresión regular que implementa la regla de validación.

Este campo no aparece a menos que la regla de validación esté definida como expresión regular.

Validation Rule Set Properties (Propiedades del conjunto de reglas de validación)

La siguiente información se muestra en la ventana Validation Rule Set Properties (Propiedades del conjunto de reglas de validación):

Nombre

Especifica el nombre del conjunto de reglas de validación.

Descripción

Proporciona una descripción para el conjunto de reglas de validación.

La página Validation Rule Set Properties (Propiedades del conjunto de reglas de validación) también incluye una lista de reglas de validación en el conjunto. Se puede hacer clic en el nombre de la regla de validación para abrir la ventana Validation Rule Properties (Propiedades de reglas de validación).

Cómo actualizar la configuración de un directorio de CA Identity Manager

Para ver los parámetros de configuración actuales de un directorio de CA Identity Manager, se debe exportar la configuración del directorio y guardarla como archivo XML.

Después de exportar la configuración del directorio, se puede modificar y volver a importar el archivo XML para actualizar el directorio. También se puede importar el archivo XML a otro directorio para configurar los mismos parámetros de configuración para ese directorio.

Exportación de un directorio de CA Identity Manager

Se debe realizar el procedimiento siguiente para exportar un directorio de CA Identity Manager.

Siga estos pasos:

1. Haga clic en Directorios.

   Aparecerá la lista de directorios de CA Identity Manager.

2. Haga clic en el nombre del directorio de que se va a exportar.

   Aparecerá la ventana de propiedades del directorio de CA Identity Manager.

3. En la parte inferior de la ventana de propiedades, haga clic en Exportar.
4. Cuando se solicite, guarde el archivo XML.

Actualización de un directorio de CA Identity Manager

El propósito de la actualización de un directorio de CA Identity Manager es lo siguiente:

- Agregar o cambiar las definiciones de objetos gestionados, incluidos los atributos de un objeto.
- Establecer los parámetros de búsqueda.
- Cambiar las propiedades de un directorio.

Nota: CA Identity Manager no suprime definiciones de objeto o atributo.

El archivo de configuración del directorio puede contener solamente los cambios que se desean realizar. No es necesario incluir propiedades o atributos que ya estén definidos.

Nota: Cuando se tiene un clúster de nodos de CA Identity Manager, solamente se puede activar un nodo de CA Identity Manager cuando se hacen cambios en la Consola de gestión. Detener todos los nodos de CA Identity Manager excepto uno antes de crear o modificar un directorio de CA Identity Manager.

Siga estos pasos:

1. Exporte la configuración actual del directorio de CA Identity Manager a un archivo XML.
2. Modifique el archivo XML para que refleje sus cambios.
3. Haga clic en Directorios.

   Aparecerá la lista de directorios de CA Identity Manager.
4. Haga clic en el nombre del directorio de que se va a actualizar.

   Aparecerán las propiedades del directorio de CA Identity Manager.
5. En la parte inferior de la ventana de propiedades, haga clic en Actualizar.
6. Escriba la ruta y el nombre de archivo del archivo XML de configuración del directorio para actualizar el directorio de CA Identity Manager o navegue hasta el archivo. Haga clic en Finalizar.

   La información de estado se muestra en el campo de salida de configuración de directorios.
7. Haga clic en Continuar.

Supresión de un directorio de CA Identity Manager

Antes de suprimir un directorio de CA Identity Manager, se deben suprimir todos los entornos de CA Identity Manager que estén asociados con éste.

Siga estos pasos:

1. En la Consola de gestión, haga clic en Directories (Directorios).

   Aparecerá la lista de directorios de CA Identity Manager.
2. Seleccionar la casilla de verificación a la izquierda del directorio (o directorios) que desee suprimir.
3. Haga clic en Suprimir.

   Aparecerá un mensaje de confirmación.
4. Haga clic en Aceptar para confirmar la eliminación.

Capítulo 6: Entornos de CA Identity Manager

Esta sección contiene los siguientes temas:

Entornos de CA Identity Manager

Un entorno de CA Identity Manager es una vista de un almacén de usuarios. En un entorno de CA Identity Manager, se pueden gestionar usuarios, grupos, organizaciones, tareas y roles. Se pueden también proporcionar cuentas de usuarios en puntos finales gestionados, como cuentas de correo electrónico u otras aplicaciones.

Mediante la Consola de gestión, se pueden realizar las tareas siguientes:

- Cree, modifique o suprima un entorno de CA Identity Manager.
- Exporte e importe un entorno de CA Identity Manager.
- Configuración de parámetros avanzados
- Importación de roles y tareas
- Restablecimiento de la cuenta de gestor del sistema

Requisitos previos para crear un entorno de CA Identity Manager

Antes de comenzar, utilice la hoja de cálculo en la siguiente tabla para recolectar la información que se necesita:

Hoja de cálculo de configuración de entornos de CA Identity Manager	
Información obligatoria	**Valor**
Un nombre del entorno de CA Identity Manager significativo que selecciona. Por ejemplo: MyEntorno.	
Una dirección URL base que CA Identity Manager utiliza para crear la dirección URL de redireccionamiento de la política de contraseñas predeterminada para el entorno. Por ejemplo: http://servidor.suempresa.org	
Un alias que se agrega a la dirección URL para acceder a tareas protegidas en el entorno. Por ejemplo: http://servidor.suempresa.org/iam/im/alias	
Un alias que se agrega a la dirección URL para acceder a tareas públicas, como las tareas de autorregistro y de contraseña olvidada. Por ejemplo: http://servidor.suempresa.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration **Nota:** Cuando el entorno no incluye tareas públicas, no se tendrá que especificar un alias público.	
Si se proporcionara un alias público, el nombre de un usuario existente que tienes las funciones de usuario público. CA Identity Manager utiliza las credenciales del usuario público en su lugar de las credenciales que ha proporcionado el usuario al acceder a las tareas públicas.	
El nombre de CA Identity Manager. (en la página 103)	

Hoja de cálculo de configuración de entornos de CA Identity Manager	
Información obligatoria	**Valor**
El nombre del directorio de aprovisionamiento, cuando el entorno de CA Identity Manager sea compatible con el aprovisionamiento.	
El identificador único de un usuario existente que administra el entorno de CA Identity Manager. Por ejemplo: miadmin.	
El nombre del agente de CA SiteMinder o grupo de agentes que protege el entorno de CA Identity Manager si CA Identity Manager se integra con SiteMinder.	

Creación de un entorno de CA Identity Manager

Los entornos de CA Identity Manager permiten gestionar objetos en un directorio con un conjunto de roles y tareas. Utilice el asistente de entorno de CA Identity Manager para guiarlo por los pasos de creación de un entorno de CA Identity Manager.

Tenga en cuenta los siguientes puntos antes de crear un entorno de CA Identity Manager:

- Suponga que está utilizando un almacén de usuario de LDAP y ha configurado un contenedor de usuarios como ou=Persona en el archivo de configuración del directorio (directory.xml) para su directorio de CA Identity Manager. Verifique que existen los usuarios que seleccione al crear el entorno de CA Identity Manager en ese contenedor. Si se selecciona una cuenta de usuario que no existe en el contenedor de usuarios, se pueden producir errores.
- Cuando se configura un entorno de CA Identity Manager para gestionar un directorio de usuarios de LDAP con una estructura de usuarios plana, el perfil del usuario seleccionado debe incluir la organización del usuario. Para ayudar a garantizar que el perfil de un usuario se ha configurado correctamente, agregue el nombre de la organización del usuario al atributo físico que corresponde al atributo conocido %ORG_MEMBERSHIP% en el archivo directory (en la página 86).xml. Por ejemplo, cuando la descripción de atributo físico se asigna al atributo conocido %ORG_MEMBERSHIP% en el archivo directory.xml y el usuario pertenece a la organización Empleados, el perfil del usuario debe contener el par de atributo/valor description=Empleados.

Siga estos pasos:

1. Si CA Identity Manager utiliza un clúster de servidores de políticas, deténgalos a todos menos a uno.
2. Si tiene un clúster de nodos de CA Identity Manager, detenga a todos los nodos de CA Identity Manager menos a uno.
3. En la Consola de gestión, haga clic en Entornos.
4. Haga clic en Nuevo.

   Se abrirá el asistente de entornos de CA Identity Manager.
5. Indique la siguiente información:

   - **Nombre del entorno**

     Introduzca un nombre único para el entorno.

   - **Descripción**

     Describe el entorno.

   - **Alias protegido**

     Especifica un nombre único, como "empleados". Este alias se agrega a la dirección URL para acceder a las tareas protegidas en el entorno de CA Identity Manager. Por ejemplo, cuando el alias es "empleados", la dirección URL para acceder al entorno de empleados es http://mi*servidor.miempresa.com*/iam/im/empleados.

     Nota: El alias distingue mayúsculas de minúsculas y no puede contener espacios. Se recomienda utilizar letras minúsculas sin puntuación ni espacios cuando al especificar el alias.

   - **Base URL**

     Especifica la dirección URL para CA Identity Manager. La dirección URL requiere un nombre de host; no puede incluir un host local. Además, no incluya el alias; por ejemplo, http://*miservidor.miempresa.com*/iam/im.

     Si se está utilizando un agente Web, asegúrese de se ha cambiado la dirección URL base se cambia para reflejar la dirección URL del agente Web.

     Nota: Si se está utilizando un agente Web para proteger recursos de CA Identity Manager, no especifique un número de puerto en el campo de dirección URL base. Si se está utilizando un agente web y la dirección URL base contiene un número de puerto, los vínculos a las tareas de CA Identity Manager no funcionarán correctamente.

     Para obtener más información sobre la protección de recursos de CA Identity Manager, consulte la *Guía de instalación* correspondiente a su servidor de aplicaciones.

     Haga clic en Siguiente.

6. Seleccione un directorio de CA Identity Manager para asociarlo al entorno que se está creando y, a continuación, haga clic en Siguiente.

7. Cuando el entorno de CA Identity Manager sea compatible con el aprovisionamiento, seleccione el servidor de aprovisionamiento adecuado que se utilizará.

   Nota: No se pide que se seleccione un servidor de aprovisionamiento si se ha seleccionado un directorio de aprovisionamiento como el directorio de CA Identity Manager.

8. Configure la compatibilidad con las tareas públicas. Normalmente, las tareas públicas son tareas de autoservicio, como las tareas de contraseña olvidada o autorregistro. Los usuarios no necesitan iniciar sesión para acceder a las tareas públicas.

   Nota: Para permitir que los usuarios utilicen tareas de autoservicio, configure la compatibilidad con las tareas públicas.

   a. Especifique un nombre único que se agrega a la dirección URL para obtener acceso a las tareas públicas.

      Ejemplo: Utilizaría la siguiente dirección URL para acceder a la tarea de autorregistro predeterminada:

      http://*miservidor.miempresa.com*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration

      En esta dirección URL, el *alias* es el nombre único que se proporciona.

   b. Especifique una de las siguientes cuentas de usuario existentes que funciona como cuenta de usuario pública. CA Identity Manager utiliza esta cuenta para permitir a los usuarios desconocidos acceder a tareas públicas sin tener que proporcionar credenciales.

      - Los usuarios de LDAP introducen el identificador único o nombre destacado de la cuenta de usuario pública. Asegúrese de que este valor se asigne al atributo %USER_ID% conocido (en la página 79). Por ejemplo, si el nombre destacado del usuario es uid=Admin1, ou=Persona, ou=Empleados, ou=NeteAuto, tipo Admin1.
      - Los usuarios de base de datos relacionales escriben el valor que se asigna al atributo conocido %USER_ID% en el archivo de configuración del directorio, o bien el identificador único del usuario.

   Haga clic en Validar para ver el identificador completo del usuario.

9. Seleccione las tareas y los roles que se crearán en este entorno. Se pueden llevar a cabo las siguientes tareas:

   - **Crear roles predeterminados**

     Cree un conjunto de tareas predeterminadas y roles que están inicialmente disponibles en el entorno. Los administradores pueden utilizar estos roles y tareas como plantillas para la creación nuevos roles y tareas en la Consola de usuario.

- **Creación solamente del rol de gestor del sistema**

  Crea solamente el rol de gestor del sistema y las tareas asociadas.

  Se requiere el rol de gestor del sistema para acceder al entorno.

  Un gestor del sistema puede crear nuevos roles y tareas en la Consola de usuario.

- **Importación de roles del archivo**

  Importa un archivo de definición del rol que haya exportado a partir de otro entorno de CA Identity Manager.

  Nota: Para utilizar el entorno de CA Identity Manager, el archivo de definiciones del rol debe incluir como mínimo el rol de gestor del sistema o un rol que incluye tareas similares.

  Seleccione la opción de importar roles en el botón de opción y escriba la ruta y el nombre de archivo del archivo de definiciones del rol o busque el archivo para importar.

10. Seleccione los archivos de definiciones del rol para crear conjuntos de tareas predeterminadas para el entorno y haga clic en Siguiente.

    Los archivos de definiciones del rol son archivos XML que definen un conjunto de tareas y roles que se requieren para que sean compatibles con funciones específicas. Por ejemplo, si desea gestionar puntos finales de Active Directory y UNIX NIS, seleccione esos archivos de definiciones del rol.

    Nota: Este paso es opcional. Si no desea crear tareas predeterminadas adicionales para que sean compatibles con nueva funcionalidad, omita esta pantalla.

11. Defina un usuario para que haga funciones de gestor del sistema para este entorno tal y como se muestra a continuación:

    a. En el campo Gestor del sistema, escriba el valor que se asigne al atributo conocido %USER_ID% en el archivo de configuración del directorio, o bien especifique una de las siguientes cuentas de usuario:

       - Los usuarios de LDAP introducen el identificador único o nombre destacado del usuario. Por ejemplo, si el nombre destacado del usuario es uid=Admin1, ou=Persona, ou=Empleados, ou=NeteAuto, tipo Admin1.
       - Los usuarios de base de datos relacionales escriben el identificador único del usuario.

b. Haga clic en Agregar.

   CA Identity Manager agrega el identificador completo del usuario a la lista de usuarios.

c. Haga clic en Siguiente.

Tenga en cuenta los siguientes puntos al especificar al gestor del sistema:

- El gestor del sistema no debe *ser* el mismo usuario que el administrador del almacén de usuarios.
- Se pueden especificar varios gestores del sistema vario para el entorno. Sin embargo, se puede especificar solamente el gestor del sistema inicial en la Consola de gestión. Para especificar gestores del sistema adicionales, asigne el rol de gestor del sistema a los usuarios adecuados en la Consola de usuario.

12. En el campo Administrador entrante, especifique una cuenta de administrador de CA Identity Manager que pueda ejecutar tareas de administración que se asignen a asignaciones de entrada.

    El usuario debe poder ejecutar todas esas tareas en cualquier usuario. El rol de gestor de sincronización de aprovisionamiento contiene las tareas de aprovisionamiento que se incluyen en las asignaciones de entrada predeterminadas.

13. Introduzca una contraseña para el almacén de claves, la base de datos de claves que cifran y descifran datos.

    Definir esta contraseña es un requisito previo para la definición de claves dinámicas. Se puede modificar la contraseña una vez que se cree el entorno mediante la tarea Claves secretas del sistema.

    Se muestra una página que resume la configuración del entorno.

14. Revise la configuración del entorno. Haga clic en Anterior para modificarla o haga clic en Finalizar para crear el entorno de CA Identity Manager con la configuración actual.

    La pantalla de salida de configuración del entorno muestra el progreso de la creación del entorno.

15. Haga clic en Continuar para salir del asistente de entornos de CA Identity Manager.

16. Inicie el entorno.

    Haga clic en el nombre del entorno y, a continuación, haga clic en Inicio.

17. Si se han detenido servidores de políticas durante el paso 1, reinícielos en este momento.

Cómo acceder a un entorno de CA Identity Manager

Una vez que se haya creado un entorno de CA Identity Manager, podrá acceder a él escribiendo una dirección URL en el navegador.

Nota: Active Javascript en el explorador que utiliza para acceder a la Consola de gestión.

El formato de la dirección URL depende de cómo se haya configurado el entorno y el tipo de tarea a la que desea acceder.

- Para acceder a tareas protegidas desde la Consola de usuario, utilice la siguiente dirección URL:

  `http://hostname/iam/im/alias`

  nombre de host

  Defina el nombre de dominio completo del servidor donde se haya instalado CA Identity Manager; por ejemplo, miservidor.miempresa.com

  alias

  Define el alias del alias de entorno, por ejemplo, "empleados".

  Inicie sesión en el entorno de CA Identity Manager con una cuenta de administrador con privilegios, como la cuenta de gestor del sistema que ha creado para el entorno de CA Identity Manager.

  Nota: Todas las tareas de CA Identity Manager se protegen a menos que configure tareas públicas.

- Para acceder a las tareas públicas, que no requieren que los usuarios proporcionen credenciales, utilicen una dirección URL con el siguiente formato:

  `http://hostname/iam/im/alias/index.jsp?task.tag=tasktag`

  nombre de host

  Defina el nombre completo del servidor donde se ha instalado CA Identity Manager; por ejemplo, miservidor.miempresa.com.

  alias

  Defina el alias para tareas públicas; por ejemplo, "autoservicio".

  task_tag

  Define la etiqueta de la tarea que se invocará.

  Especificará la etiqueta de la tarea se especifica al configurar una tarea en la Consola de usuario.

  Las etiquetas de la tarea para las tareas de autorregistro y restablecimiento de contraseña olvidada predeterminadas son SelfRegistration y ForgottenPasswordReset.

  Nota: Para obtener más información, consulte la *Guía de administración*.

Cómo configurar un entorno para el aprovisionamiento

Se puede configurar un entorno para el aprovisionamiento una vez se haya activado el acceso al servidor de aprovisionamiento (en la página 174).

A continuación, cree un usuario de CA Identity Manager especial, denominado "Administrador entrante", cree una conexión al servidor de aprovisionamiento y configure la sincronización de entrada en gestor de aprovisionamiento.

Nota: Cuando se modifiquen las propiedades de aprovisionamiento para un entorno, asegúrese de reiniciar el servidor de aplicaciones para que los cambios surtan efecto.

Configuración del administrador entrante

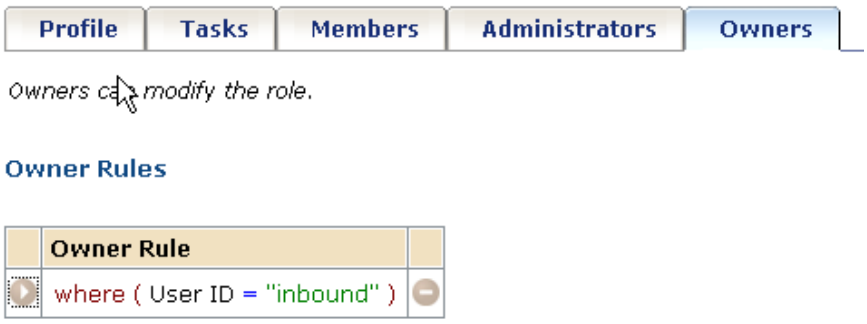
Para que la sincronización de entrada funcione, cree un usuario de CA Identity Manager especial denominado "administrador *entrante*". En versiones anteriores de CA Identity Manager, al administrador entrante se le llamaba "*usuario corporativo*". Ningún usuario inicia sesión en esta cuenta de usuario; en su lugar, CA Identity Manager la utiliza internamente. Sin embargo, cree esta cuenta de usuario y proporcione las tareas adecuadas.

Siga estos pasos:

1. Inicie sesión en el entorno de CA Identity Manager como usuario con el rol de gestor del sistema.
2. Cree un usuario. Podría asignarle el nombre "**usuario de entrada**" como recordatorio de su finalidad.
3. Seleccione Roles de administrador, Modificar roles de administrador y seleccione un rol que contenga las tareas que se utilizan para la sincronización.
   - Aprovisionamiento: Crear usuario
   - Aprovisionamiento: Activar/desactivar usuario
   - Aprovisionamiento: Modificar usuario

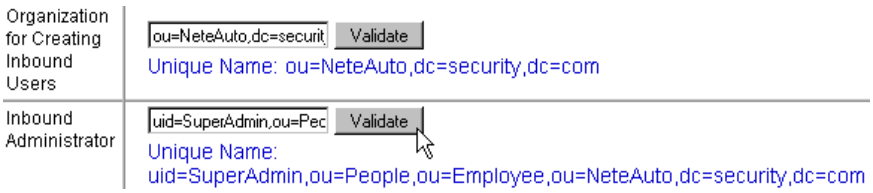
   Nota: Si no se han modificado las tareas de sincronización predeterminadas, utilice el rol Gestor de la sincronización del aprovisionamiento.

4. En la ficha Miembros, agregue una política de miembros que incluya lo siguiente:
   - Una regla de miembros que cumpla el nuevo usuario.
   - Una regla de ámbito que proporciona acceso a todos los usuarios afectados por cambios en el directorio de aprovisionamiento que activan la sincronización de entrada.



5. En la Consola de gestión:
   a. Seleccione el entorno.
   b. Seleccione Configuración avanzada, Aprovisionamiento.
   c. Complete el campo Organización para crear usuarios de entrada si el directorio de CA Identity Manager incluye una organización.

      Esta organización es donde se crean usuarios cuando se produce la sincronización de entrada. Por ejemplo, cuando se agrega un usuario al directorio de aprovisionamiento, CA Identity Manager lo agrega a esta organización.
   d. Complete el campo Administrador de entrada con el ID de usuario del usuario que se ha creado en el paso 2.
   e. Haga clic en Validar para confirmar que el ID de usuario se ha aceptado tal y como se muestra en el siguiente ejemplo, donde el ID de usuario completo aparece bajo el ID de usuario que se ha introducido.



   f. Modificar otros campos en esta pantalla. No se requiere realizar ningún cambio.

      Cuando se modifican campos, asegúrese de comprender cómo interactúan los campos. Para obtener detalles de cada campo, haga clic en el vínculo Ayuda de la pantalla.

Conéctese a un entorno en el servidor de aprovisionamiento

Siga estos pasos:

1. En la Consola de gestión, haga clic en Entornos.

   Se muestra una lista de entornos existentes.
2. Haga clic en el nombre del entorno desea asociar al servidor de aprovisionamiento.
3. Haga clic en el icono de flecha correcto en el campo servidor de aprovisionamiento.

   Se abrirá la pantalla de propiedades de aprovisionamiento.
4. Seleccione el servidor de aprovisionamiento que desee.
5. Haga clic en Guardar en la parte inferior de la página.
6. Configure la sincronización en el gestor de aprovisionamiento (en la página 199).

Configuración de la sincronización en el gestor de aprovisionamiento

La sincronización de entrada mantiene a CA Identity Manager actualizado con los últimos cambios que se producen en el directorio de aprovisionamiento. Entre los cambios se incluyen los que se han realizado mediante el gestor de aprovisionamiento y los cambios en puntos finales en los que el servidor de aprovisionamiento tiene un conector. Cada servidor de aprovisionamiento es compatible con un entorno único. Sin embargo, se pueden configurar entornos de copia de seguridad en sistemas diferentes en un clúster en caso de que el entorno actual no esté disponible.

Siga estos pasos:

1. Seleccione Inicio, CA Identity Manager, Gestor de aprovisionamiento.
2. Haga clic en Sistema, Configuración de CA Identity Manager.
3. Complete el campo Nombre de host con el nombre del sistema en el que se ha instalado el servidor de CA Identity Manager.

4. Complete el campo Puerto con el número de puerto de servidor de aplicaciones.
5. Complete el campo de nombre de entorno con el alias correspondiente al entorno.
6. Seleccione Conexión segura si se desea el protocolo HTTPS se comunique con el servidor de CA Identity Manager en lugar de utilizar HTTP y cifrar las notificaciones individuales.
7. Haga clic en Agregar.
8. Repita los pasos 3-6 para cada una de las versiones de copia de seguridad del entorno.

   Si el servidor de aplicaciones para el entorno actual no está disponible, CA Identity Manager producirá un error de entorno de copia de seguridad. Se pueden volver a clasificar los entornos actuales y de copia de seguridad para establecer la clasificación de error por conmutación.
9. Si este es el primer entorno, rellene los campos Secreto compartido utilizando la contraseña que se ha introducido durante instalación de CA Identity Manager del usuario para componentes incrustados.

   Nota: Estos campos no se aplican si se activa FIPS en esta instalación.
10. Establezca el nivel de registro tal y como se muestra a continuación:
    - No Log (Ningún registro): no se escribe información en el archivo de registro.
    - Error: solamente se registran los mensajes de error.
    - Información: se registran los mensajes de error y de información (valor predeterminado).
    - Advertencia: se registran los mensajes de error, advertencia y de información.
    - Depurar: se registra toda la información.
11. Reinicie el servidor de aplicaciones antes de que inicie sesión en el entorno.

Nota: Para registros de operaciones de sincronización de entrada y determinados problemas que se produzcan durante la sincronización, consulte el siguiente archivo:

PSHOME\logs\etanotify<date>.log

Importación de roles de aprovisionamiento personalizados

Al crear el entorno, tiene la posibilidad de utilizar los roles predeterminados o un archivo de definición del rol personalizado que se cree. Si se importan definiciones del rol personalizadas, importe *también* las definiciones del rol de únicamente aprovisionamiento. Una vez creado el entorno, importe las definiciones del rol del archivo ProvisioningOnly-RoleDefinitions.xml, que se encuentra en una de estas carpetas:

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

La ubicación predeterminada de *admin_tools* es:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Sincronización de cuentas para la tarea Restablecer contraseña del usuario

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

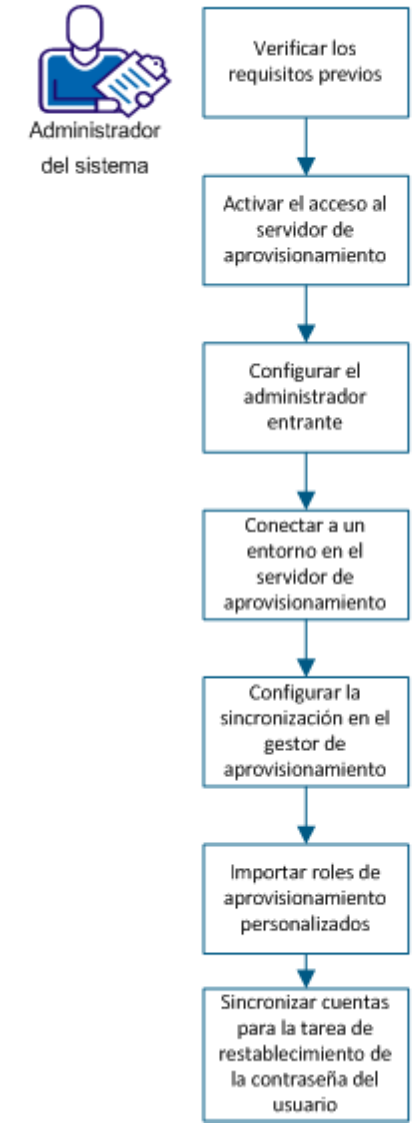
En este archivo, la configuración de sincronización de cuentas predeterminada para la tarea Restablecer contraseña del usuario está definida a Desactivada. (Antes de habilitar el aprovisionamiento, la configuración de sincronización está definida a Al completar la tarea.)

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.

Cómo crear e implementar conectores mediante Connector Xpress

Se puede configurar el aprovisionamiento para que un entorno proporcione cuentas en otros sistemas a los usuarios que gestiona CA Identity Manager. Las cuentas proporcionan a los usuarios el acceso a recursos adicionales, como una cuenta de correo electrónico. Estas cuentas adicionales se proporcionan mediante la asignación de roles de aprovisionamiento, que crea CA Identity Manager.

Cómo configurar un entorno para el aprovisionamiento



Como administrador, realice los pasos siguientes:

1. Verificación de los requisitos previos (en la página 203)
2. Activación del acceso al servidor de aprovisionamiento (en la página 174)

3. Configuración del administrador entrante (en la página 197)
4. Conéctese a un entorno en el servidor de aprovisionamiento (en la página 199)
5. Configuración de la sincronización en el gestor de aprovisionamiento (en la página 199)
6. Importación de roles de aprovisionamiento personalizados (en la página 201)
7. Sincronización de cuentas para la tarea de restablecimiento de la contraseña del usuario (en la página 201)

Verificación de los requisitos previos

Antes de configurar el entorno para el aprovisionamiento, asegúrese de que el directorio de aprovisionamiento se haya instalado en CA Directory. Para obtener más información, consulte la *Guía de instalación*.

Activación del acceso al servidor de aprovisionamiento

Se activa el acceso al servidor de aprovisionamiento mediante el vínculo de directorios de la Consola de gestión.

Nota: Un requisito previo a este procedimiento es instalar el directorio de aprovisionamiento en CA Directory. Para obtener más información, consulte la *Guía de instalación*.

Siga estos pasos:

1. Abra la Consola de gestión de escribiendo la siguiente URL en un explorador:

   `http://`*`nombre de host`*`:`*`puerto`*`/iam/immanage`

   nombre de host

   Define el nombre de host completamente cualificado del sistema donde está instalado el servidor de CA Identity Manager.

   puerto

   Define el número de puerto de servidor de aplicaciones.

2. Haga clic en Directorios.

   Se mostrará la ventana de directorios de CA Identity Manager.

3. Haga clic en Create from Wizard (Crear a partir del asistente).

4. Escriba la ruta y el nombre de archivo del archivo XML del directorio para configurar el directorio de aprovisionamiento. Se almacena en directoryTemplates\ProvisioningServer en la carpeta de herramientas administrativas. La ubicación predeterminada de esa carpeta es:

   - Windows: <rutainstalación>\tools
   - UNIX: <rutainstalación2>/tools

   Nota: Se puede utilizar este archivo de configuración del directorio como se instale sin realizar modificaciones.

5. Haga clic en Siguiente.

6. Proporcione valores para los campos de esta ventana como se muestra a continuación:

   Nombre

   Es un nombre para el directorio de aprovisionamiento asociado al servidor de aprovisionamiento que se está configurando.

   - Si CA Identity Manager no se integra con SiteMinder, especifique cualquier nombre significativo para que el objeto que CA Identity Manager utiliza se conecte al directorio de usuarios.
   - Si CA Identity Manager se integra con SiteMinder, existen dos opciones:

     Si se desea crear un objeto de conexión con el directorio de usuarios en SiteMinder, se debe especificar cualquier nombre significativo. CA Identity Manager crea este objeto en SiteMinder con el nombre especificado.

     Si desea conectarse a un directorio de usuarios de SiteMinder existente, especifique el nombre del objeto de conexión con el directorio de usuarios de SiteMinder exactamente tal como aparece en la interfaz de usuario del servidor de políticas.

   Descripción

   (Opcional). Describe el directorio de CA Identity Manager.

   Host

   Especifica el nombre de host o la dirección IP del sistema en el que se ha instalado el servidor de usuarios.

   Puerto

   Especifica el número de puerto del directorio de usuarios.

Dominio

Especifica el nombre del dominio de aprovisionamiento que gestiona CA Identity Manager.

Importante: Al crear un directorio de aprovisionamiento mediante la Consola de gestión con los caracteres de idioma extranjero como nombre de dominio, se produce un error en la creación del directorio de aprovisionamiento.

El nombre debe coincidir con el nombre del dominio de aprovisionamiento especificado durante la instalación.

Nota: el nombre de dominio distingue entre mayúsculas y minúsculas.

Nombre de usuario

Especifica un usuario que puede iniciar sesión en el gestor de aprovisionamiento.

El usuario debe tener el perfil de administrador de dominios o un conjunto equivalente de privilegios para el dominio de aprovisionamiento.

Contraseña

Especifica la contraseña para el usuario global especificado en el campo Nombre de usuario.

Confirmar contraseña

Se debe volver a introducir la contraseña escrita en el campo Contraseña para confirmarse.

Conexión segura

Indica si CA Identity Manager utiliza una conexión segura.

Asegúrese de seleccionar esta opción para almacenes de usuarios de Active Directory.

Parámetros de búsqueda de directorios

maxrows define el número máximo de resultados que CA Identity Manager puede devolver al buscar un directorio de usuarios. Este valor anula cualquier límite establecido en el directorio LDAP. Al aplicar una configuración que entre en conflicto, el servidor de LDAP utiliza la configuración de menor nivel.

Nota: El parámetro maxrows no limita el número de resultados que se muestran en la pantalla de tarea de CA Identity Manager. Para configurar la configuración de visualización, modifique la definición de la pantalla de lista en la Consola de usuario de CA Identity Manager. Para obtener instrucciones, consulte la *Guía de diseño de la Consola de usuario*.

timeout determina el número máximo de segundos que CA Identity Manager busca en un directorio antes de terminar la búsqueda.

Conexiones de conmutación por error

El nombre de host y el número de puerto de uno o varios sistemas opcionales que son servidores de aprovisionamiento alternativos. Si se muestran varios servidores, CA Identity Manager intenta conectarse a los sistemas en el orden en el que se clasifican.

Los servidores de aprovisionamiento alternativos se usan si se produce un error con el servidor de aprovisionamiento principal. Cuando el servidor de aprovisionamiento principal esté disponible de nuevo, se continuará utilizando el servidor de aprovisionamiento alternativo. Si se desea volver a usar el servidor de aprovisionamiento, reinicie los servidores de aprovisionamiento alternativos.

7. Haga clic en Siguiente.
8. Seleccione los objetos que se desean gestionar, como Usuarios o Grupos.
9. Después de haber configurado los objetos según sea necesario, haga clic en Show Summary and Deploy Directory (Mostrar resumen e implementar el directorio) y revise la configuración del directorio de aprovisionamiento.
10. Haga clic en una de estas acciones:
    a. Haga clic en Atrás para modificar.
    b. Haga clic en Guardar para guardar la información del directorio si se desea volver más tarde para realizar la implementación.
    c. Haga clic en Finalizar para completar este procedimiento y empezar a configurar un entorno con aprovisionamiento (en la página 197).

Configuración del administrador entrante

Para que la sincronización de entrada funcione, cree un usuario de CA Identity Manager especial denominado "administrador *entrante*". En versiones anteriores de CA Identity Manager, al administrador entrante se le llamaba "*usuario corporativo*". Ningún usuario inicia sesión en esta cuenta de usuario; en su lugar, CA Identity Manager la utiliza internamente. Sin embargo, cree esta cuenta de usuario y proporcione las tareas adecuadas.

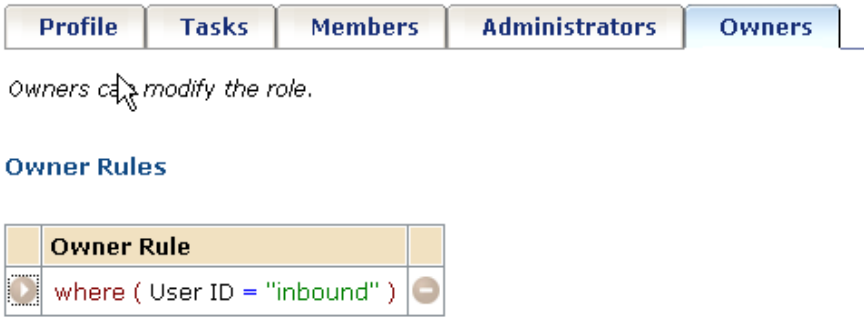
Siga estos pasos:

1. Inicie sesión en el entorno de CA Identity Manager como usuario con el rol de gestor del sistema.
2. Cree un usuario. Podría asignarle el nombre "**usuario de entrada**" como recordatorio de su finalidad.

3. Seleccione Roles de administrador, Modificar roles de administrador y seleccione un rol que contenga las tareas que se utilizan para la sincronización.
   - Aprovisionamiento: Crear usuario
   - Aprovisionamiento: Activar/desactivar usuario
   - Aprovisionamiento: Modificar usuario

   Nota: Si no se han modificado las tareas de sincronización predeterminadas, utilice el rol Gestor de la sincronización del aprovisionamiento.

4. En la ficha Miembros, agregue una política de miembros que incluya lo siguiente:
   - Una regla de miembros que cumpla el nuevo usuario.
   - Una regla de ámbito que proporciona acceso a todos los usuarios afectados por cambios en el directorio de aprovisionamiento que activan la sincronización de entrada.

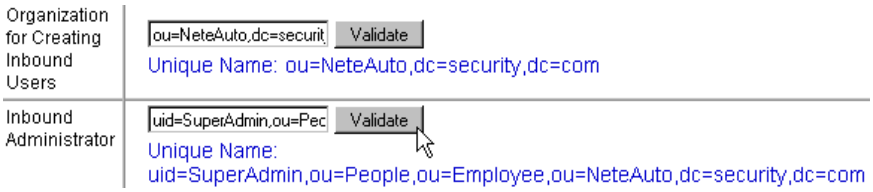


5. En la Consola de gestión:
   a. Seleccione el entorno.
   b. Seleccione Configuración avanzada, Aprovisionamiento.
   c. Complete el campo Organización para crear usuarios de entrada si el directorio de CA Identity Manager incluye una organización.

      Esta organización es donde se crean usuarios cuando se produce la sincronización de entrada. Por ejemplo, cuando se agrega un usuario al directorio de aprovisionamiento, CA Identity Manager lo agrega a esta organización.

d. Complete el campo Administrador de entrada con el ID de usuario del usuario que se ha creado en el paso 2.

e. Haga clic en Validar para confirmar que el ID de usuario se ha aceptado tal y como se muestra en el siguiente ejemplo, donde el ID de usuario completo aparece bajo el ID de usuario que se ha introducido.



f. Modificar otros campos en esta pantalla. No se requiere realizar ningún cambio.

Cuando se modifican campos, asegúrese de comprender cómo interactúan los campos. Para obtener detalles de cada campo, haga clic en el vínculo Ayuda de la pantalla.

Conéctese a un entorno en el servidor de aprovisionamiento

Siga estos pasos:

1. En la Consola de gestión, haga clic en Entornos.

   Se muestra una lista de entornos existentes.

2. Haga clic en el nombre del entorno desea asociar al servidor de aprovisionamiento.
3. Haga clic en el icono de flecha correcto en el campo servidor de aprovisionamiento.

   Se abrirá la pantalla de propiedades de aprovisionamiento.

4. Seleccione el servidor de aprovisionamiento que desee.
5. Haga clic en Guardar en la parte inferior de la página.
6. Configure la sincronización en el gestor de aprovisionamiento (en la página 199).

Configuración de la sincronización en el gestor de aprovisionamiento

La sincronización de entrada mantiene a CA Identity Manager actualizado con los últimos cambios que se producen en el directorio de aprovisionamiento. Entre los cambios se incluyen los que se han realizado mediante el gestor de aprovisionamiento y los cambios en puntos finales en los que el servidor de aprovisionamiento tiene un conector. Cada servidor de aprovisionamiento es compatible con un entorno único. Sin embargo, se pueden configurar entornos de copia de seguridad en sistemas diferentes en un clúster en caso de que el entorno actual no esté disponible.

Siga estos pasos:

1. Seleccione Inicio, CA Identity Manager, Gestor de aprovisionamiento.
2. Haga clic en Sistema, Configuración de CA Identity Manager.
3. Complete el campo Nombre de host con el nombre del sistema en el que se ha instalado el servidor de CA Identity Manager.
4. Complete el campo Puerto con el número de puerto de servidor de aplicaciones.
5. Complete el campo de nombre de entorno con el alias correspondiente al entorno.
6. Seleccione Conexión segura si se desea el protocolo HTTPS se comunique con el servidor de CA Identity Manager en lugar de utilizar HTTP y cifrar las notificaciones individuales.
7. Haga clic en Agregar.
8. Repita los pasos 3-6 para cada una de las versiones de copia de seguridad del entorno.

   Si el servidor de aplicaciones para el entorno actual no está disponible, CA Identity Manager producirá un error de entorno de copia de seguridad. Se pueden volver a clasificar los entornos actuales y de copia de seguridad para establecer la clasificación de error por conmutación.
9. Si este es el primer entorno, rellene los campos Secreto compartido utilizando la contraseña que se ha introducido durante instalación de CA Identity Manager del usuario para componentes incrustados.

   Nota: Estos campos no se aplican si se activa FIPS en esta instalación.
10. Establezca el nivel de registro tal y como se muestra a continuación:
    - No Log (Ningún registro): no se escribe información en el archivo de registro.
    - Error: solamente se registran los mensajes de error.
    - Información: se registran los mensajes de error y de información (valor predeterminado).
    - Advertencia: se registran los mensajes de error, advertencia y de información.
    - Depurar: se registra toda la información.
11. Reinicie el servidor de aplicaciones antes de que inicie sesión en el entorno.

Nota: Para registros de operaciones de sincronización de entrada y determinados problemas que se produzcan durante la sincronización, consulte el siguiente archivo:

PSHOME\logs\etanotify<date>.log

Importación de roles de aprovisionamiento personalizados

Al crear el entorno, tiene la posibilidad de utilizar los roles predeterminados o un archivo de definición del rol personalizado que se cree. Si se importan definiciones del rol personalizadas, importe *también* las definiciones del rol de únicamente aprovisionamiento. Una vez creado el entorno, importe las definiciones del rol del archivo ProvisioningOnly-RoleDefinitions.xml, que se encuentra en una de estas carpetas:

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

La ubicación predeterminada de *admin_tools* es:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Sincronización de cuentas para la tarea Restablecer contraseña del usuario

Para habilitar el aprovisionamiento de un entorno de CA 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.

Gestión de entornos

En esta sección se describe cómo gestionar un entorno.

Modificación de las propiedades del entorno de CA Identity Manager

La pantalla de propiedades del entorno de CA Identity Manager en la Consola de gestión permite realizar las siguientes tareas:

- Consulte la configuración actual del entorno.
- Modifique la descripción, la dirección URL base y los alias protegidos y públicos.

- Importe un entorno de CA Identity Manager existente después de actualizar.

  Nota: Para obtener más información sobre la importación de entornos existentes de CA Identity Manager, consulte la sección de actualización de la *Guía de instalación*.

- Inicie y detenga el entorno.
- Acceda a las páginas para configurar las siguientes tareas:
  - **Configuración avanzada**

    Configura funciones avanzadas, incluidas las funciones que se crean mediante as API de CA Identity Manager.

  - **Role and Task Settings (Configuración de roles y tareas)**

    Importa un archivo de definición del rol que haya exportado a partir de otro entorno de CA Identity Manager.

  - **Gestor del sistema**

    Asigna roles de gestor del sistema.

Siga estos pasos:

1. Si CA Identity Manager utiliza un clúster de servidores de políticas de SiteMinder, deténgalos a todos menos a uno.
2. Si tiene un clúster de nodos de CA Identity Manager, detenga a todos los nodos de CA Identity Manager menos a uno.
3. Haga clic en Entornos.

   La pantalla de entornos de CA Identity Manager se muestra con una lista de entornos de CA Identity Manager.

4. Haga clic en el nombre del entorno de CA Identity Manager que va a modificar.

   Aparece la pantalla de propiedades de CA Identity Manager y se muestran las siguientes propiedades:

   OID

   Define el identificador único del entorno. CA Identity Manager genera este identificador al crear un entorno de CA Identity Manager.

   Utilice el OID al configurar la eliminación de tareas de una base de datos de persistencia de la tarea. Consulte la *Guía de instalación*.

   Nombre

   Especifica el nombre único del entorno de CA Identity Manager.

   Descripción

   Proporciona una descripción del entorno de CA Identity Manager.

Directorio de CA Identity Manager

Especifica el directorio de CA Identity Manager con el que se asocia el entorno.

Enable Verbose Log Output (Activar resultados de registro detallados)

Controla la cantidad de información que registra CA Identity Manager y se muestra en el registro del entorno al importar un entorno. El registro del entorno se muestra en la ventana de estado en la Consola de gestión al importar un entorno u otras definiciones de objeto de un archivo.

Nota: Si se activa esta casilla de verificación, repercutirá en el rendimiento.

En el registro detallado se incluyen mensajes de validación e implementación para cada objeto (tarea, pantalla, rol y política) y sus atributos en el entorno.

Para ver el registro detallado, active esta casilla de verificación y guarde las propiedades del entorno. Al importar roles u otros parámetros de configuración de un archivo, la información adicional se mostrará en el registro.

Servidor de aprovisionamiento

Especifica el directorio de aprovisionamiento que se utiliza como almacén de usuarios de aprovisionamiento.

Haga clic en el botón de flecha correcto para configurar el directorio de aprovisionamiento en la página de propiedades de aprovisionamiento.

Versión

Define el número de versión de CA Identity Manager.

Base URL

Especifique la parte de la dirección URL de CA Identity Manager que no incluye el alias protegido o público para el entorno.

CA Identity Manager utiliza la dirección URL base para la dirección URL de redireccionamiento con objeto de que señale a la tarea de servicios de contraseña en la política de contraseñas predeterminada para el entorno.

Alias protegido

Define el nombre de la dirección URL base para acceder a las tareas protegidas en la Consola de usuario para un entorno de CA Identity Manager.

Alias público

Define el nombre de la dirección URL base para acceder a tareas públicas, como las de autorregistro y contraseña olvidada.

Usuario público

Define la cuenta de usuario que CA Identity Manager utiliza en su lugar de las credenciales que proporciona el usuario para acceder a las tareas públicas.

Job Timeout (Tiempo de espera de trabajos)

Determina la cantidad de tiempo que CA Identity Manager espera después de que una tarea se envíe antes de mostrarse un mensaje de estado.

Este valor se establece en la página de Consola de usuario en Configuración avanzada.

Estado

Detiene o reinicia el entorno de CA Identity Manager.

Migre los datos de persistencia de la tarea desde CA Identity Manager 8.1

Migre datos desde una base de datos de persistencia de la tarea de CA Identity Manager 8.1 a la de la tarea de CA Identity Manager 12.6.4.

Para obtener más información, consulte la *Guía de instalación*.

Nota: La opción de migrar datos de persistencia de la tarea del botón de CA Identity Manager 8.1 solamente se pueden ver en entornos que se han creado en versiones anteriores de CA Identity Manager y que se han migrado a CA Identity Manager 12.6.4.

5. Modifique la descripción, la dirección URL base o el alias protegido o público, según sea necesario.
6. Si se han modificado propiedades del entorno, reinicie el entorno de CA Identity Manager.
7. Si se han detenido servidores de políticas durante el paso 1, reinícielos en este momento.

Configuración del entorno

La información específica de entorno se almacena en tres archivos de configuración del entorno:

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

Nota: *El alias* hace referencia al alias del entorno. Especifique el alias al crear el entorno.

Genera un archivo ZIP que contiene estos archivos, que reflejan la configuración actual, al exportar la configuración del entorno.

Una vez que se haya exportado la configuración del entorno, importe la configuración para llevar a cabo una de las siguientes tareas:

- Gestione varios entornos con una configuración similar. En este caso, cree un entorno con la configuración que necesita, importe dicha configuración a otros entorno y, a continuación, personalícela en cada entorno, según sea necesario.
- Migre un entorno desde un sistema de desarrollo a un sistema de producción.
- Actualice un entorno existente después de actualizar a una versión nueva de CA Identity Manager.

Exportación de entornos de CA Identity Manager

Para implementar un entorno de CA Identity Manager en un sistema de producción, exporte el entorno desde un sistema provisional o de desarrollo, e importe ese entorno en el sistema de producción.

Nota: Cuando se importa un entorno previamente exportado, CA Identity Manager muestra un registro en una ventana de estado en la Consola de gestión. Para ver la información de validación e implementación para cada uno de los objetos gestionados y sus atributos en este registro, seleccione Enable Verbose Log Output (Activar resultados de registro detallados) en la página de propiedades del entorno *antes de* exportar el entorno. Tenga en cuenta que si se selecciona el campo Enable Verbose Log Output (Activar resultados de registro detallados), se pueden provocar problemas de rendimiento importantes durante la importación.

Siga estos pasos:

1. Haga clic en Environments (Entornos) en la Consola de gestión.

   La pantalla de entornos de CA Identity Manager se muestra con una lista de entornos de CA Identity Manager.

2. Seleccione el entorno que desea exportar.
3. Haga clic en el botón Exportar.

   Se mostrará la pantalla de descarga de archivos.

4. Guarde el archivo ZIP en una ubicación que sea accesible desde el sistema de producción.
5. Haga clic en Finalizar.

La información del entorno se exporta a un archivo ZIP que se puede importar en otro entorno.

Importación de entornos de CA Identity Manager

Se puede importar la configuración del entorno de CA Identity Manager para llevar a cabo una de las tareas siguientes:

- Gestione varios entornos con una configuración similar. En este caso, cree un entorno con la configuración que necesita, importe dicha configuración a otros entorno y, a continuación, personalícela en cada entorno, según sea necesario.
- Migre un entorno desde un sistema de desarrollo a un sistema de producción.
- Actualice un entorno existente después de actualizar a una versión nueva de CA Identity Manager.

Siga estos pasos:

1. Haga clic en Environments (Entornos) en la Consola de gestión.

   La pantalla de entornos de CA Identity Manager se muestra con una lista de entornos de CA Identity Manager.

2. Haga clic en el botón Import (Importar).

   Se abrirá la pantalla de importación de entornos.

3. Busque el archivo ZIP que se requiere para importar un entorno.
4. Haga clic en Finalizar.

El entorno se importa en CA Identity Manager.

Reinicio de un entorno de CA Identity Manager.

Siga estos pasos:

1. Haga clic en Environments (Entornos) en la Consola de gestión.

   La pantalla de entornos de CA Identity Manager se muestra con una lista de entornos de CA Identity Manager.

2. Haga clic en el nombre del entorno de CA Identity Manager que se va a iniciar.

   Se mostrará la pantalla de propiedades del entorno de CA Identity Manager.

3. Seleccione una de las siguientes opciones:

   Restart Environment (Reiniciar entorno)

   Detiene e inicia un entorno.

   Detener

   Detiene un entorno que se esté ejecutando actualmente.

   Iniciar

   Inicia un entorno que no se esté ejecutando actualmente.

Supresión de entornos de CA Identity Manager

Utilice este procedimiento para eliminar un entorno de CA Identity Manager.

Nota: Si CA Identity Manager se integra con SiteMinder para la autenticación avanzada, CA Identity Manager también suprime el dominio de la política de SiteMinder que protege el entorno y los esquemas de autenticación predeterminados que se crean para el entorno.

Siga estos pasos:

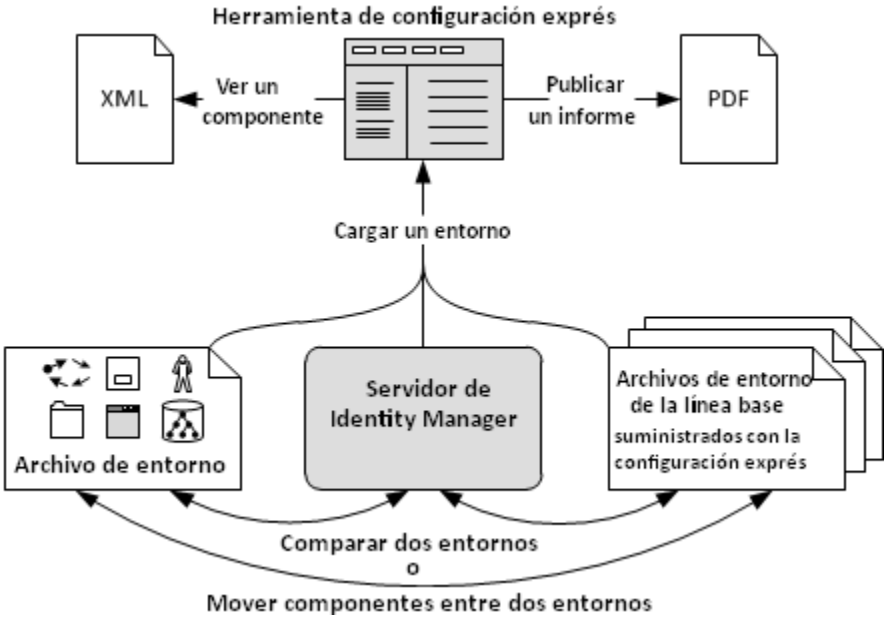
1. En la pantalla Entornos, active la casilla de verificación para suprimir entornos de CA Identity Manager.
2. Haga clic en Suprimir.

   CA Identity Manager muestra un mensaje de confirmación.
3. Haga clic en Aceptar para confirmar la eliminación.

Gestión de la configuración

Config Xpress es una herramienta que se incluye con CA Identity Manager. Se puede utilizar esta herramienta para analizar y trabajar con las configuraciones de los entornos de CA Identity Manager.

Y lo más importante, la herramienta permite mover componentes entre entornos. Config Xpress detecta automáticamente algunos otros componentes obligatorios y solicita que también se muevan. Con esta ayuda se puede guardar el trabajo y reducir el riesgo de que existan problemas.



Siga estos pasos:

1. Configuración de Config Xpress (en la página 218).
2. Antes de poder utilizar la herramienta, cargue un entorno de CA Identity Manager (en la página 219) en Config Xpress para el análisis.
3. Utilice Config Xpress para llevar a cabo estas tareas con el entorno cargado:
   - Mueva componentes entre entornos (en la página 221).
   - Publique un informe en formato PDF de los componentes del sistema (en la página 222).
   - Muestre la configuración de XML para un componente particular (en la página 223).

Configuración de Config Xpress

Los archivos de instalación para Config Xpress se incluyen en la unidad de instalación; sin embargo, la herramienta no se instala.

Config Xpress tiene los siguientes requisitos de software:

- CA Identity Manager r12.0 y posterior
- Sistema operativo Windows
- Tiempo de ejecución de Adobe Air
- Lector de PDF para ver informes

Siga estos pasos:

1. Descargue el tiempo de ejecución de Adobe Air en http://get.adobe.com/air y, a continuación, instálelo.
2. Asegúrese de que se hayan instalado las herramientas de administración.
3. Busque el archivo de instalación de Config Xpress en la siguiente ubicación:

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

4. Ejecute Config Xpress.air para instalar Config Xpress.
5. Cuando se complete la instalación, Config Xpress se iniciará.

Carga de entornos en Config Xpress

Para poder utilizar Config Xpress, cargue uno o más entornos en la herramienta. Esta tarea permite trabajar con el entorno en Config Xpress.

Se puede cargar un entorno en Config Xpress directamente desde un servidor de CA Identity Manager activo, o bien se puede cargar desde un archivo de entorno. Si se utiliza uno de los archivos de entorno de línea de referencia que se instalan con Config Xpress, se puede comparar el entorno con la configuración lista para utilizar.

El proceso de carga de entornos puede tardar unos minutos.

Siga estos pasos:

1. Abra Config Xpress.
2. Para cargar un entorno **activo** directamente desde un servidor de CA Identity Manager:
   a. Haga clic en la ficha Servidor (Red).
   b. Introduzca el nombre y puerto del servidor de CA Identity Manager. Por ejemplo:

      `nombreservidor.ca.com:8080`

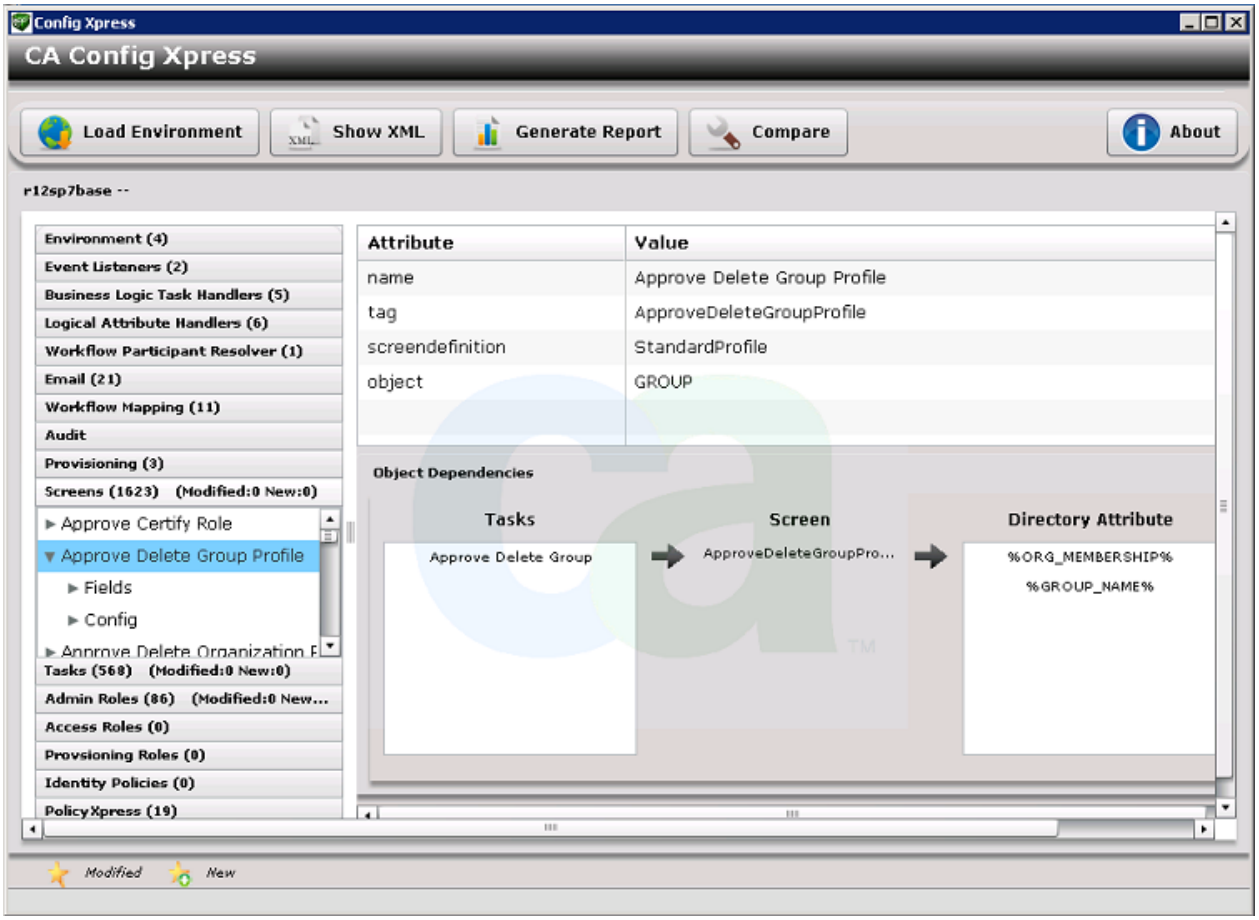
   c. Seleccione Utilizar HTTPS si el servidor se ha configurado para permitir HTTPS solamente.
   d. Seleccione 12.5 SP7 si la versión del servidor es más reciente que r12.5 SP6.
   e. Haga clic en Conectar.
   f. Seleccione un entorno de la lista *Choose Environment to load* (Seleccionar entorno para cargar) y, a continuación, haga clic en Cargar.
3. Para cargar un **archivo de entorno** que se ha exportado del entorno de CA Identity Manager:
   a. Exporte un entorno de CA Identity Manager.
   b. En Config Xpress, haga clic en la ficha Sistema de archivos.
   c. Seleccione la versión y, a continuación, explore el archivo de entorno y haga clic en Entorno.
4. Para cargar un **archivo de entorno de línea de referencia** que se ha instalado con Config Xpress:
   a. Haga clic en la ficha de versiones de base.
   b. Seleccione la versión que se requiere y, a continuación, haga clic en Seleccionar.

Config Xpress analiza el entorno y, a continuación, se muestran los detalles del entorno.

Ahora se pueden publicar todos los entornos (o algunos) en PDF (en la página 222) o XML (en la página 223). Si se carga un segundo entorno, se pueden comparar estos entornos y mover componentes (en la página 221) entre ellos.

Ejemplo: Config Xpress después de que se haya cargado un archivo de configuración de línea de referencia.

Esta captura de pantalla muestra cómo se visualizan en Config Xpress los objetos dependientes:



Cómo mover un componente de un entorno a otro

Sin Config Xpress, la tarea de mover componentes entre áreas provisionales resulta compleja y es probable que se produzcan errores.

Cuando se utiliza Config Xpress para mover componentes, la herramienta también mueve todos los objetos obligatorios. Por ejemplo, si se mueve una tarea que requiere una pantalla, Config Xpress pregunta si desea seleccionar también los componentes. Config Xpress comprende que la tarea utiliza esta pantalla y que se debe mover también al entorno de destino.

Si desea mover un componente a un entorno activo, Config Xpress lo cargará inmediatamente. Si desea mover el componente a un archivo de entorno, guarde el componente como archivo XML y, a continuación, importe ese archivo en el entorno.

Siga estos pasos:

1. Cargue el entorno que contiene el componente que desea mover.
2. Compare este entorno con otro:
   a. Haga clic en Comparar.
   b. Cargue el entorno de destino.

      Config Xpress muestra una lista de las diferencias entre los dos entornos.
3. En la lista de diferencias, busque el componente que desee mover. Puede hacer clic en la columna Nombre para ordenar la lista.
4. En cada componente, lleve a cabo los siguientes pasos:
   a. Seleccionar el elemento en la columna Acción.

      Config Xpress analizará el componente, que puede llevar unos minutos.
   b. Si el componente tiene componentes que dependen de este, se mostrará el cuadro para agregar pantallas dependientes modificadas. Haga clic en Sí o No para continuar.

   Cuando se hayan seleccionado todos los componentes que desea mover, ya se podrán mover los componentes actualizados.
5. Si se están moviendo los componentes a un servidor activo, haga clic en Upload To (Cargar en).

   Los componentes se mueven de inmediato.
6. Si se están moviendo los componentes a un archivo de entorno:
   a. Haga clic en Save.
   b. Introduzca un nombre de archivo y, a continuación, vuelva a hacer clic en Guardar.

Config Xpress guarda todos los componentes que se hayan seleccionado en un archivo XML. Ahora se puede importar este archivo XML en el entorno de destino real.

Publicación de informes en formato PDF

Config Xpress puede generar un informe que documenta el estado actual de un entorno de CA Identity Manager. Se puede utilizar este informe para tomar una instantánea de un entorno de producción. Cuando se genera el informe, decida si incluir la configuración total, o bien solamente los cambios desde la instalación.

Este informe es útil para futuras referencias o como parte de un plan de recuperación de sistemas.

Siga estos pasos:

1. Cargue un entorno en Config Xpress.
2. Haga clic en Generar informe.

   En el cuadro de diálogo de generación de informes en formato PDF, se puede cambiar el tamaño de la fuente y se puede introducir texto para el título o las portadas. Decida también si incluir todos los elementos de configuración, o bien solamente los elementos nuevos o modificados.

   Importante: Si no se hace clic en el cuadro *Only include details of new or modified tasks, screens, roles (Solamente incluir detalles tareas, pantallas y roles nuevos o modificados),* el informe incluirá el entorno completo. El archivo en formato PDF tendrá unas 2000 páginas y más de 40 MB.
3. Haga clic en Aceptar.
4. Introduzca el nombre de un archivo y, a continuación, guarde el informe. El proceso de guardar el archivo puede durar varios minutos; mucho más tiempo si ha decidido publicar el entorno completo.

   El informe se abre en el lector de PDF.

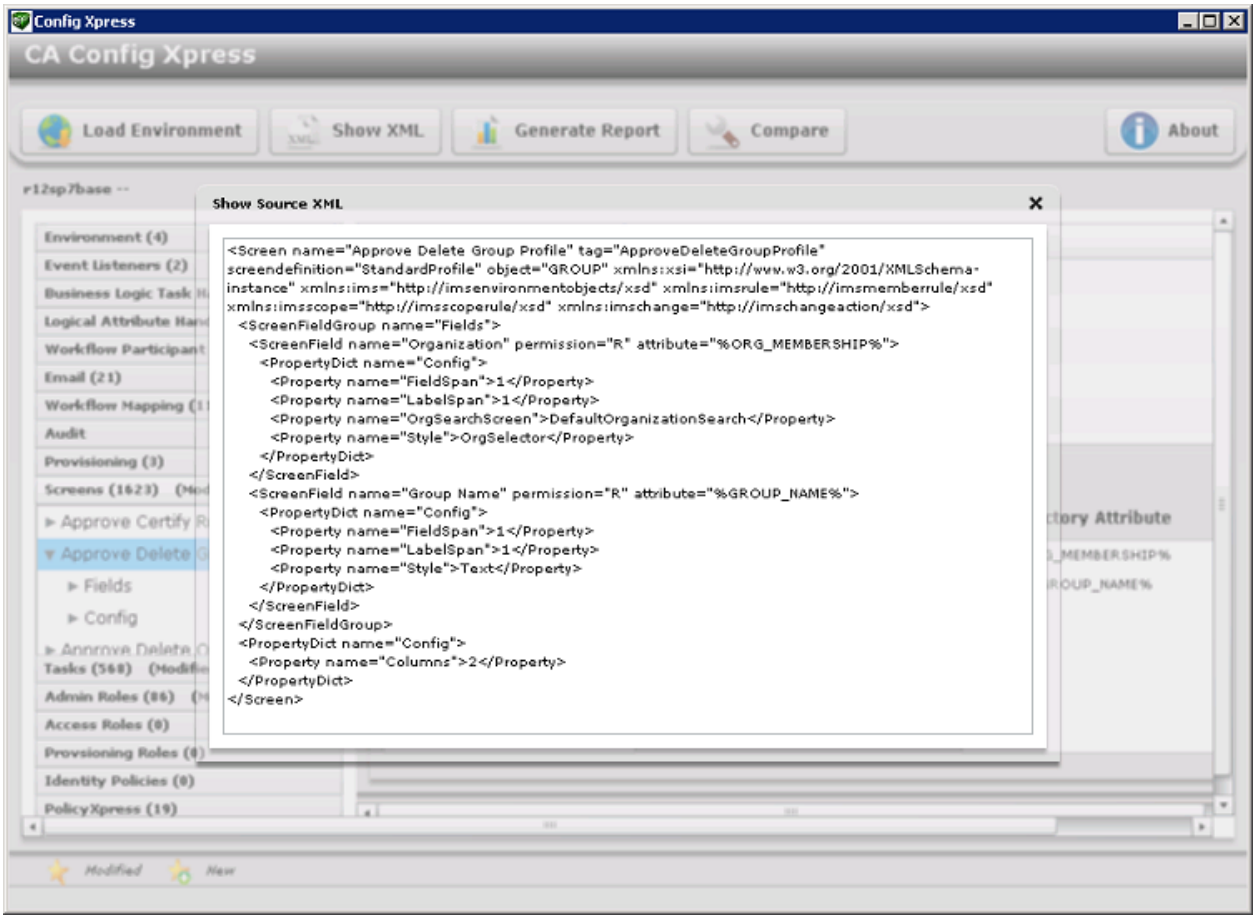
Visualización de la configuración de XML

Config Xpress puede mostrar la configuración de XML para un componente concreto. Se puede estudiar este archivo XML como ayuda para comprender un sistema.

Siga estos pasos:

1. Cargue un entorno en Config Xpress.
2. Haga clic en un componente en la pantalla Config Xpress.
3. Haga clic en Mostrar XML.

   Se mostrará la configuración de XML:



Optimización de la evaluación de reglas de la política

Las reglas de la política, que identifican de forma dinámica un conjunto de usuarios, se utilizan en la evaluación de políticas de miembros del rol, administradores y propietarios, así como políticas de identidad. La evaluación de estas reglas puede tardar un tiempo significativo en llevar a cabo las implementaciones de CA Identity Manager de gran tamaño.

Nota: Para obtener más información sobre las políticas de miembros, administradores, propietarios y de identidad, consulte la *Guía de administración*.

Para reducir el tiempo de evaluación de las reglas que incluyan atributos de usuario, se puede activar la opción de evaluación en memoria. Cuando se activa la opción de evaluación en memoria, CA Identity Manager recupera información del almacén de usuarios acerca de un usuario que se tiene que evaluar y almacena una representación de ese usuario en memoria. CA Identity Manager utiliza la representación en memoria para comparar los valores del atributo con las reglas de la política. Esto limita el número de llamadas que CA Identity Manager hace directamente al almacén de usuarios.

Activa la opción de evaluación en memoria para un entorno en la Consola de gestión.

Siga estos pasos:

1. Abra la Consola de gestión.
2. Seleccione Environments (Entornos), *Environment Name (Nombre del entorno*), Advanced Settings (Configuración avanzada), Miscellaneous (Varios).

   Se abrirá la página de propiedades definidas por el usuario.
3. Introduzca el siguiente texto en el campo Propiedad:

   UseInMemoryEvaluation
4. Introduzca *uno de* los siguientes números en el campo Valor:

   0

   La evaluación en memoria se desactiva.

   1

   La evaluación en memoria se activa. Cuando esta opción se especifica, la comparación de atributos distingue mayúsculas de minúsculas.

   3

   La evaluación en memoria se activa. Cuando esta opción se especifica, la comparación de atributos no distingue mayúsculas de minúsculas.
5. Haga clic en Agregar.

   CA Identity Manager agrega la nueva propiedad a la lista de propiedades existentes para el entorno.
6. Haga clic en Save.

Role and Task Settings (Configuración de roles y tareas)

Desde la pantalla Role and Task Settings (Configuración de roles y tareas) en la Consola de gestión, se puede importar o exportar configuración de pantallas, fichas, roles y tarea en un archivo XML denominado "archivo de definiciones del rol". CA Identity Manager proporciona archivos de definiciones del rol predeterminados que crear pantallas, fichas, roles y tareas de un conjunto de funcionalidad. Por ejemplo, hay un archivo de definiciones del rol que es compatible con el aprovisionamiento inteligente y otros archivos que son compatibles con pantallas de gestión de puntos finales.

Además, se puede utilizar un archivo de definiciones del rol para aplicar la configuración de un entorno a varios. Lleve a cabo las siguientes tareas:

- Configure los parámetros de pantallas, fichas, tareas y roles en un entorno.
- Exporte esta configuración en un archivo XML.
- Importe el archivo XML al entorno que se requiere.

Exportación de la configuración de roles y tareas

Realice el siguiente procedimiento para la configuración de roles y tareas.

Siga estos pasos:

1. En la Consola de gestión, haga clic en Entornos.

   Aparecerá una lista de entornos de CA Identity Manager.

2. Haga clic en el nombre del entorno de CA Identity Manager adecuado.

   Aparecerá la pantalla Properties (Propiedades) de ese entorno.

3. Haga clic en Role and Task Settings (Configuración de roles y tareas) y haga clic en Exportar.

4. Haga clic en Abrir para ver el archivo en una ventana del explorador o Guardar para guardar la configuración en un archivo XML.

Importación de la configuración de roles y tareas

La configuración de roles y tareas se definen en archivos XML denominados "archivos de definiciones del rol". Se pueden importar archivos de definiciones del rol predeterminados para que sean compatibles con conjuntos específicos de funcionalidad de CA Identity Manager (por ejemplo, Aprovisionamiento Inteligente) o archivos de definiciones del rol de importación de un entorno a otro.

Nota: Se pueden importar también definiciones del rol para conectores personalizados que se crean mediante Connector Xpress. Cree estos archivos de definiciones del rol con el generador de definiciones del rol. Para obtener más información, consulte la *Guía de Connector Xpress*.

Realice el siguiente procedimiento para importar la configuración de roles y tareas.

Siga estos pasos:

1. En la Consola de gestión, haga clic en Entornos.

   Aparecerá una lista de entornos de CA Identity Manager.

2. Haga clic en el nombre del entorno de CA Identity Manager donde desea importar la configuración de roles y tareas.

   Aparecerá la pantalla Properties (Propiedades) de ese entorno.

3. Haga clic en Role and Task Settings (Configuración de roles y tareas) y haga clic en Import (Importar).

4. Complete una de las siguientes acciones:

   - Seleccione uno o más archivos de definiciones del rol para crear tareas y roles predeterminados para el entorno.

     Para seleccionar todos los archivos de definiciones del rol disponibles, haga clic en la opción de seleccionar o deseleccionar todo.

   - Escriba la ruta y el nombre de archivo para el archivo de definiciones del rol con objeto de buscar el archivo o exportarlo. A continuación, haga clic en Finalizar.

5. Haga clic en Finalizar.

   El estado se mostrará en la ventana Role Configuration Output (Salida de configuración de rol).

6. Haga clic en Continuar para salir.

Cómo crear roles y tareas para puntos finales dinámicos

Mediante Connector Xpress, se pueden configurar conectores dinámicos para permitir el aprovisionamiento y la gestión de bases de datos SQL y directorios LDAP. Para cada conector dinámico, se puede utilizar el generador de definiciones del rol para crear definiciones de tareas y pantallas para pantallas de gestión de cuentas que se muestran en la Consola de usuario.

Después de que se ejecute el generador de definiciones del rol, importe el archivo (en la página 226) de definiciones del rol que se ha generado en la Consola de gestión.

Nota: Para obtener más información sobre el generador de definiciones del rol, consulte la *Guía de Connector Xpress*.

Modificación de la cuenta de gestor del sistema

Un gestor del sistema es responsable de configurar y mantener un entorno de CA Identity Manager. Normalmente, entre las tareas de un gestor del sistema se incluyen:

- Creación y gestión del entorno inicial
- Creación y modificación de roles de administrador
- Creación y modificación de otras cuentas de administrador

Cree una cuenta de gestor del sistema al crear un entorno de CA Identity Manager. Si esta cuenta está bloqueada (por ejemplo, si el gestor del sistema olvida la contraseña) puede volver a crear la cuenta utilizando el asistente de gestor del sistema.

El asistente de gestor del sistema ofrece orientación por los pasos para asignar un rol de gestión de sistema a un usuario.

Tenga en cuenta los siguientes puntos antes de modificar la cuenta de gestor del sistema:

- Asegúrese de utilizar un almacén de usuarios de LDAP y ha configurado un contenedor de usuarios como ou=Persona en el archivo de configuración del directorio (directory.xml) para su directorio de CA Identity Manager. Los usuarios seleccionados deben existir en el mismo contenedor donde configure el gestor del sistema. Si se selecciona una cuenta de usuario que no existe en el contenedor de usuarios, se pueden producir errores.
- Cuando el entorno de CA Identity Manager gestiona un directorio de usuarios con una estructura de usuario plana, el perfil del usuario seleccionado debe incluir también la organización. Para garantizar que el perfil de un usuario se haya configurado correctamente, agregue el nombre de la organización del usuario al atributo físico que corresponde al atributo conocido %ORG_MEMBERSHIP% en el archivo directory (en la página 86).xml. Por ejemplo, cuando la descripción de atributo físico se asigna al atributo conocido %ORG_MEMBERSHIP% en el archivo directory.xml y el usuario pertenece a la organización Empleados, el perfil del usuario debe contener el par de atributo/valor description=Empleados.

Siga estos pasos:

1. En la pantalla de entornos de CA Identity Manager, haga clic en el nombre del entorno de CA Identity Manager adecuado.

   Se muestran las propiedades de esa pantalla de entorno particular.

2. Haga clic en Gestor del sistema.

   Se mostrará el asistente de gestor del sistema.

3. Escriba el nombre único del usuario que tiene el rol de gestor del sistema tal y como se muestra a continuación:

   - Para usuarios de base de datos relacionales, escriba el identificador único para el usuario o valor que se asigna al atributo conocido %USER_ID% en el archivo de configuración del directorio.
   - Para usuarios de LDAP, escriba el nombre destacado del usuario. Por ejemplo, si el nombre destacado del usuario es uid=Admin1, ou=Persona, ou=Empleados, ou=NeteAuto, tipo Admin1.

   Nota: Asegúrese de que el gestor del sistema *no* sea el mismo usuario que el administrador del almacén de usuarios.

4. Haga clic en Validar para ver el identificador completo del usuario.

5. Haga clic en Siguiente.

6. En la segunda página del asistente, seleccione un rol para asignárselo al usuario tal y como se muestra a continuación:
   - Si desea asignar el rol de gestor del sistema, lleve a cabo las siguientes tareas:
     a. Active el siguiente botón de radio junto al rol de gestor del sistema.
     b. Haga clic en Finalizar.
   - Si desea asignar un rol distinto del rol de gestor del sistema, lleve a cabo las siguientes tareas:
     a. Seleccione una condición en la primera lista.
     b. Escriba un nombre de rol parcial o completo, o bien un asterisco (*) en el segundo cuadro de lista. Haga clic en Buscar.
     c. Seleccione el rol para asignar en la lista de resultados de la búsqueda.
     d. Haga clic en Finalizar.

   La pantalla de salida de configuración de gestor del sistema muestra la información de estado.
7. Haga clic en Continuar para cerrar el asistente de Gestor del sistema.

Acceso al estado de un entorno de CA Identity Manager

CA Identity Manager incluye una página de estado que se puede utilizar para verificar el siguiente estado:

- El directorio de CA Identity Manager se ha cargado correctamente.
- CA Identity Manager se puede conectar al almacén de usuarios.
- El entorno de CA Identity Manager se carga correctamente.

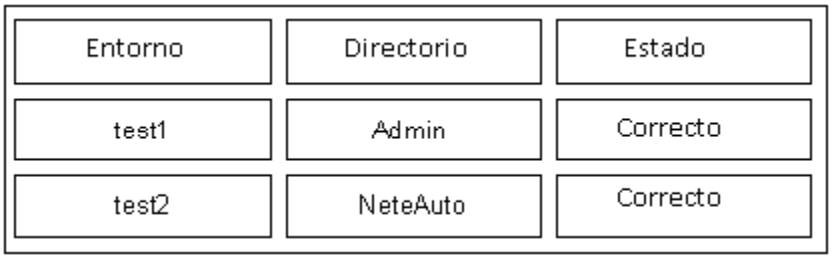
Para acceder a la página de estado, escriba la siguiente dirección URL en el explorador:

`http://hostname/iam/im/status.jsp`

nombre de host

Determina el nombre completo del servidor donde se ha instalado CA Identity Manager; por ejemplo, miservidor.miempresa.com.

Si el entorno de CA Identity Manager se inicia y todas las conexiones se están ejecutando correctamente, la página de estado se parecerá a la de la siguiente ilustración:



La página de estado también indica si el entorno cumple con la FIPS 140-2.

Solución de problemas de entornos de CA Identity Manager

En la siguiente tabla se describen posibles mensajes de error y el proceso de solución de problemas:

Mensaje	Descripción	Resolución de problemas
No cargado	El directorio de CA Identity Manager que se asocia al entorno no se ha cargado al iniciar CA Identity Manager.	1. Verifique que se esté ejecutando el almacén de usuarios. Si CA Identity Manager se integra con SiteMinder, verifique que SiteMinder se puede conectar al almacén de usuarios.
Not OK (No es correcto)	CA Identity Manager no se puede conectar al directorio de CA Identity Manager.	En la interfaz de usuario del servidor de políticas, se puede verificar la conexión abriendo la página de propiedades de la conexión del directorio de usuarios de SiteMinder, que se asocia al almacén de usuarios. A continuación, haga clic en el botón de ver el contenido. Si se puede ver el contenido del almacén de usuarios, SiteMinder se puede conectar correctamente. Para obtener más información sobre el servidor de políticas, consulte la *Guía de configuración del servidor de políticas del gestor de acceso web de CA SiteMinder*. 2. Reinicie CA Identity Manager y el servidor de políticas.

Mensaje	Descripción	Resolución de problemas
La conexión de SM no es correcta	CA Identity Manager no se puede conectar al servidor de políticas de SiteMinder (para implementaciones que incluyen SiteMinder)	1. Verifique las siguientes condiciones: ■ El servidor de políticas está en ejecución. ■ El agente web está protegiendo recursos. Se puede verificar que el agente web esté ejecutando correctamente accediendo a la interfaz de usuario del servidor de políticas. Si se le piden las credenciales, significará que el agente web está funcionando correctamente. 2. Reinicie CA Identity Manager y el servidor de políticas.
IMS no está disponible en este momento	Se ha producido un error en CA Identity Manager.	Compruebe el registro de servidor de aplicaciones para ver los detalles del error.
Mensaje de error 500 de Windows	La página de estado no se muestra cuando se accede a ella aunque se elimine la conectividad con el directorio de usuarios de LDAP.	Desactive la opción del explorador de Internet que muestra el mensaje de error de forma descriptiva para ver la página de estado.

Capítulo 7: Configuración avanzada

La ventana Configuración avanzada de la Consola de gestión permite configurar los siguientes parámetros:

- Acceso a las pantallas de los parámetros de configuración avanzada.
- Configuración avanzada de importación y exportación, como se describe en Configuración personalizada de importación y exportación (en la página 248).

Esta sección contiene los siguientes temas:

Auditoría

Los registros de auditorías mantienen un registro de las operaciones realizadas en un entorno de CA Identity Manager. Se pueden utilizar los datos en registros de auditoría para controlar la actividad de un sistema.

Eventos de auditorías de CA Identity Manager. Un evento es una operación generada por una tarea de CA Identity Manager. Una tarea puede generar varios eventos. Por ejemplo, la tarea CreateUser puede generar los eventos CreateUserEvent y AddToGroupEvent.

De forma predeterminada, CA Identity Manager exporta toda la información del evento a la base de datos de auditoría. Para controlar el tipo y cantidad de información del evento que registra CA Identity Manager, se pueden realizar las tareas siguientes:

- Activar la auditoría para tareas de administración de CA Identity Manager.
- Activar la auditoría para algunos o todos los eventos de CA Identity Manager que generen las tareas de administración.
- Registrar información del evento en estados específicos, por ejemplo, cuando se completa o se cancela un evento.
- Registrar información acerca de atributos implicados en un evento. Por ejemplo, se pueden registrar atributos que cambian durante un evento ModifyUserEvent.
- Establecer el nivel de la auditoría para eventos y atributos.

Identificadores de tareas lógicas del negocio

Un identificador de tareas lógicas del negocio realiza la lógica del negocio personalizada antes de que se envíe una tarea de CA Identity Manager para su procesamiento. Normalmente, la lógica del negocio personalizada valida los datos. Por ejemplo, un identificador de tareas lógicas del negocio puede comprobar el límite de pertenencia de un grupo antes de que CA Identity Manager agregue un miembro al grupo. Cuando se alcanza el límite de pertenencia a un grupo, el identificador de tareas lógicas del negocio muestra un mensaje que informa al administrador de grupos de que no se ha podido agregar el miembro nuevo.

Se pueden utilizar los identificadores de tareas lógicas del negocio predeterminados o se pueden crear identificadores personalizados mediante la API del identificador de tareas lógicas del negocio.

Nota: Para obtener información acerca de la creación de lógica del negocio personalizada, consulte la *Guía de programación para Java*.

La pantalla Identificadores de tareas lógicas del negocio (BLTH) contiene una lista de identificadores de tareas lógicas del negocio globales existentes. La lista incluye los identificadores predefinidos que se incluyen con CA Identity Manager y los identificadores personalizados definidos en el sitio. CA Identity Manager ejecuta los identificadores en el orden en que aparecen en esta lista.

Los identificadores de tareas lógicas del negocio globales se pueden implementar solamente en Java.

Borrar automáticamente campos de contraseña en la tarea Restablecimiento de la contraseña del usuario

Se puede configurar CA Identity Manager para que borre automáticamente los campos de contraseña cuando un valor introducido previamente infringe una política de contraseñas o cuando los valores de los campos Contraseña y Confirmar contraseña no coinciden.

Siga estos pasos:

1. Inicie la Consola de gestión.
2. Seleccione el entorno que desee gestionar, a continuación, haga clic en Configuración avanzada.

   Aparecerá la página Advanced Settings.
3. Haga clic en Identificadores de tareas lógicas del negocio (BLTH), BlthPasswordServices.

   Aparecerá la página de propiedades de los identificadores de lógica del negocio.
4. Cree las siguientes propiedades:

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|
5. Verifique que los parámetros de configuración de ConfirmPasswordHandler son los siguientes:
   - Tipo de objeto: Usuario
   - Clase: ConfirmPasswordHandler
   - ConfirmationAttributeName: |passwordConfirm|
   - OldPasswordAttributeName: |oldPassword|
   - passwordAttributeName: %PASSWORD%

   Los usuarios ahora pueden borrar campos de contraseña en la tarea Restablecimiento de la contraseña del usuario.

Lista de eventos

Las tareas de administración incluyen *eventos*, acciones que realiza CA Identity Manager para completar la tarea. Una tarea puede incluir varios eventos. Por ejemplo, la tarea Crear usuario puede incluir eventos de creación del perfil de un usuario, adición del usuario a un grupo y asignación de roles.

CA Identity Manager audita eventos, impone reglas del negocio específicas del cliente asociadas con eventos y, cuando los eventos se asignan a los procesos de flujo de trabajo, se requiere la aprobación de los eventos.

Se puede usar esta página para ver una lista de los eventos que están disponibles en CA Identity Manager.

Notificaciones de correo electrónico

CA Identity Manager puede enviar notificaciones de correo electrónico cuando se completa una tarea o evento, o cuando un evento bajo control del flujo de trabajo llega a un estado específico. Por ejemplo, un mensaje de correo electrónico puede informar un aprobador de que un evento requiere aprobación.

Para especificar el contenido de las notificaciones de correo electrónico, se pueden utilizar plantillas de correo electrónico predeterminadas o se pueden personalizar las plantillas para que se adapten a las necesidades de cada caso.

Mediante la Consola de gestión, se pueden realizar las tareas siguientes:

- Activar las notificaciones de correo electrónico para un entorno de CA Identity Manager.
- Especificar los conjuntos de plantillas para crear mensajes de correo electrónico.
- Indicar los eventos y las tareas para los cuales se envían notificaciones de correo electrónico.

Escuchas de eventos

Una tarea de CA Identity Manager está formada por una o varias acciones, denominadas eventos, que realiza CA Identity Manager durante la ejecución de la tarea. Por ejemplo, la tarea Crear usuario puede incluir los siguientes eventos:

- CreateUserEvent: crea un perfil de usuario en una organización.
- AddToGroupEvent (opcional): agrega al usuario como miembro de un grupo.
- AssignAccessRole (opcional): asigna un rol de acceso al usuario.

Una *escucha de eventos* está a la "escucha" de un evento específico y, a continuación, realiza una lógica del negocio personalizada en un punto específico en el ciclo de vida de un evento. Por ejemplo, después de que se cree un usuario nuevo en CA Identity Manager, una escucha de eventos puede agregar la información de un usuario a una base de datos de otra aplicación.

Nota: Para obtener más información sobre la configuración de escuchas de eventos, consulte la *Guía de programación para Java*.

Políticas de identidad

Una política de identidad se aplica a un conjunto de cambios de negocio a usuarios que cumplen ciertas reglas o condiciones. Se pueden utilizar políticas de identidad para hacer lo siguiente:

- Automatizar ciertas tareas de gestión de identidades, como por ejemplo la asignación de roles y la pertenencia a un grupo, la asignación de recursos o la modificación de los atributos del perfil de usuario.
- Imponer la segregación de obligaciones. Por ejemplo, se puede crear una política de identidad que prohíba a los miembros del rol Comprobar firmante tener el rol Comprobar aprobador.
- Imponer el cumplimiento. Por ejemplo, se pueden auditar usuarios que tengan un cargo determinado y ganen más de 100000 $.

Los conjuntos de políticas de identidad se crean y se gestionan en la Consola de usuario. Para obtener más información sobre las políticas de identidad, consulte la *Guía de administración*.

Antes de utilizar las políticas de identidad, utilice la Consola de gestión para llevar a cabo las siguientes tareas:

- Activar las políticas de identidad para un entorno de CA Identity Manager.
- Establecer el nivel de recursión (opcional).

Identificadores de atributos lógicos

Los atributos lógicos de CA Identity Manager permiten mostrar atributos de almacén de usuarios (denominados *atributos físicos*) en un formato sencillo en las pantallas de tarea. Los administradores de CA Identity Manager utilizan las pantallas de tarea para realizar funciones en CA Identity Manager.

Los atributos lógicos no están presentes en un almacén de usuarios. Normalmente, representan uno o más atributos físicos para simplificar la presentación. Por ejemplo, el atributo lógico *fecha* puede representar los atributos físicos *mes*, *día* y *año*.

Los atributos lógicos se procesan mediante identificadores de atributos lógicos, que son objetos Java que se escriben utilizando la API de atributos lógicos. Por ejemplo, cuando se muestra una pantalla de tarea, un controlador de atributos lógicos podría convertir los datos de un atributo físico del almacén de usuarios en datos de un atributo lógico.

Se pueden utilizar los atributos lógicos e identificadores de atributos lógicos predefinidos incluidos con CA Identity Manager o se pueden crear otros nuevos usando la API de atributos lógicos.

Nota: Para obtener más información, consulte la *Guía de programación para Java*.

Opciones varias

Las propiedades definidas por el usuario que se definen en esta pantalla se aplican a todo el entorno de CA Identity Manager. Se transfieren como pares nombre-valor al método init() de todos los objetos de Java personalizados que se creen con las API de CA Identity Manager. Un objeto personalizado puede utilizar estos datos de cualquier manera que requiera la lógica del negocio del objeto.

Las propiedades definidas por el usuario también están definidas para un objeto personalizado particular. Por ejemplo, si las propiedades definidas por el usuario están definidas en la pantalla Propiedades de una escucha de eventos llamada MiEscucha. Las propiedades definidas por el usuario específicas de un objeto y las propiedades de todo el entorno definidas en las pantallas Varios se transfieren en una llamada única a MyListener.init().

Para agregar una propiedad definida por el usuario, especifique un nombre y un valor de propiedad y haga clic en Agregar.

Para suprimir una o varias propiedades definidas por el usuario, seleccione la casilla de verificación que se encuentra junto a cada par nombre-valor que desee suprimir y haga clic en Suprimir.

Cuando se hayan hecho los cambios, haga clic en Guardar. Reinicie el servidor de aplicaciones para que se apliquen los cambios.

Nota: Todas las propiedades de Varios distinguen entre mayúsculas y minúsculas. Por lo tanto, si se define una propiedad denominada SelfRegistrationLogoutUrl y otra propiedad denominada selfregistrationlogouturl, se agregarán las dos propiedades.

Reglas de notificación

Una regla de notificación determina qué usuarios deben recibir notificaciones de correo electrónico. Cuando se completa una tarea o un evento de una tarea llega a un estado concreto como de aprobación pendiente, aprobada o rechazada, los usuarios reciben una notificación de correo electrónico según la regla de notificación.

Nota: Para obtener más información sobre la función de notificación de correo electrónico, consulte la *Guía de administración*.

CA Identity Manager incluye las siguientes reglas de notificación predeterminadas:

ADMIN_ADAPTER

Envía un mensaje de correo electrónico al administrador que inicia la tarea.

USER_ADAPTER

Envía un mensaje de correo electrónico al usuario al que afecta la tarea

USER_MANAGER

Envía un mensaje de correo electrónico al gestor del usuario en el contexto actual

Para crear reglas de notificación personalizadas, se puede utilizar la API de reglas de notificaciones.

Nota: Para obtener más información sobre las reglas de notificaciones, consulte la *Guía de programación para Java*.

Seleccionadores de organizaciones

Un seleccionador de organizaciones es un identificador de atributos lógicos personalizado que determina dónde crea CA Identity Manager el perfil de un usuario autorregistrado, que está basado en la información que proporciona el usuario durante el registro. Por ejemplo, el perfil para usuarios que proporcionan un código promocional cuando se registran puede que se agregue a una organización de usuarios de promoción.

Aprovisionamiento

Esta pantalla se utiliza cuando se está usando CA Identity Manager con aprovisionamiento.

Nota: Un procedimiento más detallado, sobre la configuración de aprovisionamiento para un entorno de CA Identity Manager (en la página 197), proporciona instrucciones paso a paso.

Las opciones de propiedades de aprovisionamiento son las siguientes:

Activado

Especifica el uso de dos almacenes de usuarios, uno para CA Identity Manager y un almacén de usuarios independiente (denominado directorio de aprovisionamiento) para cuentas de aprovisionamiento. Si esta opción se desactiva, solamente se utiliza el almacén de usuarios de CA Identity Manager.

Use Session Pool (Uso de agrupación de sesiones)

Activa el uso de una agrupación de sesiones.

Session Pool Initial Sessions (Sesiones iniciales de la agrupación de sesiones)

Define el número mínimo de sesiones disponibles en la agrupación al inicio.

Valor predeterminado: 8

Session Pool Maximum Sessions (Máximo de sesiones de la agrupación de sesiones)

Define el número máximo de sesiones de la agrupación.

Valor predeterminado: 32

Enable Password Changes from Endpoint Accounts (Activar cambios de la contraseña de cuentas de puntos finales)

Define la configuración de Activar agente de sincronización de contraseñas para cada usuario del servidor de aprovisionamiento. Esta opción permite la sincronización de contraseñas entre usuarios de CA Identity Manager y cuentas de puntos finales asociadas.

Activar la acumulación de eventos de pertenencia del rol de aprovisionamiento

Si se activa, esta casilla de verificación garantiza que CA Identity Manager ejecutará los eventos relacionados con la pertenencia al rol de aprovisionamiento en un orden específico. Cuando se ejecute este evento, todas las acciones de agregar se combinarán en una sola operación y se enviarán al servidor de aprovisionamiento con el fin de procesarlas. Una vez que haya finalizado el procesamiento de las acciones de agregar, CA Identity Manager combinará las acciones de eliminar en una sola operación y enviará dicha operación al servidor de aprovisionamiento. Se genera un evento único, llamado AccumulatedProvisioningRoleEvent, para ejecutar los eventos en este orden.

Nota: Para obtener más información sobre AccumulatedProvisioningRoleEvent, consulte la *Guía de administración*.

Organización para crear usuarios de entrada

Define la ruta completamente cualificada al almacén de usuarios que utiliza CA Identity Manager. Este campo aparece solamente cuando el almacén de usuarios incluye una organización.

Administrador entrante

Define una cuenta de administrador de CA Identity Manager que puede ejecutar tareas asignadas a asignaciones de entrada. Estas tareas se incluyen en el rol Gestor de la sincronización del aprovisionamiento. El administrador debe ser capaz de ejecutar cada tarea en cualquier usuario de CA Identity Manager.

Directorio de aprovisionamiento

El directorio de aprovisionamiento es un repositorio para la información de aprovisionamiento que incluye el dominio, los usuarios globales, los tipos de punto final, los puntos finales, las cuentas y las plantillas de cuenta. Cuando se selecciona, aparecen otras opciones para asignar el almacén de usuarios de CA Identity Manager al directorio de aprovisionamiento.

Activar el agrupamiento de sesiones

Para mejorar el rendimiento, CA Identity Manager puede preadjudicar un número de sesiones para que se agrupen durante la comunicación con el servidor de aprovisionamiento.

Si la opción Session Pools (Agrupaciones de sesiones) está desactivada, CA Identity Manager crea y destruye sesiones según sea necesario.

Para un entorno nuevo, Session Pools (Agrupaciones de sesiones) estará activado de forma predeterminada. Para entornos existentes, se puede activar Session Pools (Agrupaciones de sesiones).

Siga estos pasos:

1. En la Consola de gestión, seleccione Advanced Settings (Configuración avanzada), Provisioning (Aprovisionamiento).
2. Seleccione Use Session Pool (Uso de agrupación de sesiones).
3. Defina el número mínimo de sesiones de la agrupación al inicio.
4. Defina el número máximo de sesiones de la agrupación.
5. Haga clic en Save.
6. Reinicie el servidor de aplicaciones.

   La opción de agrupación de sesiones estará activada con los parámetros de configuración definidos.

Activación de la sincronización de contraseñas

El servidor de aprovisionamiento permite sincronizar contraseñas entre usuarios de CA Identity Manager y cuentas de usuarios de puntos finales asociadas. Dicho de otra manera, cuando se crea o se modifica un usuario que tenga roles de aprovisionamiento en CA Identity Manager, el usuario de aprovisionamiento se establece para permitir cambios de la contraseña de cuentas de puntos finales.

Nota: Cuando se activa esta función en la Consola de gestión, *todos* los usuarios del entorno se establecen para permitir cambios de la contraseña de cuentas de puntos finales.

Para activar la sincronización de contraseñas

1. En la Consola de gestión, seleccione Advanced Settings (Configuración avanzada), Provisioning (Aprovisionamiento).
2. Active Enable Password Changes from Endpoint Accounts (Activar cambios de contraseña de cuentas de puntos finales).
3. Haga clic en Save.
4. Reinicie el servidor de aplicaciones.

Asignaciones de atributos

Las asignaciones de atributos asocian los atributos de usuarios en tareas de administración relacionadas con el aprovisionamiento, como el aprovisionamiento de creación de usuario, con los atributos correspondientes en el servidor de aprovisionamiento. Un atributo de aprovisionamiento único se puede asignar a varios atributos en el almacén de usuarios de CA Identity Manager.

Las asignaciones predeterminadas existen para los atributos en las tareas predeterminadas, que se clasifican en la sección Asignaciones de entrada. Si se modifica una de estas tareas de administración para utilizar atributos diferentes, se deben actualizar las asignaciones de atributos según sea necesario.

Asignaciones de entrada

Las asignaciones de entrada asignan eventos, que genera el servidor de aprovisionamiento, a una tarea de administración. Estas asignaciones están predefinidas y no se pueden modificar.

Asignaciones de salida

Las asignaciones de salida asocian eventos, que generan las tareas de administración, con eventos que se aplican al directorio de aprovisionamiento. Las asignaciones predeterminadas existen para los eventos que afectan a los atributos del usuario.

Consola de usuario

Se accede a un entorno de CA Identity Manager mediante la Consola de usuario, una aplicación web que permite a los usuarios realizar tareas de administración. Se definen ciertas propiedades para la Consola de usuario que los administradores usan para acceder a un entorno en la página Consola de usuario en la Consola de gestión.

La página Consola de usuario incluye los siguientes campos:

Propiedades generales

Define las propiedades que se aplican a un entorno.

Show Recently Completed Tasks (Mostrar tareas completadas recientemente)

Determina si CA Identity Manager muestra un mensaje de estado cuando se completa una tarea.

Cuando esta opción está seleccionada, los usuarios deben hacer clic en Aceptar para borrar el mensaje de estado que muestra CA Identity Manager.

Para desactivar el mensaje y evitar que los usuarios tengan que hacer clic en Aceptar cuando aparezca cada mensaje de estado, anule la selección de esta opción.

Show About Link (Mostrar el vínculo Acerca de)

Determina si aparece un vínculo Acerca de en la esquina inferior derecha de la Consola de usuario. Cuando esta opción está seleccionada, los usuarios de CA Identity Manager pueden hacer clic en el vínculo Acerca de para ver información de la versión de los componentes de CA Identity Manager.

Activación de cambio de idioma

Determina si CA Identity Manager incluye la lista desplegable Elegir idioma en la pantalla de inicio de sesión y en la Consola de usuario. Cuando este campo está seleccionado, los usuarios de CA Identity Manager pueden cambiar el idioma de la Consola de usuario seleccionando un idioma nuevo en la lista.

Nota: Para mostrar el campo Elegir idioma, se debe verificar que se selecciona el campo Enable Language Switching (Activar cambio de idioma) *y* se configura CA Identity Manager para que sea compatible con varios idiomas.

Consulte la *Guía de diseño de la Consola de usuario* si desea obtener más información.

Job Timeout (Tiempo de espera de trabajos)

Determina la cantidad de tiempo que CA Identity Manager espera después de que una tarea se envíe antes de mostrarse un mensaje de estado.

Cuando la tarea se completa en la cantidad especificada de tiempo, CA Identity Manager muestra el siguiente mensaje:

Tarea finalizada

Si la tarea tarda más tiempo en completarse o está bajo control del flujo de trabajo, CA Identity Manager muestra el siguiente mensaje:

"Task has been submitted for processing on the current date" ("Se ha enviado la tarea para su procesamiento en la *fecha actual*").

Nota: Es posible que los cambios no se apliquen inmediatamente.

Propiedades de los temas

Permiten personalizar el icono y el título de la Consola de usuario en un entorno. Por ejemplo, se pueden agregar un logotipo de la compañía y el nombre de la compañía a las pantallas de la Consola de usuario.

Entre las propiedades de los temas se incluyen los siguientes parámetros de configuración:

Icon (URI) (Icono [URI])

Define el icono mediante un URI a una imagen disponible para el servidor de aplicaciones.

Ejemplo: http://myserver.mycompany.com/images/front/logo.gif

Icon Link (URI) (Vínculo de icono [URI])

Define el vínculo de navegación a la imagen mediante un URI.

Icon Title (Título del icono)

Define la información sobre herramientas que parece como texto al mover el ratón por encima del icono.

Título

Especifica el texto personalizado que se muestra al lado del icono en la parte superior de la Consola de usuario.

Nota: Si se ha definido una máscara personalizada, se puede especificar un icono o título haciendo referencia a un archivo de propiedades para la máscara. Por ejemplo, si la entrada para la imagen del icono en el archivo de propiedades para una máscara personalizada es image/logo.gif, se puede introducir esa misma cadena en el campo de icono.

Propiedades de inicio de sesión

Especifican el método de autenticación y la ubicación de la página de inicio de sesión a la cual se dirigen usuarios cuando acceden a un entorno.

Authentication Provider module class name (Nombre de clase de módulo de proveedor de autenticación)

Especifica el nombre de clase del módulo de proveedor de autenticación.

Página Inicio de sesión

Especifica la página a la que se dirige a los usuarios cuando acceden a un entorno.

Servicios Web

El servicio web de ejecución de tareas (TEWS) de CA Identity Manager permite que las aplicaciones de clientes de terceros envíen tareas de CA Identity Manager a CA Identity Manager ejecución remota.

La pantalla de propiedades de servicios web permite configurar TEWS para un entorno. En esta pantalla, se pueden llevar a cabo las siguientes tareas:

- Activar TEWS para un entorno de CA Identity Manager.
- Generar documentos con un lenguaje de descripción de servicios web (WSDL) específicos para una tarea.
- Permitir la suplantación.
- Especificar que la contraseña de administrador se requiere para la autenticación.
- Configurar la autenticación de SiteMinder.
- Configurar SiteMinder para asegurar la dirección URL de servicios web, si CA Identity Manager se integra con SiteMinder.
- Especificar la autenticación de token de nombre de usuario de servicios de seguridad web.
- Especificar como mínimo uno de los tres posibles tipos de autenticación.

Para obtener información relativa al suministro de solicitudes remotas a CA Identity Manager mediante el servicio web de ejecución de tareas, consulte la *Guía de programación para Java*.

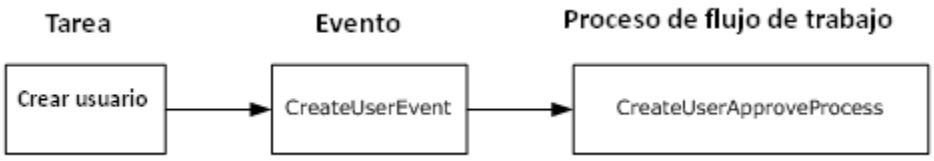
Workflow Properties (Propiedades del flujo de trabajo)

Si se activa, la función de flujo de trabajo controla la ejecución de una tarea de CA Identity Manager asociada con un proceso de flujo de trabajo.

Un proceso de flujo de trabajo es un conjunto de pasos que se realizan para lograr un objetivo de negocio, como crear una cuenta de usuario. Normalmente, uno de estos pasos implica aprobar o rechazar la tarea.

Una tarea de administración se asocia a uno o varios eventos, que pueden activar uno o varios procesos de flujo de trabajo. Después de que los procesos de flujo de trabajo se completen, CA Identity Manager realiza o rechaza la tarea que está basada en los resultados de los procesos de flujo de trabajo.

La siguiente ilustración muestra la relación entre una tarea de CA Identity Manager, un evento asociado y un proceso de flujo de trabajo:



Workflow Properties (Propiedades del flujo de trabajo)

La casilla de verificación se utiliza para activar o desactivar el flujo de trabajo del entorno de CA Identity Manager.

Delegación de elementos de trabajo

Si se activa, la delegación de elementos de trabajo permite a un participante (el delegador) especificar que otro usuario (el delegado) obtenga los permisos para aprobar tareas en la lista de trabajo del delegador. Un participante puede asignar elementos de trabajo a otro aprobador durante períodos en los que el delegador esté “fuera de la oficina.” Los delegadores conservan acceso completo a sus elementos de trabajo durante el período de delegación.

La delegación utiliza el siguiente atributo conocido:

%DELEGATORS%

Este atributo conocido almacena los nombres de los usuarios que estén delegando en el usuario con el atributo, así como el tiempo en que se creó la delegación.

Nota: Para obtener más información sobre la delegación de elementos de trabajo, consulte la *Guía de administración*.

Workflow Participant Resolvers (Asignadores de participantes del flujo de trabajo)

Las actividades de un proceso de flujo de trabajo, como aprobar o rechazar una tarea, las realizan los *participantes.*

La pantalla Workflow Participant Resolvers (Asignadores de participantes del flujo de trabajo) se utiliza para asignar un asignador de participante personalizado a un clase de Java de asignador de participantes completamente cualificado.

Un *asignador de participantes* personalizado es un objeto de Java que determina los participantes de una actividad de flujo de trabajo y devuelve una lista a CA Identity Manager. A continuación, CA Identity Manager transfiere la lista al motor del flujo de trabajo.

Por lo general, sólo deberá escribir un asignador de participantes personalizado si ninguno de los asignadores de participantes estándares puede ofrecer la lista de participantes que requiere una actividad.

Nota: Para obtener información acerca del desarrollo de asignadores de participantes personalizados, consulte la *Guía de programación para Java*. Para obtener información acerca de los asignadores de participantes estándares, consulte la *Guía de administración*.

Configuración personalizada de importación y exportación

En la pantalla Configuración avanzada en la Consola de gestión, se puede aplicar la configuración avanzada a varios entornos, como se muestra a continuación:

- Configurar los parámetros de configuración avanzada en un entorno.
- Exportar la configuración avanzada a un archivo XML.
- Importar el archivo XML a los entornos obligatorios.

Errores de falta de memoria de la máquina virtual de Java

Síntoma:

Se reciben errores de falta de memoria de JVM durante períodos de estrés o de carga elevada que afectan a la funcionalidad del servidor de CA Identity Manager.

Solución:

Se recomienda que se establezcan las opciones de depuración de JVM para que se alerte en condiciones de falta de memoria.

Nota: Para obtener más información sobre el establecimiento de opciones de depuración de JVM, consulte Debugging Options in Java HotSpot VM Options en http://www.oracle.com.

Capítulo 8: Auditoría

Esta sección contiene los siguientes temas:

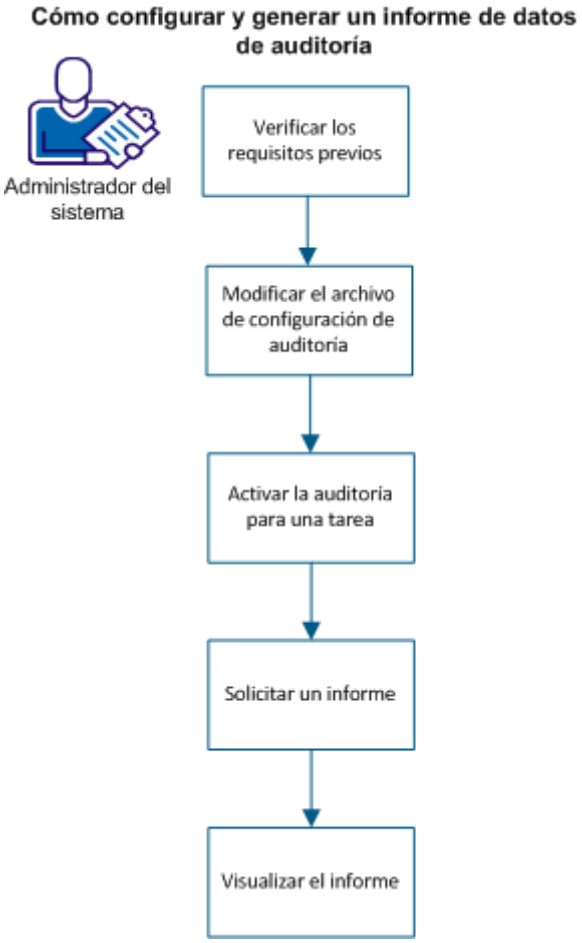
Cómo configurar y generar un informe de datos de auditoría

Los datos de auditoría proporcionan un registro del historial de operaciones que se producen en un entorno. Cuando se configura y se activa la auditoría, el sistema registra información acerca de las tareas en una base de datos de auditoría. La información de la auditoría se puede utilizar para generar informes. A continuación, se muestran algunos ejemplos de datos de auditoría:

- Actividad del sistema para un período especificado de un tiempo.
- Eventos de inicio y cierre de sesión de usuarios mientras se accede a un entorno concreto.
- Las tareas que realiza un usuario específico.
- Una lista de objetos modificados durante un período específico.
- Los roles asignados a usuarios.
- Las operaciones realizadas para una determinada cuenta de usuario.

Los datos de auditoría se generan para los *eventos* de CA Identity Manager. Un evento es una operación generada por una tarea de CA Identity Manager. Por ejemplo, la tarea Crear usuario puede incluir un evento AssignAccessRoleEvent.

El diagrama siguiente describe cómo un administrador del sistema configura la auditoría y genera un informe en los datos de auditoría:



Como administrador, realice los pasos siguientes:

1. Verificación de los requisitos previos (en la página 251)
2. Modificación de un archivo de configuración de auditoría (en la página 251)
3. Activación de la auditoría para una tarea (en la página 256)
4. Solicitud de informe (en la página 257)
5. Visualización del informe (en la página 260)

Verificación de los requisitos previos

Verifique que los requisitos previos siguientes se cumplan antes de configurar los valores de auditoría:

- Se crea una instancia de la base de datos separada para almacenar datos que se relacionan con la auditoría. De forma predeterminada, el archivo de esquema de la base de datos de CA Identity Manager se encuentra en la ubicación siguiente:
  - **Windows**: <rutainstalación>\Identity Manager\tools\db
- Configure la conexión del servidor de informes para solicitar y ver el informe de auditoría.
- Agregue un objeto de conexión para el informe de auditoría. Realice los pasos siguientes:
  a. Inicie sesión en la Consola de usuario con privilegios administrativos.
  b. Vaya a Roles y tareas, Tareas de administración y busque un informe de auditoría para modificar.
  c. Introduzca el nombre de conexión siguiente en el objeto de conexión para el campo Informe:
     `rptParamConn`

Modificación de un archivo de configuración de auditoría

Configure los valores de la auditoría en el archivo de configuración de auditoría para definir el tipo de información que CA Identity Manager debe auditar. Se puede configurar un archivo de configuración de auditoría para realizar lo siguiente:

- Auditar algunas o todas las tareas de administración que han generado eventos.
- Registrar información del evento en estados específicos, como cuando se completa o se cancela un evento.
- Registrar información acerca de atributos implicados en un evento. Por ejemplo, se pueden registrar atributos que cambian durante un evento ModifyUserEvent.

- Establecer el nivel de la auditoría para el registro de atributos.

El archivo de configuración de auditoría es un archivo XML que se crea exportando la configuración de una auditoría. El archivo tiene el siguiente esquema:

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

Para obtener más información sobre los elementos de auditoría y esquema, consulte los comentarios en el archivo de configuración de auditoría.

Los elementos AuditProfileAttribute indican los atributos que audita CA Identity Manager. Los atributos se aplican al objeto especificado en el elemento AuditProfile.

Nota: Si no hay ningún atributo de perfil de auditoría especificado, se registrarán todos los atributos del objeto especificados en el elemento AuditProfile.

La siguiente tabla muestra los atributos válidos para los tipos de objeto de CA Identity Manager:

Atributos válidos para los tipos de objeto de CA Identity Manager

Tipo de objeto	Atributos válidos
ACCESS ROLE	■ name: nombre visible por el usuario para el rol. ■ description: comentario opcional sobre la finalidad del rol. ■ members: usuarios que pueden utilizar el rol. ■ administrators: usuarios que pueden asignar administradores o miembros de roles. ■ owners: usuarios que pueden modificar el rol. ■ enabled: indica si el rol está activado o no. ■ assignable: indica si un administrador puede asignar el rol o no. ■ tasks: tareas de acceso asociadas al rol.

Atributos válidos para los tipos de objeto de CA Identity Manager	
Tipo de objeto	**Atributos válidos**
ACCESS TASK	■ name: nombre visible por el usuario para la tarea. ■ description: comentario opcional sobre la finalidad de la tarea. ■ application: aplicación asociada a la tarea. ■ tag: identificador único de la tarea. ■ reserved1, reserved2, reserved3, reserved4: valores de los campos reservados para la tarea.
ADMINISTRATIVE ROLE	■ name: nombre visible por el usuario para el rol. ■ description: comentario opcional sobre la finalidad del rol. ■ members: usuarios que pueden utilizar el rol. ■ administrators: usuarios que pueden asignar administradores o miembros de roles. ■ owners: usuarios que pueden modificar el rol. ■ enabled: indica si el rol está activado o no. ■ assignable: indica si un administrador puede asignar el rol o no. ■ tasks: tareas asociadas al rol.

Atributos válidos para los tipos de objeto de CA Identity Manager	
Tipo de objeto	**Atributos válidos**
ADMINISTRATIVE TASK	■ name: nombre visible por el usuario para la tarea. ■ description: comentario opcional sobre la finalidad de la tarea. ■ tag: identificador único de la tarea. ■ category: la categoría en la interfaz de usuario de CA Identity Manager donde aparece la tarea. ■ primary_object: objeto sobre el que opera la tarea. ■ action: operación que se realiza en el objeto. ■ hidden: indica si la tarea *no* aparece en los menús. ■ public: indica si la tarea está disponible para los usuarios que no han iniciado sesión en CA Identity Manager. ■ auditing: indica si la tarea activa el registro de la información de la auditoría. ■ external: indica si la tarea es externa. ■ url: dirección URL a la que CA Identity Manager redirige al usuario cuando se ejecuta una tarea externa. ■ workflow: indica si los eventos de CA Identity Manager asociados con la tarea activan el flujo de trabajo. ■ webservice: indica si para la tarea se pueden generar resultados WSDL (lenguaje de descripción de servicios web) desde la Consola de gestión de CA Identity Manager.
GROUP	Cualquier atributo válido definido para el objeto de grupo en el archivo de configuración del directorio (directory.xml).
ORGANIZATION	Cualquier atributo válido definido para el objeto de organización en el archivo de configuración del directorio (directory.xml).
PARENTORG	

Atributos válidos para los tipos de objeto de CA Identity Manager	
Tipo de objeto	**Atributos válidos**
RELATIONSHIP	■ %CONTAINER%: identificador único del objeto principal. Por ejemplo, si el objeto RELATIONSHIP describe la pertenencia a un rol, el contenedor sería el rol. ■ %CONTAINER_NAME%: nombre visible por el usuario del grupo principal. ■ %ITEM%: identificador único del objeto que está contenido en el objeto principal. Por ejemplo, si el objeto RELATIONSHIP describe la pertenencia a un rol, los elementos serían los miembros de roles. ■ %ITEM_NAME%: nombre visible por el usuario para el grupo anidado.
USER	Cualquier atributo válido definido para el objeto de usuario en el archivo de configuración del directorio (directory.xml).
NINGUNO	Ningún atributo.

Nota: Los puntos siguientes se aplican a la tabla anterior:

- Enabled, assignable, auditable, workflow, hidden, webservice y public se registran como true o false.
- Al auditar tareas para roles, se registra el nombre visible por el usuario.
- La base de datos almacena miembros, administradores y políticas de propietario en formato XML compilado. Este formato es diferente de la interfaz de usuario, donde cada política aparece como una expresión.

Siga estos pasos:

1. Inicie sesión en la Consola de gestión, seleccione el entorno, Configuración avanzada y haga clic en Auditoría.
2. Haga clic en Exportar.

   El sistema exporta la configuración de auditoría actual a un archivo XML de configuración de auditoría.

3. Modifique la configuración de auditoría en el archivo XML que se ha exportado en el paso anterior. Lleve a cabo las siguientes tareas:
   a. Active el valor para la auditoría ="true" y proporcione el valor Nombre de JNDI de "iam_im_<auditdb>.xml" para el origen de datos del elemento.
   b. Especifique el siguiente nombre de JNDI:
      `java:/auditDbDataSource`

      Nota: El origen de datos se encuentra en la ubicación siguiente:
      `iam/im/jdbc/auditDbDataSource`
   c. Agregue, modifique o suprima los elementos del archivo.
   d. Modifique el nivel de información que se registra para cada evento.
4. Repita los pasos 1 y 2. Haga clic en Importar y cargue el archivo XML modificado de los valores de configuración de auditoría.
5. Reinicie el entorno.

El archivo de configuración de auditoría se ha actualizado ahora.

Activación de la auditoría para una tarea

Active la auditoría para las tareas para las cuales se ha configurado la auditoría en el archivo de configuración de auditoría.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario con los privilegios de administrador del sistema.
2. Cree o modifique la tarea para la cual desea activar la auditoría.
3. En la ficha Perfil, garantice que la casilla de verificación Activar auditoría esté seleccionada.
4. Haga clic en Enviar.

Ahora la auditoría está activada.

Solicitud de informe

Para ver el informe, solicite un informe a un usuario que disponga de privilegios de administración de informes. Seleccione el informe adecuado que siga los datos de auditoría. Si su solicitud de informes requiere aprobación, el sistema le envía una alerta de correo electrónico.

Antes de programar un informe, realice los pasos siguientes:

1. Inicie sesión en la Consola de usuario con privilegios administrativos.
2. Vaya a Roles y tareas, Modificar la tarea de administración y seleccione un informe de auditoría para modificar.
3. Seleccione la ficha Fichas y haga clic en ReportServerScheduler de IAM para editarla.
4. Marque la casilla de verificación Activar opción Repetición.
5. Haga clic en Aceptar y, a continuación, en Enviar.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario con privilegios de usuario de tareas de informes.
2. Seleccione Informes, Tareas de informes y Solicitar un informe.

   Aparecerá una lista de informes.
3. Seleccione un informe de auditoría.

   Aparecerá una pantalla de parámetros.
4. Haga clic en Programar informe y seleccione una programación para su informe.

   Ahora

   Especifica que el informe se ejecuta de inmediato.

   Una vez

   Especifica que el informe se ejecuta una vez,durante un período de tiempo específico. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

   (Sólo informe de auditoría) Cada hora

   Especifica que el informe se genera a la hora de inicio y, en lo sucesivo, cada 'n' horas; 'n' indica el intervalo entre informes sucesivos. Seleccione la fecha de inicio y de finalización, así como la hora de inicio y de finalización y el intervalo entre informes sucesivos.

(Sólo informe de auditoría) Diario

Especifica que el informe se genera a la hora de inicio y, en lo sucesivo, cada 'n' días; 'n' indica el intervalo entre informes sucesivos. Seleccione la fecha de inicio y de finalización, así como la hora de inicio y de finalización y el intervalo entre informes sucesivos.

(Sólo informe de auditoría) Cada semana

Especifica que el informe se genera cada semana en el día seleccionado desde la fecha de inicio. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

(Sólo informe auditoría) Cada mes

Especifica que el informe se genera mensualmente a partir de la fecha de inicio y, en lo sucesivo, cada 'n' meses. 'n' indica el intervalo entre informes sucesivos. Seleccione la fecha de inicio y de finalización, así como la hora de inicio y de finalización y el intervalo entre informes sucesivos.

(Solo informe de auditoría) Ejecute el informe un día específico del mes

Especifica que el informe se genera el día específico del mes que ha seleccionado. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

(Sólo informe de auditoría) Primer lunes

Especifica que el informe se genera en el primer lunes del mes. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

(Solo informe de auditoría) Último día del mes

Especifica que el informe se genera el último día del mes. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

(Solo informe de auditoría) En un día x de la semana y de todos los meses

Especifica que el informe se genera un día y una semana específica de cada mes. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe. Por ejemplo, puede generar un informe el viernes de la tercera semana de cada mes.

5. Haga clic en Enviar.

   La solicitud de informe se ha enviado. En función de la configuración del entorno, la solicitud se ejecuta inmediatamente o se ejecuta después de la aprobación por parte de un administrador.

   Normalmente un administrador del sistema u otro usuario con privilegios de administración de informes deben aprobar una solicitud de informes antes de que el sistema la complete. Es necesaria una aprobación porque algunos informes pueden requerir mucho tiempo o recursos del sistema significativos para ejecutarse. Si su solicitud de informes requiere aprobación, el sistema le envía una alerta de correo electrónico.

   Nota: Active el flujo de trabajo para el entorno si la aprobación es necesaria.

Visualización del informe

Es posible que, en función de la configuración del entorno, un informe no esté disponible para consultarlo hasta que un administrador haya aprobado la solicitud para ese informe. Si su solicitud de informes tiene una aprobación pendiente, el sistema le envía una alerta de correo electrónico. El informe que se desea consultar no aparece en la lista de búsqueda hasta que se aprueba.

Nota: Para poder ver informes en CA Identity Manager mediante el uso de la tarea Ver mis informes, es necesario activar una sesión con cookies de terceros en el explorador.

Siga estos pasos:

1. En la Consola de usuario, vaya a Informes, Tareas de informes y, a continuación, haga clic en Ver mis informes.
2. Busque el informe generado que desea ver.

   Se mostrarán tanto las instancias de los informes generados mediante repetición como los generados a petición.

   Nota: Si el estado del informe es Pendiente/Repetición, el informe no se genera y puede tardar tiempo en completarse la acción.
3. Seleccione el informe que desea ver.
4. (Opcional) Haga clic en Exportar este informe (esquina superior izquierda) para exportar el informe a los formatos siguientes:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003), datos solo
   - Microsoft Excel (97-2003), editable
   - Formato de texto enriquecido (RTF)
   - Valores separados por comas (CSV)
   - XML

Limpieza de la base de datos de auditoría

La base de datos de auditoría puede acumular registros que ya no son necesarios. Para eliminar estos registros, se debe ejecutar el siguiente procedimiento de la base de datos en el directorio db\auditing:

`garbageCollectAuditing12` *`ID de entorno MM/DD/AAAA`*

ID de entorno

Define el nombre del entorno de CA Identity Manager

MM/DD/AAAA

Define la fecha antes de la cual se deberán eliminar los registros de auditoría.

Capítulo 9: Entornos de producción

Esta sección proporciona descripciones funcionales paso a paso para migrar funcionalidades específicas. Es necesario asegurarse de que se utiliza solamente cuando se haya realizado un número limitado de cambios en el entorno de desarrollo y que dichos cambios se hayan entendido bien.

Esta sección contiene los siguientes temas:

Para migrar roles de administrador y definiciones de la tarea

Se pueden personalizar las tareas y los roles de CA Identity Manager para cubrir las necesidades específicas de una compañía. La personalización implica la creación o modificación de tareas y roles de administrador o el uso de una tarea Crear o Modificar para una tarea o un rol de administrador.

Un método alternativo, aunque *no recomendado*, es la modificación de roles y tareas en el archivo roledefinition.xml. Se debe utilizar este método para cambios muy limitados a causa del riesgo de cometer errores al editar.

Este proceso migrará solamente los roles administrativos y las definiciones de tarea. Si los roles estuvieran vinculados a organizaciones, se debe considerar la posibilidad de migrar el entorno de CA Identity Manager entero.

Importante: Si se han cambiado las definiciones de rol o de tarea en el entorno de producción, dichos cambios se perderán cuando se importen las definiciones de rol o de tarea de un entorno de desarrollo. La importación de definiciones de rol y de tarea sobrescribirá las definiciones de rol y de tarea que existan con los mismos nombres.

Para exportar las definiciones de tarea y rol de administrador

Si se han realizado cambios directamente en el archivo roledefinition.xml, éste se puede importar directamente en el entorno de producción. En el caso contrario, para exportar las definiciones de tarea y rol, se debe llevar a cabo lo siguiente:

1. Si tiene un clúster de servidores de políticas, compruebe que se está ejecutando solamente un servidor de políticas.
2. Detenga todos los nodos de CA Identity Manager menos uno.
3. Inicie sesión en la Consola de gestión.
4. Haga clic en los entornos de CA Identity Manager.
5. Seleccione el entorno de CA Identity Manager del cual se deben exportar las definiciones de rol y de tarea.
6. Haga clic en Roles, a continuación, haga clic en Exportar y proporcione un nombre para el archivo.
7. Siga las instrucciones del siguiente procedimiento para importar este archivo.

Para importar las definiciones de tarea y rol de administrador

Siga estos pasos:

1. Copie el archivo creado en el procedimiento anterior en el entorno de producción.
2. Inicie sesión en la Consola de gestión en el entorno de producción.
3. Haga clic en los entornos de CA Identity Manager.
4. Seleccione el entorno de CA Identity Manager adecuado.
5. Haga clic en Roles.
6. Haga clic en Importar y especifique el nombre del archivo XML que genere la exportación.
7. Si estos pasos se han realizado correctamente, inicie todos los nodos de CA Identity Manager y servidores de políticas extra que haya detenido.

   Nota: Si todavía se deben realizar cambios en un entorno de CA Identity Manager, repita el paso 6.

Para verificar la importación de rol y tarea

Para verificar que los roles y las tareas se han importado correctamente, es necesario conectarse a CA Identity Manager como una cuenta de administrador que puede utilizar las siguientes tareas:

- Modificar la función de administración
- Modificación de tareas de administración

Estas tareas se deben ejecutar y se debe verificar que los roles y las tareas reflejan las definiciones de rol recientemente importadas.

Para migrar máscaras de CA Identity Manager

Las máscaras de CA Identity Manager se pueden personalizar para que aporten una apariencia específica a la aplicación. Si se han modificado o creado máscaras nuevas para un conjunto de usuarios, se deben llevar a cabo los siguientes pasos para migrar máscaras del entorno de desarrollo al de producción.

Si se está modificando una máscara, se deben copiar los archivos modificados.

Siga estos pasos:

1. Copie los archivos nuevos y modificados del servidor de desarrollo al de producción, como archivos de imagen, hojas de estilo, archivos de propiedades y la página de consola (index.jsp).
2. Si se están usando varias máscaras, configure la respuesta de SiteMinder.

   Nota: Para obtener más información sobre la importación de varias máscaras, consulte la *Guía de configuración*.

Para verificar la migración de máscaras, es necesario conectarse a la Consola de usuario y comprobar que la máscara aparece correctamente.

Actualización de CA Identity Manager en un entorno de producción

Después de haber migrado CA Identity Manager de desarrollo a producción, puede que sea necesario realizar actualizaciones incrementales. Para migrar la funcionalidad de CA Identity Manager nueva del entorno de desarrollo al entorno de producción, se deben ejecutar los siguientes pasos:

1. Migrar entornos de CA Identity Manager.
2. Copiar el archivo iam_im.ear.
3. Migrar las definiciones del proceso del flujo de trabajo.

Para migrar un entorno de CA Identity Manager

Un entorno de CA Identity Manager se crea desde la Consola de gestión. El entorno de CA Identity Manager incluye un conjunto de definiciones de tarea y rol, definiciones del flujo de trabajo, funciones personalizadas que se crean con las API de CA Identity Manager y un directorio de CA Identity Manager.

Siga estos pasos:

1. Si CA Identity Manager se integra con SiteMinder y tiene un clúster de servidores de políticas, compruebe que se está ejecutando solamente un servidor de políticas.
2. Detenga todos los nodos de CA Identity Manager menos uno.
3. Exporte los entornos de CA Identity Manager de la Consola de gestión en el entorno de desarrollo.
4. Importe los entornos exportados en la Consola de gestión en el entorno de producción.
5. Si CA Identity Manager se integra con SiteMinder, vuelva a proteger los territorios de CA Identity Manager en la interfaz de usuario del servidor de políticas.

   El dominio de la política no se exporta del almacén de políticas cuando se exporta un entorno de CA Identity Manager.
6. Reinicie el servidor de políticas y los nodos de CA Identity Manager que se hayan detenido.

Cuando se migra un entorno de CA Identity Manager, se producen las siguientes actividades:

- Si el mismo objeto existe en las dos ubicaciones, los cambios del servidor de desarrollo sobrescriben los cambios del servidor de producción.
- Si se crean objetos nuevos en el entorno de desarrollo, éstos se agregan al servidor de producción.
- Si se crean objetos nuevos en el servidor de producción, éstos se mantienen.

Para exportar un entorno de CA Identity Manager

Para implementar un entorno de CA Identity Manager en un sistema de producción, exporte el entorno desde un sistema provisional o de desarrollo, e importe ese entorno en el sistema de producción.

Nota: Cuando se importa un entorno previamente exportado, CA Identity Manager muestra un registro en una ventana de estado en la Consola de gestión. Para ver la información de validación e implementación para cada uno de los objetos gestionados y sus atributos en este registro, seleccione Enable Verbose Log Output (Activar resultados de registro detallados) en la página de propiedades del entorno *antes de* exportar el entorno. Tenga en cuenta que si se selecciona el campo Enable Verbose Log Output (Activar resultados de registro detallados), se pueden provocar problemas de rendimiento importantes durante la importación.

Siga estos pasos:

1. Haga clic en Environments (Entornos) en la Consola de gestión.

   La pantalla de entornos de CA Identity Manager se muestra con una lista de entornos de CA Identity Manager.

2. Seleccione el entorno que desea exportar.
3. Haga clic en el botón Exportar.

   Se mostrará la pantalla de descarga de archivos.

4. Guarde el archivo ZIP en una ubicación que sea accesible desde el sistema de producción.
5. Haga clic en Finalizar.

   La información del entorno se exporta a un archivo ZIP que se puede importar en otro entorno.

Para importar un entorno de CA Identity Manager

Después de haber exportado un entorno de CA Identity Manager de un sistema de desarrollo, se puede importar en un sistema de producción.

Siga estos pasos:

1. Haga clic en Environments (Entornos) en la Consola de gestión.

   La pantalla de entornos de CA Identity Manager se muestra con una lista de entornos de CA Identity Manager.

2. Haga clic en el botón Import (Importar).

   Se abrirá la pantalla de importación de entornos.

3. Busque el archivo ZIP que se requiere para importar un entorno.

4. Haga clic en Finalizar.

El entorno se importa en CA Identity Manager.

Para verificar la migración del entorno de CA Identity Manager

Para verificar la migración adecuada del entorno de CA Identity Manager, se debe confirmar que el entorno de CA Identity Manager aparece en la interfaz de usuario del servidor de políticas para el servidor de políticas del entorno de producción.

En la interfaz de usuario del servidor de políticas, se deben verificar los puntos siguientes:

- Los parámetros de configuración del directorio de usuarios de CA Identity Manager son precisos.
- El dominio de CA Identity Manager nuevo existe.
- Los esquemas de autenticación correctos protegen los territorios de CA Identity Manager.

Además, al conectarse a la Consola de gestión, se debe verificar que el entorno de CA Identity Manager aparece cuando se seleccionan los entornos.

Migración de iam_im.ear para JBoss

Se debe volver a implementar el archivo iam_im.ear cada vez que se migre la funcionalidad del entorno de desarrollo al entorno de producción. Al migrar todo el EAR, se garantiza que el entorno de producción es idéntico al entorno de desarrollo.

Siga estos pasos:

1. Copie iam_im.ear de su entorno de desarrollo a una ubicación a la que pueda acceder el entorno de producción.
2. En la copia de iam_im.ear, edite la información de conexión del servidor de políticas, para que refleje el entorno de producción.

   Para realizar este cambio, copie *jboss_home*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml de su entorno de producción en iam_im.ear.
3. Sustituya el archivo iam_im.ear instalado por la copia de iam_im.ear de su entorno de desarrollo del paso 1, como se muestra a continuación:
   a. En el servidor de producción, suprima iam_im.ear:

      cluster_node_jboss_home\server\default\deploy\iam_im.ear

   b. Sustituya los archivos suprimidos por la copia editada de iam_im.ear del entorno de desarrollo.
4. Repita estos pasos para cada nodo del clúster.

Migración de iam_im.ear para WebLogic

Se debe volver a implementar el archivo iam_im.ear cada vez que se migre la funcionalidad del entorno de desarrollo al entorno de producción. Al migrar todo el EAR, se garantiza que el entorno de producción es idéntico al entorno de desarrollo.

Siga estos pasos:

1. Conserve la información de conexión del servidor de políticas

   La información de conexión del servidor de políticas se almacena en el archivo ra.xml en el directorio policyserver_rar/WEB-INF. Copie este archivo en otra ubicación, para que se pueda sustituir en el iam_im.ear antes de volver a implementarlo.
2. Copie iam_im.ear en una ubicación disponible para el servidor de administración de WebLogic.
3. Sustituya la información de conexión del servidor de políticas.

   En iam_im.ear, sustituya el archivo policyserver_rar/WEB-INF/ra.xml por el que se ha conservado en el paso 1.
4. Vuelva a implementar iam_im.ear
   a. Inicie sesión en la consola de WebLogic.
   b. Diríjase a Deployments (Implementaciones), Aplicación, Identity Manager.

En la ficha Implementar, seleccione Deploy (Re-Deploy) Application (Implementar [volver a implementar] la aplicación.

Migración de iam_im.ear para WebSphere

Siga estos pasos:

1. Copie el script *imsInstall.jacl* de *was_im_tools_dir**WebSphere-tools* en el directorio *deployment_manager_dir* *bin* donde:
   - *was_im_tools_dir* es el directorio en el sistema de desarrollo donde se instalan las herramientas de CA Identity Manager para WebSphere.
   - *deployment_manager_dir* es la ubicación donde se instala el gestor de implementación.
2. En el sistema de desarrollo donde se ha configurado la aplicación de CA Identity Manager, copie *was_im_tools_dir* *WebSphere-tools**imsExport.bat* o *imsExport.sh* a *was_home**bin.*
3. En la línea de comandos, navegue a *was_home**bin.*
4. Asegúrese de que el servidor de aplicaciones WebSphere esté en funcionamiento.
5. Exporte la aplicación de CA Identity Manager implementada como se muestra a continuación:

   Para Windows, introduzca este comando:

   `imsExport.bat "path-to-exported-ear"`

   donde *path-to-exported-ear* es la ruta completa y el nombre de archivo que crea la utilidad imsExport.

   Para sistemas de Windows, utilice barras diagonales (/) en lugar de barras inversas (\) cuando especifique la ruta a was_im.ear. Por ejemplo:

   ```
   imsExport.bat "c:/Archivos de programa/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   Para UNIX, introduzca este comando:

   `./wsadmin -f imsExport.jacl -conntype RMI -port 2809 path to exported ear`

   donde *path to exported ear* es la ruta completa que incluye el nombre de archivo del EAR exportado.
6. Copie el archivo EAR exportado de la ubicación del sistema de desarrollo donde se exportó a una ubicación en el sistema en el que se instale el gestor de implementación.
7. Sustituya *was_im_tools_dir*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml por el archivo del entorno de producción.

   El archivo ra.xml contiene la información de conexión del servidor de políticas.

8. En el sistema donde se instale el gestor de implementación, implemente el EAR de Identity Manager:
   a. En la línea de comandos, navegue a:

      deployment_manager_dir \bin.

   b. Asegúrese de que el servidor de aplicaciones WebSphere esté en funcionamiento.

   c. Ejecute el script imsInstall.jacl como se muestra a continuación:

   Nota: El script imsInstall.jacl puede tardar varios minutos ejecutarse.

   Windows:

      wsadmin -f imsInstall.jacl *"path-to-copied-ear" cluster_name*

      donde *path-to-copied-ear* es la ruta completa que incluye el nombre de archivo del EAR de Identity Manager que se ha copiado en el sistema del gestor de implementación.

      Por ejemplo:

      wsadmin -f imsInstall.jacl "c:\Archivos de programa\CA\Identity Manager\WebSphere-tools\was_im.ear" im_cluster

   UNIX:

      ./wsadmin -f imsInstall.jacl *path-to-copied-ear cluster_name*

      donde *path-to-copied-ear* es la ruta completa que incluye el nombre de archivo del EAR de Identity Manager que se ha copiado en el sistema del gestor de implementación.

      Por ejemplo:

      ./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. Si CA Identity Manager se integra con SiteMinder, verifique los siguientes puntos:
   - Los agentes de SiteMinder se pueden conectar al almacén de políticas.
   - El servidor de políticas se puede conectar al almacén de usuarios.
   - Se han creado los dominios de CA Identity Manager.

Migración de las definiciones del proceso del flujo de trabajo

Si se ha utilizado flujo de trabajo en el entorno de desarrollo, exporte las definiciones del flujo de trabajo e impórtelas en el entorno de producción. A continuación, configure el flujo de trabajo en cada uno de los nodos del servidor.

Exportación de las definiciones del proceso

En el sistema del entorno de desarrollo, se exportan las definiciones del proceso de flujo de trabajo.

Siga estos pasos:

1. Asegúrese de que el servidor de aplicaciones esté en funcionamiento.
2. Vaya a *admin_tools*\Workpoint\bin\ y ejecute Archive.bat (para Windows) o Archive.sh (para UNIX) como se muestra a continuación:
   a. En el cuadro de diálogo Importar, seleccione el objeto raíz.
   b. Haga clic en Agregar.
   c. Especifique el nombre del archivo que se debe generar.
   d. Haga clic en Exportar.
   e. Haga clic en Ir.

   admin_tools hace referencia a las herramientas administrativas, que se instalan de forma predeterminada en una de las siguientes ubicaciones:

   - **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
3. Siga las instrucciones de la siguiente sección, para importar las definiciones del proceso (en la página 272).

Importación de las definiciones del proceso

En el sistema de entorno de producción, importar las definiciones del proceso de flujo de trabajo.

Siga estos pasos:

1. Reinicie el servidor de aplicaciones.
2. Opcionalmente, se puede crear una copia de seguridad de las definiciones actuales exportando las definiciones mediante el procedimiento anterior.

3. Vaya a *admin_tools*\Workpoint\bin\ y ejecute el script Archive como se muestra a continuación:

   a. En el cuadro de diálogo Importar, seleccione todos los elementos que se deben importar.

   b. Cuando se solicita el uso del formato nuevo o antiguo, se conserva el formato antiguo.

      El formato nuevo no es compatible con CA Identity Manager.

   c. Proporcione el nombre del archivo que genera la exportación.

   d. Haga clic en Ir.

   admin_tools hace referencia a las herramientas administrativas, que se instalan de forma predeterminada en una de las siguientes ubicaciones:

   - **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Capítulo 10: Registros de CA Identity Manager

Esta sección contiene los siguientes temas:

Cómo realizar el seguimiento de problemas en CA Identity Manager

CA Identity Manager incluye los siguientes métodos para registrar estados y realizar el seguimiento de incidencias:

Tarea Ver tareas enviadas

Muestra el estado de todos los eventos y tareas en un entorno de CA Identity Manager. Los administradores utilizan esta tarea en la Consola de usuario.

Ver tareas enviadas proporciona los siguientes tipos de información:

- La lista de eventos y tareas que tienen lugar en el entorno.
- La lista de atributos asociados a un evento.
- Eventos correctos y erróneos.
- Eventos que están en estado pendiente o detenido.
- Eventos rechazados, que incluyen el motivo del rechazo.
- Estado de la sincronización de cuentas.
- Estado de la sincronización de políticas de identidad.
- Información de aprovisionamiento (cuando el aprovisionamiento está activado).

Registros del servidor de aplicaciones

Muestran información sobre todos los componentes de una instalación de CA Identity Manager, así como detalles de todas las operaciones de CA Identity Manager.

La ubicación y el tipo del archivo de registro depende de cuáles de los siguientes tipos de servidores de aplicaciones se estén utilizando:

- WebLogic: la información de CA Identity Manager se escribe en Salida estándar. De forma predeterminada, Salida estándar es la ventana de la consola en la cual la instancia del servidor se está ejecutando.
- JBoss: la información de CA Identity Manager se escribe en la ventana de la consola donde se está ejecutando la instancia del servidor y en *jboss_home*\server\log\server.log
- WebSphere: la información de CA Identity Manager se escribe en la ventana de la consola donde se está ejecutando la instancia del servidor y en *was_home*\AppServer\logs*server_name*\SystemOut

Consulte la documentación de su servidor de aplicaciones para obtener más información.

Archivo de registro del servidor del directorio

Contiene información acerca de la actividad que se produce en el directorio de usuarios.

El tipo de información que se registra y la ubicación del archivo de registro dependen del tipo de servidor de directorio que se esté utilizando. Consulte la documentación del servidor del directorio para obtener más información.

Archivo de registro del servidor de políticas

Muestra la siguiente información cuando CA Identity Manager se integra con SiteMinder:

- Incidencias de conexión de SiteMinder
- Incidencias de autenticación de SiteMinder
- La información acerca de objetos gestionados de CA Identity Manager en el almacén de políticas de SiteMinder.
- Evaluación de la política de contraseñas

Para obtener información acerca de la configuración de registros de SiteMinder, consulte *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

Generador de perfiles del servidor de políticas

Si CA Identity Manager se integra con SiteMinder, permite encontrar diagnósticos del servidor de política internos y funciones de procesamiento, incluidas las funciones relacionadas con CA Identity Manager.

Para obtener más información, consulte Cómo realizar el seguimiento de componentes y campos de datos (en la página 277).

Archivos de registro del agente web

Si CA Identity Manager se integra con SiteMinder, los agentes web escriben información en los dos siguientes registros:

- Archivo de registro de errores: contiene los errores de nivel operativo y del programa, por ejemplo, si el agente web no se puede comunicar con servidor de políticas.
- Archivo de registro de seguimiento: contiene los mensajes de advertencia e informativos, como los mensajes de seguimiento y los mensajes de estado del flujo. También incluye datos como los detalles del encabezado y las variables de cookie.

Nota: Para obtener más información sobre los archivos de registro del agente web, consulte *CA SiteMinder Web Access Manager Web Agent Configuration Guide*.

Cómo realizar el seguimiento de componentes y campos de datos

Cuando CA Identity Manager se integra con SiteMinder, se puede usar el generador de perfiles del servidor de políticas de SiteMinder para hacer un seguimiento de los componentes y campos de datos en las extensiones de CA Identity Manager para el servidor de políticas. El generador de perfiles permite configurar filtros para la salida del seguimiento de modo que solamente se capturen los valores específicos para un componente o campo de datos.

Nota: Para obtener instrucciones sobre el uso del generador de perfiles del servidor de políticas, consulte *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

Se puede activar el seguimiento para los siguientes componentes:

Function_Begin_End

Proporciona instrucciones de seguimiento de bajo nivel cuando se ejecutan ciertos métodos en las extensiones de CA Identity Manager para el servidor de políticas.

IM_Error

Realiza un seguimiento de los errores de tiempo de ejecución en las extensiones de CA Identity Manager para el servidor de políticas de SiteMinder.

IM_Info

Proporciona información general sobre el seguimiento de las extensiones de CA Identity Manager.

IM_Internal

Realiza un seguimiento de la información general acerca de operaciones de CA Identity Manager internas.

IM_MetaData

Proporciona información de seguimiento cuando CA Identity Manager procesa los metadatos del directorio.

IM_RDB_Sql

Proporciona información de seguimiento para bases de datos relacionales.

IM_LDAP_Provider

Proporciona información de seguimiento para directorios LDAP.

IM_RuleParser

Realiza un seguimiento del proceso de análisis y evaluaciones de miembros, propietarios y políticas de administración, que se definen en un archivo XML que se interpreta en el tiempo de ejecución.

IM_RuleEvaluation

Realiza un seguimiento de las evaluaciones de miembros, administradores, propietarios y reglas del ámbito.

IM_MemberPolicy

Realiza un seguimiento de la evaluación de políticas de miembros, incluidas la pertenencia y el ámbito.

IM_AdminPolicy

Realiza un seguimiento de la evaluación de políticas de administración.

IM_OwnerPolicy

Realiza un seguimiento de la evaluación de políticas de propietario.

IM_RoleMembership

Realiza un seguimiento de la información relativa a la pertenencia a roles, como la lista de roles que tiene un usuario y la lista de miembros de un rol determinado.

IM_RoleAdmins

Realiza un seguimiento de la información relativa a la administración de roles, como la lista de roles que puede administrar un usuario y la lista de administradores de un rol determinado.

IM_RoleOwners

Realiza un seguimiento de la información relativa a la propiedad de roles, como la lista de roles que posee un usuario y la lista de propietarios de un rol determinado.

IM_PolicyServerRules

Realiza un seguimiento de la evaluación de reglas de miembros, como RoleMember, RoleAdmin, RoleOwner que el servidor de políticas haya resuelto y reglas de ámbito, como las reglas Todo y AccessTaskFilter para AccessTasks.

IM_LLSDK_Command

Realiza un seguimiento de la comunicación entre el SDK de CA Identity Manager interno y el servidor de políticas. El soporte técnico utiliza este componente de seguimiento.

IM_LLSDK_Message

Realiza un seguimiento de los mensajes que envía explícitamente el código Java al servidor de políticas del SDK de CA Identity Manager interno. El soporte técnico utiliza este componente de seguimiento.

IM_IdentityPolicy

Realiza un seguimiento de la evaluación y la aplicación de las políticas de identidad.

IM_PasswordPolicy

Realiza un seguimiento de la evaluación de políticas de contraseña.

IM_Version

Proporciona información acerca de la versión de CA Identity Manager.

IM_CertificationPolicy

Realiza un seguimiento de la evaluación de políticas de certificación.

IM_InMemoryEval

Realiza un seguimiento del procesamiento de políticas de CA Identity Manager, incluidas las políticas de identidad, miembros, administración y propietarios. El soporte técnico utiliza este componente de seguimiento.

IM_InMemoryEvalDetail

Proporciona detalles adicionales sobre el procesamiento de las políticas de CA Identity Manager, incluidas las políticas de identidad, miembros, administración y propietarios. El soporte técnico utiliza este componente de seguimiento.

Los campos de datos para los cuales se puede configurar seguimiento se muestran en *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

Capítulo 11: Protección de CA Identity Manager

Esta sección contiene los siguientes temas:

Seguridad de la Consola de usuario

La Consola de usuario es la interfaz de usuario que permite a los administradores gestionar objetos como usuarios, grupos y organizaciones en un entorno de CA Identity Manager. Estos objetos se asignan a un conjunto de roles y tareas asociados. Cuando un administrador inicia sesión en la Consola de usuario, las tareas relacionadas con el administrador se muestran en ese entorno.

De forma predeterminada, CA Identity Manager protege el acceso a la Consola de usuario con la autenticación nativa. Los administradores de CA Identity Manager introducen un nombre de usuario y contraseña válidos para conectarse a un entorno de CA Identity Manager. CA Identity Manager autentica el nombre y la contraseña con respecto al almacén de usuarios que gestiona CA Identity Manager.

Si CA Identity Manager se integra con SiteMinder, CA Identity Manager utiliza *automáticamente* la autenticación básica de SiteMinder para proteger el entorno. No es necesario realizar ninguna configuración adicional para utilizar la autenticación básica. Se pueden configurar métodos de autenticación avanzados mediante la interfaz de usuario administrativa de SiteMinder.

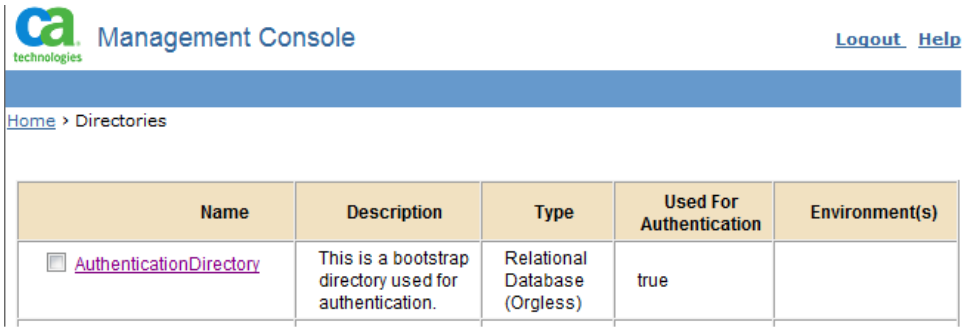
Nota: Para obtener más información, consulte la *Guía de configuración del servidor de políticas del gestor de acceso web de CA SiteMinder*.

Seguridad de la Consola de gestión

La Consola de gestión permite a los administradores crear y gestionar entornos y directorios de CA Identity Manager. Los administradores también pueden usar la Consola de gestión para configurar la funcionalidad personalizada para un entorno.

La instalación de CA Identity Manager incluye una opción de asegurar la Consola de gestión. Esta opción está seleccionada de forma predeterminada. Durante la instalación, se especifican las credenciales que CA Identity Manager utiliza para autenticar un administrador que puede acceder a la Consola de gestión. CA Identity Manager crea un usuario con las credenciales que se proporcionen en un directorio de bootstrap denominado AuthenticationDirectory. Este directorio se puede ver en la Consola de gestión.

Nota: No se puede utilizar la seguridad nativa para proteger la Consola de gestión cuando CA Identity Manager se integra con CA SiteMinder.



Adición de administradores de la Consola de gestión adicionales

De forma predeterminada, una Consola de gestión que protege la seguridad de CA Identity Manager nativa tiene una cuenta de administrador, que se crea en un directorio de CA Identity Manager nuevo durante la instalación.

Para agregar administradores adicionales, se especifica un directorio de CA Identity Manager que contenga usuarios que deban acceder a la Consola de gestión. El uso de un directorio existente permite conceder acceso a la Consola de gestión a usuarios de la organización sin tener que crear cuentas nuevas.

Se puede especificar solamente un directorio para la autenticación. No se puede suprimir un directorio mientras se está configurando para la autenticación.

Siga estos pasos:

1. Inicie sesión en la Consola de gestión con las credenciales de usuario proporcionadas durante la instalación.
2. Abra Directorios y haga clic en el directorio que contenga los usuarios que requieran acceso a la Consola de gestión.
3. Haga clic en Update Authentication.
4. Seleccione la opción Used for Authentication.
5. Introduzca el nombre de inicio de sesión para el primer usuario y haga clic en Agregar.
6. Continúe agregando usuarios que requieran acceso a la Consola de gestión hasta que todos los usuarios se hayan agregado. A continuación, haga clic en Guardar.

   Los usuarios especificados ahora podrán utilizar su nombre de usuario y contraseña para acceder a la Consola de gestión.

Desactivación de la seguridad nativa para la Consola de gestión

Si se activó la seguridad nativa para la Consola de gestión y ahora se desea utilizar una aplicación diferente para protegerlo, se debe desactivar la seguridad nativa antes de implementar otro método de seguridad.

Siga estos pasos:

1. Desactive la seguridad nativa para la Consola de gestión en el archivo web.xml como se muestra a continuación:
   a. Abra *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml en un editor de texto.
   b. Establezca el valor del parámetro Enable para ManagementConsoleAuthFilter como false como se muestra a continuación:
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-class>com.netegrity.ims.manage.filter.ManagementConsoleAuthFilter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>false</param-value>
   </init-param>
   </filter>
   ```
   c. Guarde el archivo web.xml.
2. Reinicie el servidor de CA Identity Manager.

   La seguridad nativa ya no protege la Consola de gestión.

Uso de SiteMinder para asegurar la Consola de gestión

Para proteger la Consola de gestión al principio, se puede crear una política de SiteMinder.

Una política de SiteMinder identifica un recurso que se desea proteger, como la Consola de gestión, y permite que un conjunto de usuarios accedan a dicho recurso.

Siga estos pasos:

1. Desactive la seguridad nativa (en la página 284) de la Consola de gestión
2. Inicie sesión en una de las siguientes interfaces como administrador con privilegios del dominio:
   - Para CA SiteMinder r12 o superior, inicie sesión en la interfaz de usuario administrativa.
   - Para CA SiteMinder 6.0 SP*x*, inicie sesión en la interfaz de usuario del servidor de políticas.

   Nota: Para obtener información sobre el uso de estas interfaces, consulte la documentación de la versión de SiteMinder que esté utilizando.
3. Busque el dominio de la política para el entorno de CA Identity Manager adecuado.

   Este dominio se crea automáticamente cuando CA Identity Manager se integra con SiteMinder. El nombre del dominio tiene el siguiente formato:

   *Identity Manager-environment*Domain

   En este formato, *Identity Manager-environment* especifica el nombre del entorno que se está modificando. Por ejemplo, si el nombre es *employees*, el nombre del dominio es *employees*Domain.
4. Cree un territorio con el siguiente filtro de recursos:

   /iam/immanage/
5. Cree una regla para el territorio. Especifique un asterisco (*) como filtro para proteger todas las páginas de la Consola de gestión.
6. Cree una nueva política y asóciela con la regla creada en el paso anterior.

   Asegúrese de asociar los usuarios que puedan acceder a la Consola de gestión con la política.
7. Reinicie el servidor de aplicaciones.

Protección de un entorno existente después de actualización

Después de actualizar a CA Identity Manager 12.6 o posterior, se puede proteger la Consola de gestión mediante la seguridad nativa.

Nota: No se puede utilizar la seguridad nativa de CA Identity Manager para proteger la Consola de gestión cuando CA Identity Manager se integra con CA SiteMinder.

Siga estos pasos:

1. Active la seguridad nativa para la Consola de gestión en el archivo web.xml como se muestra a continuación:

   a. Abra *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml en un editor de texto.

   b. Establezca el valor del parámetro Enable para ManagementConsoleAuthFilter como true como se muestra a continuación:

   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-class>com.netegrity.ims.manage.filter.ManagementCon
   soleAuthFilter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>true</param-value>
   </init-param>
   </filter>
   ```

   c. Guarde el archivo web.xml.

2. Cree la tabla IM_AUTH_USER en el almacén de objetos de CA Identity Manager.

   La tabla IM_AUTH_USER almacena información acerca de los administradores de la Consola de gestión.

   a. Navegue a CA\Identity Manager\IAM Suite\Identity Manager\tools\db\objectstore.

   b. Ejecute uno de los siguientes scripts con respecto al almacén de objetos:

      - sql_objectstore.sql
      - oracle_objectstore.sql

   Nota: Para obtener información acerca de la ejecución de un script con respecto a una base de datos existente, consulte la documentación del distribuidor de esa base de datos.

3. Utilice la herramienta de contraseñas para cifrar la contraseña de usuario.

   La herramienta de contraseña se instala con las herramientas de CA Identity Manager en la ubicación siguiente:

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

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   Herramienta de contraseña

   Ejecute la herramienta de contraseña mediante el comando siguiente:
   `pwdtools -JSAFE -p anypassword`

   La opción JSAFE cifra un valor de texto sin formato mediante el algoritmo PBE.

1. Inserte la información de usuario bootstrap en la tabla IM_AUTH_USER. Especifique valores para todas las columnas en la tabla IM_AUTH_USER.

   Por ejemplo:

   USER_NAME: admin1

   PASSWORD: *anypassword*

   DISABLED: 0

   ID:1

2. Reinicie el servidor de CA Identity Manager.

   La seguridad nativa protege la Consola de gestión.

Protección de ataques CSRF

CA Identity Manager se ha mejorado para reforzar la resistencia frente a ataques de falsificación de solicitud entre sitios (CSRF). De forma predeterminada, la mejora está desactivada en CA Identity Manager.

Para activar la mejora, se deben llevar a cabo los siguientes pasos:

1. Abra el archivo web.xml que se encuentra en la siguiente ubicación:

   `application-server/iam_im.ear/user_console.war/WEB-INF`

2. Busque el elemento <context-param> con <param-name> csrf-prevention-on.
3. Establezca <param-value> como true.
4. Reinicie el servidor de aplicaciones.

Capítulo 12: Integración de CA SiteMinder

Esta sección contiene los siguientes temas:

SiteMinder y CA Identity Manager

Cuando CA Identity Manager se integra con CA SiteMinder, CA SiteMinder puede agregar la siguiente funcionalidad a un entorno de CA Identity Manager:

Autenticación avanzada

CA Identity Manager incluye autenticación nativa para entornos de CA Identity Manager de forma predeterminada. Los administradores de CA Identity Manager introducen un nombre de usuario y contraseña válidos para conectarse a un entorno de CA Identity Manager. CA Identity Manager autentica el nombre y la contraseña con respecto al almacén de usuarios que gestiona CA Identity Manager.

Cuando CA Identity Manager se integra con CA SiteMinder, CA Identity Manager utiliza la autenticación básica de CA SiteMinder para proteger el entorno. Cuando se crea un entorno de CA Identity Manager, se crean un dominio de la política y un esquema de autenticación en CA SiteMinder para proteger dicho entorno.

Cuando CA Identity Manager se integra con CA SiteMinder, también se puede utilizar la autenticación de SiteMinder para proteger la Consola de gestión.

Tareas y roles de acceso

Los roles de acceso permiten a los administradores de CA Identity Manager asignar privilegios en aplicaciones que CA SiteMinder proteja. Los roles de acceso representan una única acción que puede realizar un usuario en una aplicación empresarial, como generar una orden de compra en una aplicación de contabilidad.

Asignación de directorios

Posiblemente, un administrador deberá gestionar usuarios cuyos perfiles existan en un almacén de usuarios diferente de aquél que se utiliza para autenticar al administrador. Al iniciar sesión en el entorno de CA Identity Manager, el administrador se autentica mediante un directorio y un directorio diferente para autorizar al administrador a gestionar usuarios.

Cuando CA Identity Manager se integra con CA SiteMinder, se puede configurar un entorno de CA Identity Manager para utilizar directorios diferentes para la autenticación y la autorización.

Máscaras para conjuntos diferentes de usuarios

Una máscara cambia la apariencia de la Consola de usuario. Cuando CA Identity Manager se integra con CA SiteMinder, se pueden activar conjuntos diferentes de usuarios para que vean máscaras distintas. Para lograr este cambio, se utiliza una respuesta de SiteMinder para asociar una máscara a un conjunto de usuarios. La respuesta se equipara con una regla en una política, que se asocia con un conjunto de usuarios. Cuando la regla se desencadena, activa la respuesta para transferir información acerca de la máscara a CA Identity Manager, para crear la Consola de usuario.

Nota: Para obtener más información, consulte la *Guía de diseño de la Consola de usuario*.

Preferencias de configuración regional para un entorno localizado

Cuando CA Identity Manager se integra con CA SiteMinder, se puede definir la preferencia de configuración regional para un usuario mediante un encabezado HTTP de imlanguage. En el servidor de políticas de SiteMinder, se establece este encabezado dentro de una respuesta de SiteMinder y se especifica un atributo de usuario como valor del encabezado. Este encabezado de imlanguage actúa como la preferencia de configuración regional de mayor prioridad para un usuario.

Nota: Para obtener más información, consulte la *Guía de diseño de la Consola de usuario*.

Más información:

Recolección de credenciales de usuario mediante un esquema de autenticación personalizado (en la página 348)

Cómo se protegen los recursos

La autenticación avanzada requiere que se utilice un servidor de políticas de SiteMinder en la implementación. El servidor de aplicaciones que hospeda el servidor de CA Identity Manager está en un entorno operativo diferente del servidor web. Para proporcionar servicios de reenvío, el servidor web requiere:

- Un complemento proporcionado por el distribuidor del servidor de aplicaciones.
- Un agente de SiteMinder para proteger los recursos de CA Identity Manager, como la Consola de usuario, el autorregistro y la función Contraseña olvidada.

El agente web controla el acceso de usuarios que soliciten recursos de CA Identity Manager. Cuando se autentica y autoriza a los usuarios, el agente web permite al servidor Web procesar las solicitudes.

Cuando el servidor web recibe la solicitud, el complemento del servidor de aplicaciones lo reenvía al servidor de aplicaciones que hospeda al servidor de CA Identity Manager.

El agente web protege los recursos de CA Identity Manager que se exponen a los usuarios y administradores.

Descripción general de la integración de SiteMinder y CA Identity Manager

Cuando el administrador de políticas y el administrador de identidades funcionan juntos para integrar SiteMinder en una instalación de CA Identity Manager existente, la arquitectura de CA Identity Manager se expande para incluir los siguientes componentes:

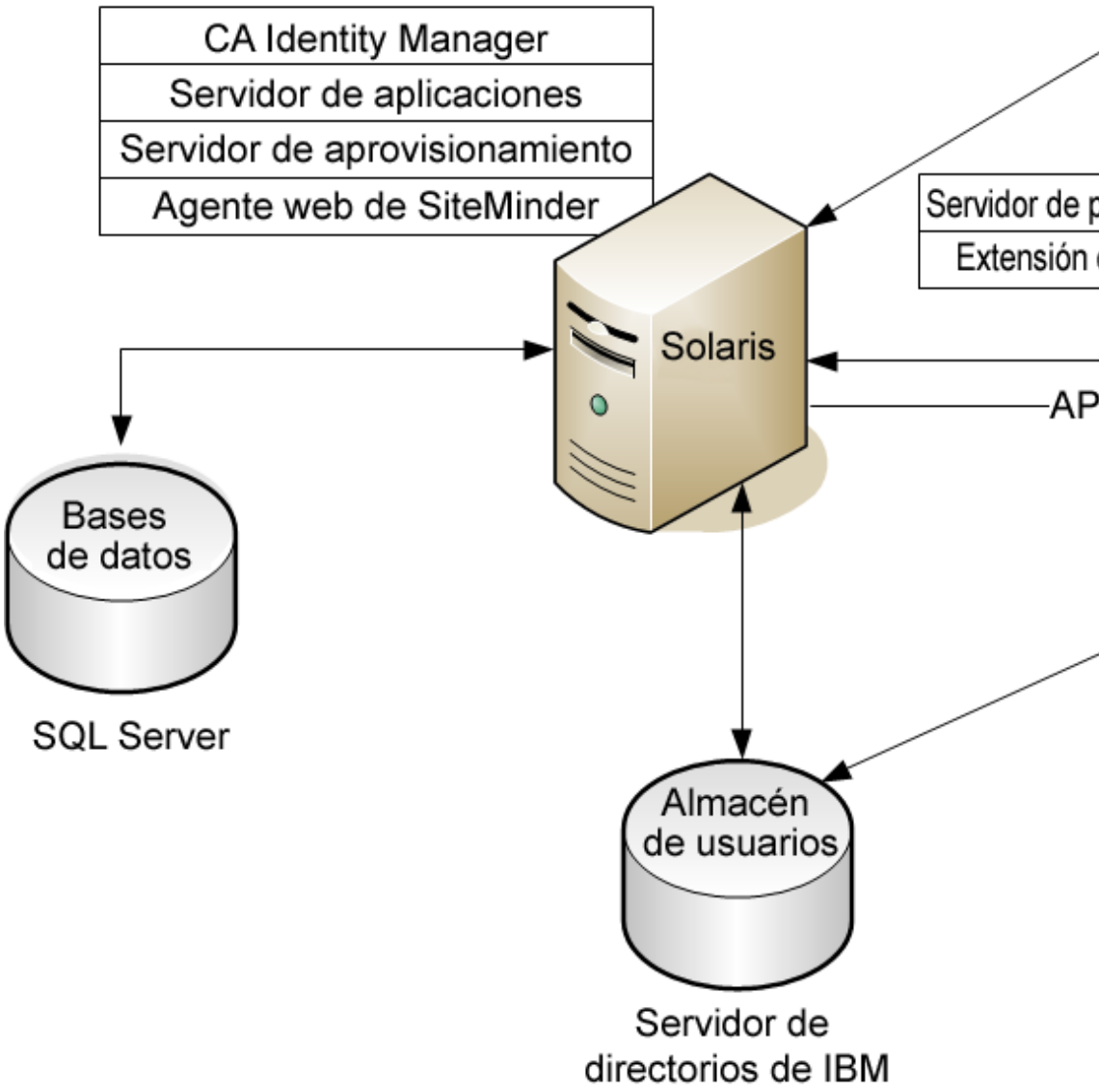
Agente web de SiteMinder

Protege el servidor de CA Identity Manager. El agente Web se instala en el sistema con el servidor de CA Identity Manager.

Servidor de políticas de SiteMinder

Proporciona autenticación avanzada y autorización para CA Identity Manager.

La siguiente ilustración es un ejemplo de una instalación de CA Identity Manager con un servidor de políticas de SiteMinder y agente Web:

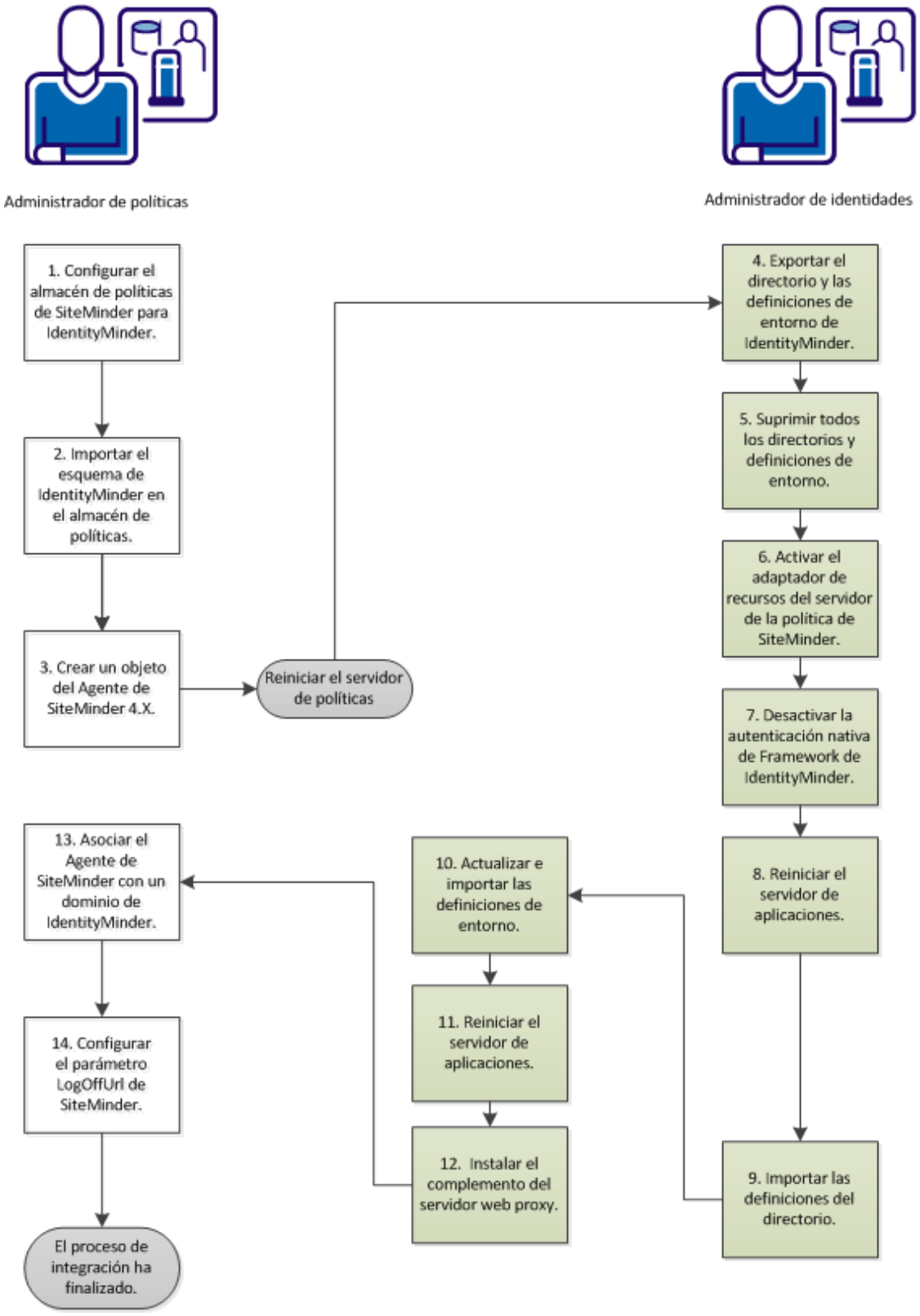

CA Identity Manager
Servidor de aplicaciones
Servidor de aprovisionamiento
Agente web de SiteMinder
Solaris
Bases de datos
SQL Server
Almacén de usuarios
Servidor de directorios de IBM

Nota: Los componentes están instalados en plataformas diferentes como ejemplo. Sin embargo, se pueden elegir otras plataformas. Las bases de datos de CA Identity Manager están en Microsoft SQL Server y el almacén de usuarios está en el servidor de directorios de IBM. El almacén de políticas de SiteMinder está en AD LDS en Windows.

Para completar este proceso se requieren dos roles: de administrador de identidades de CA Identity Manager y de administrador de políticas de SiteMinder. En algunas organizaciones, una persona reúne ambos roles. Cuando hay dos personas implicadas, es necesario que se dé una estrecha colaboración para completar los procedimientos de este escenario. El administrador de políticas empieza y termina el proceso, y el administrador de identidades realiza todos los pasos intermedios.

Importante: En el caso de instalaciones de CA Identity Manager a partir de la versión 12.5 SP7, se necesitan archivos de política jurisdiccional de fuerza ilimitada de la Extensión Criptográfica Java (bibliotecas de JCE). Estas bibliotecas se descargan del sitio web de Oracle. Se deben cargar en la siguiente carpeta: <Java_path>\<jdk_version>\jre\lib\security\.

El siguiente diagrama ilustra el proceso completo de la integración de SiteMinder en CA Identity Manager:


Administrador de políticas
Administrador de identidades
1. Configurar el almacén de políticas de SiteMinder para IdentityMinder.
2. Importar el esquema de IdentityMinder en el almacén de políticas.
3. Crear un objeto del Agente de SiteMinder 4.X.
Reiniciar el servidor de políticas
4. Exportar el directorio y las definiciones de entorno de IdentityMinder.
5. Suprimir todos los directorios y definiciones de entorno.
6. Activar el adaptador de recursos del servidor de la política de SiteMinder.
7. Desactivar la autenticación nativa de Framework de IdentityMinder.
8. Reiniciar el servidor de aplicaciones.
9. Importar las definiciones del directorio.
10. Actualizar e importar las definiciones de entorno.
11. Reiniciar el servidor de aplicaciones.
12. Instalar el complemento del servidor web proxy.
13. Asociar el Agente de SiteMinder con un dominio de IdentityMinder.
14. Configurar el parámetro LogOffUrl de SiteMinder.
El proceso de integración ha finalizado.

Siga estos pasos:

1. Configure el almacén de políticas de SiteMinder para CA Identity Manager. (en la página 299)
2. Importe el esquema de CA Identity Manager en el almacén de políticas. (en la página 305)
3. Cree un objeto agente de SiteMinder 4.X. (en la página 305)
4. Exporte los entornos y directorios de CA Identity Manager. (en la página 307)
5. Suprima todas las definiciones del entorno y el directorio. (en la página 308)
6. Active el adaptador de recursos del servidor de políticas de SiteMinder. (en la página 309)
7. Desactive el filtro de autenticación del marco de trabajo de CA Identity Manager nativo. (en la página 310)
8. Reinicie el servidor de aplicaciones. (en la página 311)
9. Configure un origen de datos para SiteMinder. (en la página 311)
10. Importe las definiciones del directorio. (en la página 312)
11. Actualice e importe las definiciones del entorno. (en la página 313)
12. Reinicie el servidor de aplicaciones. (en la página 311)
13. Instale el complemento del servidor proxy web. (en la página 313)
14. Asocie el agente de SiteMinder con un dominio de CA Identity Manager. (en la página 334)
15. Configure el parámetro LogOffUrl de SiteMinder. (en la página 334)

Configuración del almacén de políticas de SiteMinder para CA Identity Manager

El administrador de políticas usa las herramientas administrativas de CA Identity Manager para acceder a los scripts de SQL o texto de esquema de LDAP para agregar el esquema de IMS al almacén de políticas. El administrador de identidades habrá instalado estas herramientas en la carpeta de herramientas de administración. Lleve a cabo *uno* los siguientes procedimientos para configurar el almacén de políticas:

Configuración de una base de datos relacional (en la página 299)

Configuración del servidor de directorios de sistemas Sun Java o IBM (en la página 300)

Configuración de Microsoft Active Directory (en la página 300)

Configuración de Microsoft ADAM (en la página 301)

Configuración del servidor de CA Directory (en la página 302)

Configuración del servidor de Novell eDirectory (en la página 303)

Configuración del directorio de Internet de Oracle (OID) (en la página 304)

Configuración de una base de datos relacional

Después de la configuración, se puede utilizar la base de datos relacional como almacén de políticas de SiteMinder.

Siga estos pasos:

1. Configure la base de datos como almacén de políticas de SiteMinder compatible.

   Nota: Para obtener instrucciones de configuración, consulte *SiteMinder Policy Server Installation Guide*.

2. Ejecute el script adecuado para su base de datos:

   - **SQL:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   Las rutas anteriores son las ubicaciones de la instalación predeterminadas. La ubicación de la instalación puede ser diferente.

Configuración del servidor de directorios de sistemas Sun Java o IBM

Para configurar un servidor de directorios de Java o IBM se aplica el archivo de esquema adecuado.

Siga estos pasos:

1. Configure el directorio como almacén de políticas de SiteMinder compatible.

   Nota: Para obtener instrucciones de configuración, consulte *CA SiteMinder Policy Server Installation Guide*.

2. Agregue el archivo de esquema LDIF adecuado al directorio. La ubicación predeterminada de Windows para los archivos LDIF es C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas.

   Adición de los siguientes archivos de esquema para su directorio:

   - **Servidor de directorios de IBM:**

     IBMDirectoryServer\V3.identityminder8

   - **Servidor de directorios de sistemas Sun Java (iPlanet):**

     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

Configuración de Microsoft Active Directory

Para configurar un almacén de políticas de Microsoft Active Directory, se debe aplicar el script activedirectory_ims8.ldif.

Siga estos pasos:

1. Configure el directorio como almacén de políticas de SiteMinder compatible.

   Nota: Para obtener instrucciones de configuración, consulte *CA SiteMinder Policy Server Installation Guide*.

2. Modifique el archivo de esquema activedirectory_ims8.ldif como se muestra a continuación:

   a. En un editor de texto, abra el archivo activedirectory_ims8.ldif. La ubicación predeterminada de Windows es:

      C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Sustituya todas las instancias de {root} por la organización raíz del directorio.

      La organización raíz debe coincidir con la organización raíz que se especificó cuando se configuró el almacén de políticas en la Consola de gestión del servidor de políticas.

Por ejemplo, si la raíz es dc=myorg,dc=com, sustituya
dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root} por dn:
CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com

c. Guarde el archivo.

3. Agregue el archivo de esquema como se describe en la documentación de su directorio.

Configuración de Microsoft ADAM

Para configurar un almacén de políticas de Microsoft ADAM, se debe aplicar el script adam_ims8.ldif.

Siga estos pasos:

1. Configure el directorio como almacén de políticas de SiteMinder compatible.

   Nota: Para obtener instrucciones de configuración, consulte *CA SiteMinder Policy Server Installation Guide*.

   Anote el valor de CN (guid).

2. Modifique el archivo de esquema adam_ims8.ldif como se muestra a continuación:

   a. Abra el archivo adam_ims8.ldif\.ldif en un editor de texto. La ubicación predeterminada de Windows es:

      C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Sustituya todas las referencias de cn={guid} por la cadena encontrada cuando se configuró el almacén de políticas de SiteMinder en el paso 1 de este procedimiento.

      Por ejemplo, si la cadena de guid es CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}, sustituya todas las referencias de cn={guid} por CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}.

   c. Guarde el archivo.

3. Agregue el archivo de esquema como se describe en la documentación de su directorio.

Configuración del servidor de CA Directory

Para configurar un servidor de CA Directory se debe crear un archivo de esquema personalizado. En los siguientes pasos, *dxserver_home* es el directorio en el que está instalado CA Directory. La ubicación de origen predeterminada para este archivo en Windows es C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory.

Siga estos pasos:

1. Configure el directorio como almacén de políticas de SiteMinder compatible.

   Nota: Para obtener instrucciones de configuración, consulte *CA SiteMinder Policy Server Installation Guide*.

2. Copie etrust_ims8.dxc en *dxserver_home*\config\schema.

3. Cree un archivo de configuración de esquema personalizado como se muestra a continuación:

   a. Copie *dxserver_home*\config\schema\default.dxg en *dxserver_home*\config\schema*company_name*-schema.dxg.

   b. Edite el archivo *dxserver_home*\config\schema*company_name*-schema.dxg agregando las líneas siguientes al final del archivo:

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. Edite el archivo *dxserver_home*\bin\schema.txt agregando el contenido de etrust_ims_schema.txt al final del archivo. La ubicación de origen predeterminada para este archivo en Windows es C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory.

5. Cree un archivo de configuración de límites personalizado como se muestra a continuación:

   a. Copie *dxserver_home*\config\limits\default.dxc en *dxserver_home*\config\limits*company_name*-limits.dxc.

   b. Aumentar el límite del tamaño predeterminado hasta 5000 en el archivo *dxserver_home*\config\limits*company_name*-limits.dxc como se muestra a continuación:

   ```
   set max-op-size=5000
   ```

   Nota: La actualización de CA Directory sobrescribe el archivo limits.dxc. Por lo tanto, es necesario asegurarse de que se restablece max-op-size a 5000 después de que la actualización se complete.

6. Edite *dxserver_home*\config\servers*dsa_name*.dxi como se muestra a continuación:

```
# schema
source "company_name-schema.dxg";

#service limits
source "company_name-limits.dxc";
```

donde *dsa_name* es el nombre del DSA que utiliza los archivos de configuración personalizados.

7. Ejecute la utilidad dxsyntax.
8. Detenga y reinicie el DSA como usuario de dsa para que los cambios del esquema se apliquen, como se muestra a continuación:

```
dxserver stop dsa_name
dxserver start dsa_name
```

Configuración del servidor de Novell eDirectory

Para configurar un almacén de políticas de servidor de Novell eDirectory, aplica el script novell_ims8.ldif.

Siga estos pasos:

1. Configure el directorio como almacén de políticas de SiteMinder compatible.

   Nota: Para obtener instrucciones de configuración, consulte *CA SiteMinder Policy Server Installation Guide*.

2. Busque el nombre destacado (DN) de NCPServer para su servidor de Novell eDirectory introduciendo la siguiente información en una ventana de comandos en el sistema donde se instala el servidor de políticas:

```
ldapsearch -h hostname -p port -b container -s sub
-D admin_login -w password objectClass=ncpServer dn
```

   Por ejemplo:

```
ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D
"cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn
```

3. Abra el archivo novell_ims8.ldif.
4. Sustituya todas las variables de NCPServer por el valor encontrado en el paso 2.

   La ubicación predeterminada para novell_ims8.ldif en Windows es:

   C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\NovelleDirectory

   Por ejemplo, si el valor de DN es cn=servername,o=servercontainer, se deberían sustituir todas las instancias de *NCPServer* por cn=servername,o=servercontainer.

5. Actualice el servidor de eDirectory con el archivo novell_ims8.ldif.

   Consulte la documentación de Novell eDirectory para obtener instrucciones.

Configuración del directorio de Internet de Oracle (OID)

Para configurar un directorio de Internet de Oracle se actualiza el archivo LDIF de oracleoid.

Siga estos pasos:

1. Configure el directorio como almacén de políticas de SiteMinder compatible.

   Nota: Para obtener instrucciones de configuración, consulte *CA SiteMinder Policy Server Installation Guide*.

2. Actualice el servidor del directorio de Internet de Oracle con el archivo oracleoid_ims8.ldif. La ubicación de la instalación predeterminada para este archivo en Windows es:

   install_path\policystore-schemas\OracleOID\

   Consulte la documentación del directorio de Internet de Oracle para obtener instrucciones.

Verificación del almacén de políticas

Para verificar el almacén de políticas, confirme los puntos siguientes:

- El registro del servidor de políticas no contiene una sección de advertencias que empieza con el código siguiente:
  `*** IMS NO SCHEMA BEGIN`

  Esta advertencia aparece solamente si se han instalado las extensiones para el servidor de políticas de SiteMinder, pero no se ha extendido el esquema del almacén de políticas.

- Los objetos de CA Identity Manager existen en el directorio o la base de datos del almacén de políticas. Los objetos de CA Identity Manager empiezan por el prefijo ims.

Importación del esquema de CA Identity Manager en el almacén de políticas

El administrador de políticas importa el esquema de CA Identity Manager en el almacén de políticas. Esta tarea permite a CA Identity Manager crear, actualizar, y suprimir objetos de política. Algunos ejemplos son objetos del directorio, territorios, dominios, reglas, políticas y los objetos de política que activan tareas y roles de acceso.

Siga estos pasos:

1. En el servidor de políticas de SiteMinder, apague el servicio de servidor de políticas.
2. Ejecute el instalador de CA Identity Manager para la versión que se esté utilizando.
3. Cuando se pregunte qué componentes instalar, seleccione las extensiones para SiteMinder (si SiteMinder está instalado de forma local).
4. Verifique que el servicio del servidor de políticas se reinicia antes de continuar.

Creación de un objeto agente de SiteMinder 4.X

El administrador de políticas crea un agente Web de SiteMinder 4.x. Esta tarea activa la comunicación entre SiteMinder y CA Identity Manager. El administrador de identidades hace referencia a este agente durante la configuración de CA Identity Manager.

Siga estos pasos:

1. Inicie sesión en la interfaz de usuario administrativa de SiteMinder.

   Las fichas relevantes para los privilegios de administrador aparecen.
2. Haga clic en Infraestructura, Agentes, Agente, Crear agente.

   Aparece el cuadro de diálogo Crear agente.
3. Seleccione Crear un nuevo objeto del tipo Agente y haga clic en Aceptar.

   Aparece el cuadro de diálogo Crear agente.
4. Introduzca un nombre y una descripción opcional.

   Nota: Utilice un nombre que se pueda asociar fácilmente con el asistente de conexión de SharePoint correspondiente.

5. Seleccione SiteMinder.
6. Seleccione Agente Web en la lista desplegable.
7. Active la funcionalidad de 4.x con los siguientes pasos:
   a. Seleccione la casilla de verificación Es compatible con agentes 4.x.

      Aparecerán los campos de configuración de confianza.

   b. Agregue los parámetros de configuración de confianza completando los campos siguientes:

      Dirección IP

      Especifica la dirección IP del servidor de políticas.

      Secreto compartido

      Especifica una contraseña que está asociada con el objeto agente 4.x. El asistente de conexión de SharePoint también requiere esta contraseña.

      Confirmar secreto

      Confirma una contraseña que está asociada con el objeto agente 4.x. El asistente de conexión de SharePoint también requiere la confirmación de esta contraseña.
8. Haga clic en Enviar.

   La tarea de creación de objeto agente se enviará para su procesamiento y aparecerá el mensaje de confirmación.

Exportación de los entornos y directorios de CA Identity Manager

El proceso de integración elimina todas las definiciones de directorio y entorno actuales. Para ayudar a garantizar que esta información se mantiene, el administrador de identidades exporta los entornos mediante la Consola de gestión de CA Identity Manager. Después de completar la integración, estas definiciones restauran los directorios y los entornos.

Siga estos pasos:

1. Abra la Consola de gestión de CA Identity Manager.
2. Haga clic en Directorios.
3. Haga clic en el primer directorio de la lista y haga clic en Exportar.
4. Guarde y archive el archivo XML deL directorio.
5. Repita este proceso con los directorios restantes.
6. Haga clic en Principal y, a continuación, en Entornos.
7. Seleccione el primer entorno.
8. Haga clic en Exportar.
9. Repita este proceso con los entornos restantes.

   Nota: Este proceso puede tardar unos minutos por cada entorno.

Supresión de todas las definiciones del entorno y el directorio

Para prepararse para que SiteMinder proteja CA Identity Manager, el administrador de identidades suprime las definiciones del entorno y el directorio mediante la Consola de gestión de CA Identity Manager.

Siga estos pasos:

1. Abra la Consola de gestión de CA Identity Manager.
2. Haga clic en Entornos.
3. Seleccione el primer entorno.
4. Haga clic en Suprimir.
5. Repita este proceso para cada uno de los entornos restantes.

   Nota: Es necesario suprimir los entornos antes de suprimir los directorios porque los entornos hacen referencia a los directorios.
6. Navegue de nuevo a la sección Directorios.
7. Seleccione todos los directorios enumerados.
8. Haga clic en Suprimir.

Activación del adaptador de recursos del servidor de políticas de SiteMinder

El administrador de identidades activa el adaptador de recursos del servidor de políticas de SiteMinder. La finalidad del adaptador es validar la cookie SMSESSION. Después de la validación, SiteMinder crea el contexto del usuario.

Siga estos pasos:

1. Navegue a la carpeta \policysever.rar\META-INF que se encuentra dentro de iam_im.ear en el servidor de aplicaciones que está ejecutando CA Identity Manager.
2. Abra el archivo ra.xml en un editor.
3. Busque el config-property Enabled y, a continuación, cambie el config-property-value a true como se muestra en el siguiente ejemplo:

```
        <config-property-name>validateSmHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. Busque la propiedad ConnectionURL y proporcione el nombre de host del servidor de políticas de SiteMinder. Utilice un nombre de dominio completo (FQDN).
5. Busque la propiedad UserName y especifique la cuenta que se utilizará para la comunicación con SiteMinder. SiteMinder es el valor predeterminado para esta cuenta.
6. Busque la propiedad AdminSecret. Proporcionar la contraseña cifrada. Copie la contraseña del archivo directory.xml que se ha exportado y péguela en ra.xml. Si no está seguro de tener una contraseña común, cifre su contraseña mediante la herramienta de contraseñas de CA Identity Manager.
7. Pegue la contraseña cifrada en el archivo ra.xml.
8. Especifique el nombre del agente 4.x que el administrador de políticas ha creado durante la configuración de SiteMinder.
9. Especifique la contraseña cifrada. Usar la herramienta de contraseñas para cifrar la contraseña si es necesario.
10. Guarde los cambios en el archivo ra.xml.

El adaptador de recursos del servidor de políticas de SiteMinder está activado.

Más información:

Modificación de un secreto compartido o una contraseña de SiteMinder (en la página 367)

Desactivación del filtro de autenticación del marco de trabajo de CA Identity Manager nativo

Con el adaptador de SiteMinder en su lugar, el filtro de autenticación del marco de trabajo ya no se necesita. El administrador de identidades puede desactivar el filtro.

Siga estos pasos:

1. Encuentre y edite el archivo web.xml en la carpeta \user_console.war\WEB-INF en iam_im.ear.
2. Encuentre FrameworkAuthFilter y cambie el valor de Enable init-param a false.

   Si se está utilizando CA Identity Manager r12.5 SP7 o posterior, verifique que los archivos de política jurisdiccional de fuerza ilimitada de la Extensión Criptográfica Java (JCE) se han descargado en \<Java_path>\<jdk_version>\jre\lib\security en el entorno de CA Identity Manager. Estos archivos permiten que CA Identity Manager se conecte a SiteMinder.

   Si las bibliotecas de JCE están instaladas, se ven los mensajes siguientes durante el inicio de la aplicación de CA Identity Manager:

   ```
   2012-07-06 11:23:56,079 WARN  [ims.default] (main) * Startup Step 2 : Attempting to start PolicyServerService
   2012-07-06 11:23:56,081 WARN [ims.default] (main) Unlimited Strength Java Crypto Extensions enabled: TRUE
   ```

   De lo contrario, el valor de la entrada "Unlimited Strength Java Crypto Extensions enabled" será false. CA Identity Manager no podrá conectarse al servidor de políticas.

Reinicio del servidor de aplicaciones

El reinicio actualiza el servidor de aplicaciones con los cambios. El administrador de identidades valida que el cambio se haya realizado correctamente y que existe una conexión correcta al servidor de políticas de SiteMinder.

Siga estos pasos:

1. Utilice el panel de servicios para reiniciar CA Identity Manager cuando su servidor de aplicaciones se esté ejecutando como un servicio.
2. Haga referencia a server.log para validar la conexión.

Configuración de un origen de datos para SiteMinder

Si su entorno de CA Identity Manager utiliza una base de datos relacional para su almacén de identidades, se requiere el administrador de identidades para completar un proceso adicional en el servidor de políticas de SiteMinder. SiteMinder requiere un origen de datos local para comunicarse con la base de datos.

Siga estos pasos:

1. Para servidores de Windows, abra la consola de administrador de orígenes de datos ODBC que se encuentra en Herramientas administrativas.
2. Haga clic en la ficha DSN de sistema.
3. Haga clic en Agregar y seleccione el controlador de SiteMinder correspondiente para su base de datos.
4. Proporcione la información necesaria para hacer referencia al almacén de usuarios de la base de datos relacional.
5. Pruebe la conectividad antes de continuar.

Importación de las definiciones del directorio

Para preparar la importación de los entornos, el administrador de identidades debe importar los directorios a los que hacen referencia los entornos. La importación de la definición del directorio en CA Identity Manager también agrega la información del directorio al almacén de políticas de SiteMinder.

Siga estos pasos:

1. Asegúrese de que CA Identity Manager se está ejecutando y está conectado a SiteMinder.
2. Navegue a la Consola de gestión de CA Identity Manager.
3. Haga clic en Directories (Directorios) y, a continuación, haga clic en Create (Crear) o Update from XML (Actualizar de XML).
4. Seleccione su archivo de configuración del directorio (directory.xml). Este archivo es el que se exportó en Exportación de los entornos y directorios de CA Identity Manager (en la página 307).
5. Haga clic en Siguiente.
6. Haga clic en Finish (Finalizar) y revise el resultado de la carga. Verifique que el directorio está presente en CA Identity Manager y SiteMinder.
7. Repita estos pasos para el almacén de aprovisionamiento y todos los directorios restantes.
8. Inicie sesión en la interfaz de usuario administrativa de SiteMinder para validar la creación de los directorios de usuarios.

Actualización e importación de las definiciones del entorno

El administrador de identidades vuelve a importar los entornos actualizados en CA Identity Manager.

Siga estos pasos:

1. A diferencia de las exportaciones del directorio, la exportación del entorno se realiza mediante un archivo ZIP. Arrastre una copia del archivo *name*.xml fuera del archivo comprimido.
2. Copie el archivo *name*.xml. Inserte una referencia al agente que protege (no al agente de 4.x de SM) al final del elemento ImsEnvironment, antes del paréntesis de cierre />: *agent="idmadmin"*
3. Guarde y pegue el archivo de nuevo en el archivo ZIP.
4. Abra la Consola de gestión de CA Identity Manager y haga clic en Environments (Entornos) y, a continuación, en Import (Importar).
5. Introduzca el nombre del archivo ZIP del entorno actualizado.
6. Haga clic en Finish (Finalizar) y revise el resultado de la importación.
7. Repita este proceso para todos los entornos restantes.
8. Reinicie el servidor de aplicaciones.

Instalación del complemento del servidor proxy web

Según la aplicación que se instale, el administrador de identidades instala uno de los siguientes complementos que el servidor web utiliza para enviar solicitudes al servidor de aplicaciones:

- WebSphere (en la página 314)
- JBoss (en la página 322)
- WebLogic (en la página 326)

Instalación del complemento del proxy en WebSphere

El servidor Web en el cual se instaló el agente Web envía solicitudes al servidor de aplicaciones que hospeda el servidor de CA Identity Manager. El complemento del proxy de servidor Web que proporciona el distribuidor ofrece este servicio.

Se deben utilizar los procedimientos aplicables para la implementación:

1. Configuración de IBM HTTP Server (en la página 314) (todos los servidores Web)
2. Configuración del complemento del proxy (en la página 315) (todos los servidores Web)
3. Uno de los siguientes:
   - Finalización de la configuración en IIS (en la página 319)
   - Finalización de la configuración en iPlanet o Apache (en la página 321)

Configuración de IBM HTTP Server

Para todos los servidores Web, se instala el complemento del proxy y se utiliza el comando configurewebserver.

Siga estos pasos:

1. Instale el complemento del proxy de la plataforma de lanzamiento de WebSphere.
2. Agregue el servidor Web a la celda de WebSphere ejecutando el comando configurewebserver1.bat como se muestra a continuación:
   a. Edite *websphere_home*\Plugins\bin\configurewebserver1.bat/,sh en un editor de texto.
   b. Agregue un nombre de usuario y contraseña después de wsadmin.bat/.sh como se muestra a continuación:
   ```
   wsadmin.bat -user wsadmin -password password -f
   configureWebserverDefinition.jacl
   ```
   c. Ejecute configurewebserver1.bat/.sh.

   Nota: Consulte la documentación de IBM WebSphere para obtener más información sobre el comando configurewebserver.
3. Continúe con el procedimiento de Configuración del complemento del proxy (en la página 315).

Configuración del complemento del proxy

Para todos los servidores Web, se actualiza el complemento mediante el comando GenPluginCfg de WebSphere:

Siga estos pasos:

1. Inicie sesión en el sistema en el que se esté instalado WebSphere.
2. En la línea de comandos, navegue a *websphere_home*\bin, donde *websphere_home* es la ubicación de la instalación de WebSphere.

   Por ejemplo:

   - **Windows:**

     C:\Archivos de programa\WebSphere\AppServer\profile\AppSrv01\bin

   - **UNIX:**

     /*home_dir*/WebSphere/AppServer/profile/AppSrv01/bin

3. Ejecute el comando GenPluginCfg.bat o GenPluginCfg.sh.

   La ejecución de este comando genera un archivo plugin-cfg.xml en la siguiente ubicación:

   websphere_home\AppServer\profiles\AppSrv01\config\cells

4. Continúe con uno de los siguientes procedimientos:

   - Finalización de la configuración en IIS (en la página 319)
   - Finalización de la configuración en iPlanet o Apache (en la página 321)

Finalización de la configuración en IIS (7.x)

Antes de iniciar este procedimiento, se debe verificar que se está utilizando la versión 6.1.0.9 o posterior, del complemento de servidor Web. Las versiones anteriores del complemento no son compatibles con el sistema operativo Windows Server 2008.

Siga estos pasos:

1. Instale la versión 7.x de IIS con los componentes de compatibilidad con la gestión de la versión 6.0 de IIS. Los componentes de compatibilidad con la administración de la versión 6.0 de IIS no están instalados de forma predeterminada.
2. Complete los siguientes pasos para activar la ventana del gestor del servidor en Windows Server 2008:
    1. Haga clic en Inicio, Herramientas administrativas, Administrador de servidores.
    2. Haga clic en Acción, Agregar roles y, a continuación, en Siguiente.
    3. Seleccione el rol del servidor Web (IIS) en la página Seleccionar roles de servidor y, a continuación, haga clic en Siguiente.
    4. Haga clic en Agregar característica, Siguiente, cuando se muestre una solicitud para la función del servicio de activación de procesos de Windows.
    5. Haga clic en Siguiente en la página de introducción de IIS.
3. Cuando se muestre la ventana Servicios de rol, verifique que las siguientes opciones estén seleccionadas además de las opciones predeterminadas que ya están seleccionadas.
    - Internet Information Services: Herramientas de administración
    - Versión de IIS 6.0 compatibilidad de gestión: Consola de administración de la versión 6.0 de IIS, Herramientas de scripting de la versión 6.0 de IIS, Compatibilidad con WMI de la versión 6.0 de IIS y Compatibilidad con la metabase de IIS
    - Desarrollo de aplicaciones: Extensiones ISAPI, Filtros ISAPI
4. Haga clic en Siguiente para activar las opciones seleccionadas y, a continuación, haga clic en Instalar en la ventana siguiente para realizar la instalación.
5. Haga clic en Cerrar en la ventana Resultados de la instalación cuando la instalación finalice.
6. Abra el símbolo del sistema y vaya a :\Archivos de programa\IBM\WebSphere\AppServer\profiles\Dmgr01\bin.
7. Ejecute el comando GenPluginCfg.bat.

    Se generará el archivo plugin-cfg.xml en esta ubicación: C:\Archivos de programa\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells.
8. Cree un directorio en c:\, por ejemplo, c:\plugin.
9. Copie el archivo plugin-cfg.xml en el directorio c:\plugin.

10. Copie el archivo iisWASPlugin_http.dll en el directorio c:\plugin.
11. Seleccione Inicio, Todos los programas, Herramientas administrativas, Administrador de Internet Information Services (IIS) en un sistema operativo Windows Server 2008. Esta acción inicia la aplicación de IIS y crea un directorio virtual nuevo para la instancia de sitio web. Estas instrucciones suponen que se está utilizando el sitio web predeterminado.
12. Expanda el árbol de la izquierda hasta ver el sitio web predeterminado.
13. Haga clic con el botón secundario del ratón en Sitio web predeterminado, Agregar directorio virtual para crear el directorio con una instalación predeterminada.
14. Introduzca setPlugins en el campo Alias en la ventana Alias del directorio virtual del Asistente para crear un directorio virtual.
15. Examine hasta el directorio c:\plugin en el campo Ruta de acceso física de la ventana Directorio de contenido del sitio web y, a continuación, haga clic en Aceptar.
16. Haga clic en el botón Probar configuración. Si se produce un error en la prueba de configuración, se pueden cambiar los permisos del directorio físico. También se puede seleccionar la opción de conectarse como y permitir que IIS se conecte como una cuenta de usuario de Windows que tenga autoridad sobre archivos en esa ruta física.
17. Haga clic en Aceptar para agregar el directorio virtual setPlugins a su sitio web.
18. Seleccione el directorio virtual setPlugins que se acaba de crear en el árbol de navegación.
19. Haga doble clic en Asignaciones de controlador y, a continuación, en Modificar permisos de características en el panel Acciones.
20. Seleccione Script y Ejecutar, si no están seleccionados ya.
21. Haga clic en Aceptar.
22. Vuelva a la ventana del gestor de IIS y expanda la carpeta de sitios web en el árbol de navegación izquierdo de esa ventana.
23. Seleccione Sitio web predeterminado en el árbol de navegación.

24. Complete los siguientes pasos en el panel de propiedades del sitio web predeterminado para agregar el filtro ISAPI:
    1. Haga doble clic en la ficha Filtros ISAPI.
    2. Haga clic para abrir el cuadro de diálogo Agregar o modificar propiedades de filtro.
    3. Introduzca iisWASPlugin en el campo Nombre de filtro.
    4. Haga clic en Explorar para seleccionar el archivo de complemento que se encuentra en el directorio c:\plugin\iisWASPlugin_http.dll.
    5. Haga clic en Aceptar para cerrar el cuadro de diálogo Agregar o modificar propiedades de filtro.
25. Seleccione el nodo de servidor de nivel superior en el árbol de navegación.
26. Haga doble clic en Restricciones de ISAPI y CGI en el panel Características.

    Para determinar el valor que se debe especificar para la propiedad Ruta de acceso ISAPI o CGI , examine y, a continuación, seleccione el mismo archivo de complemento seleccionado en el paso anterior. Por ejemplo: c:\plugin\iisWASPlugin_http.dll.
27. Haga clic en Agregar el panel Acciones.
28. Introduzca WASPlugin en el campo Descripción , seleccione Permitir ejecución de la ruta de extensión y, a continuación, haga clic en Aceptar para cerrar el cuadro de diálogo Restricciones de ISAPI y CGI .
29. Cree el archivo nuevo plugin-cfg.loc en la ubicación c:\plugin. Establezca el valor en el archivo plugin-cfg.loc a la ubicación del archivo de configuración. La ubicación predeterminada es C:\plugin\plugin-cfg.xml.

Actualización del agente web

Después de configurar IIS 7.x, haga los cambios siguientes en el agente web:

1. Haga clic en Grupos de aplicaciones y cambie la agrupación de aplicaciones predeterminada al modo clásico.
2. Haga clic en Enviar.
3. Asegúrese de que el agente esté más arriba en la lista de prioridades de los filtros ISAPI que el complemento para el servidor de aplicaciones que utiliza CA Identity Manager.
4. Reinicie la versión 7.x de IIS y el perfil del servidor de aplicaciones WebSphere.

Finalización de la configuración en IIS

Después de configurar IBM HTTP Server y el complemento del proxy, es necesario asegurarse de que el archivo plugin-cfg.xml del proxy se encuentra en la ubicación correcta y realizar los pasos para configurar un archivo de complemento adicional.

Siga estos pasos:

1. Copie plugin-cfg.xml como se muestra a continuación:
   a. Inicie sesión en el sistema donde el agente Web esté instalado.
   b. Cree una carpeta sin espacios en la unidad C:. Por ejemplo: C:\plugin.
   c. Copie el archivo plugin-cfg.xml en la carpeta C:\plugin.
2. Cree un archivo llamado plugin-cfg.loc en la carpeta C:\plugin y agregue la línea siguiente en el archivo:

   C:\plugin\plugin-cfg.xml
3. Descargue el instalador del complemento de WebSphere de www.ibm.com al sistema donde WebSphere esté instalado.
4. Vaya a la ubicación del instalador del complemento de WebSphere.
5. Genere el archivo iisWASPlugin_http.dll mediante este comando:

   ```
   install is:javahome "c:\IBM\WebSphere\AppServer\Java
   ```

   Responda a las preguntas que se presenten en función de su configuración.

   Cuando el asistente finalice, el archivo iisWASPlugin_http.dll se guardará en la carpeta C:\IBM\WebSphere\Plugs\bin. Busque una subcarpeta de 32 bits o 64 bits.
6. Copie el archivo iisWASPlugin_http.dll en la carpeta C:\plugin en el sistema con el agente Web.
7. Cree un directorio virtual de la siguiente manera:
   a. Abra el gestor IIS.
   b. Haga clic en con el botón secundario del ratón en Sitio web predeterminado.
   c. Haga clic en Nuevo directorio virtual y proporcione estos valores:

      Alias: sePlugins (distingue entre mayúsculas y minúsculas).

      Ruta: c:\plugin

      Permiso: lectura y ejecución (ISAPI o CGI)

8. Agregue un filtro ISAPI como se muestra a continuación:
   a. Haga clic con el botón secundario del ratón en Sitio web predeterminado.
   b. Haga clic en Propiedades.
   c. Haga clic en Agregar en la ficha Filtro ISAPI.
   d. Proporcione estos valores:

      Nombre del filtro: sePlugins

      Archivo ejecutable: c:\plugin\ iisWASPlugin_http.dll
9. Cree una extensión del servicio web como se muestra a continuación:
   a. En gestor de IIS6, expanda el nombre del equipo.
   b. Cree una extensión del servicio web y establézcalo como permitido.

      Nombre de la extensión: WASPlugin

      Ruta de acceso: c:\plugin\ iisWASPlugin_http.dll
   c. Haga clic con el botón secundario del ratón en cada extensión del servicio web para cambiarlo al estado Permitido.
10. Reinicie el servidor web de IIS.

    En el servicio de WWW principal, es necesario garantizar que el complemento de WebSphere (sePlugin) aparece después del complemento del agente Web de SiteMinder y que el complemento de WebSphere se ha iniciado correctamente.

Finalización de la configuración en iPlanet o Apache

Después de configurar IBM HTTP Server y el complemento del proxy, es necesario asegurarse de que el archivo plugin-cfg.xml del proxy se encuentra en la ubicación correcta y reiniciar el servidor web.

Siga estos pasos:

1. Copie plugin-cfg.xml en el sistema donde se ha instalado el complemento del proxy en la ubicación siguiente:

   websphere_home\AppServer\profiles*server_name*\config\cells*websphere_cell*\nodes\webserver1_node\servers\webserver1\

2. Garantice que el complemento de WebSphere (libns41_http.so) está cargado después del complemento de agente Web de SiteMinder (NSAPIWebAgent.so) en todos los servidores web de iPlanet.

3. Compruebe el orden de complementos en *iplanet_home*/https-*instance*/config/magnus.conf para los servidores Web de iPlanet 6.0.

4. Copie las líneas siguientes de *iplanet_home*/https-*instance*/config/magnus.conf en *iplanet_home*/https-*instance*/config/obj.conf (servidores Web de iPlanet 5.x):

   ```
   Init fn="load-modules" funcs="as_init,as_handler,as_term"
   shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init"
   bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg.xml"
   ```

   Agregue el siguiente código después de AuthTrans fn="SiteMinderAgent" en el archivo obj.conf:

   ```
   Service fn="as_handler"
   ```

5. Asegúrese de que el complemento del agente Web de SiteMinder (mod2_sm.so) está cargado antes del complemento de WebSphere (mod_ibm_app_server_http.so) en los servidores Web de Apache. Este comando se encuentra en la sección de asistencia de objetos dinámicos compartidos (DSO) *apache_home*/config/httpd.conf.

6. Reinicie el servidor web.

Instalación del complemento del proxy para JBoss

Después de que el agente Web de SiteMinder autentique y autorice una solicitud para un recurso de CA Identity Manager, el servidor Web enviará la solicitud al servidor de aplicaciones que hospeda el servidor de CA Identity Manager. Para enviar estas solicitudes, se debe instalar y configurar un conector JK en el sistema donde esté instalado el agente Web de SiteMinder. Consulte el siguiente sitio web de Jakarta Project para obtener más información sobre el conector JK:

http://community.jboss.org/wiki/usingmodjk12withjboss

En las herramientas administrativas de CA Identity Manager se incluyen archivos de configuración de ejemplo que se pueden utilizar para configurar el conector JK. Para obtener instrucciones, consulte el archivo readme.txt en el directorio anotado en la siguiente tabla:

Plataforma	Ubicación
Servidor web de IIS en un sistema Windows	C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\ConnectorConfiguration\windows\IIS_JBoss*
Servidor web del sistema Sun Java en un sistema Solaris	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss*
Servidor web de Apache en un sistema Solaris	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/apache_JBoss*

Instalación y configuración de un complemento de aplicaciones de JBoss (IIS 7.x)

Este procedimiento describe la configuración del complemento de Apache de JBoss a partir de IIS 7.0

Siga estos pasos:

1. Implemente y actualice los filtros ISAPI en el sistema de archivos.

   Implemente la carpeta ISAPI en la raíz de la unidad C.

2. Edite el archivo jakarta.reg que se encuentra en la carpeta descomprimida.

   Si se colocó la carpeta ISAPI en la raíz de C:\, no cambie este archivo. Si se colocó en una carpeta diferente, especifíquela en las líneas 9, 11 y 12.

3. Guarde los cambios y, a continuación, haga doble clic para actualizar el registro.

4. Edite el archivo workers.properties especificando la ubicación del servidor de aplicaciones JBoss. El puerto y el tipo no deben cambiar.

5. Instale IIS 7 o IIS 7.5 en Windows 2008.

6. Abra el gestor del sistema y verifique que la extensión ISAPI y el filtro ISAPI de IIS están instalados.
7. Inicie inetmgr en la ventana Ejecutar.
8. Seleccione el nombre de m/c y haga doble clic en Restricciones de ISAPI y CGI.
9. Haga clic en el botón Agregar en el panel derecho.
10. Aparecerá la ventana Agregar restricciones ISAPI o CGI.
11. Seleccione isapi_redirect.dll e introduzca la descripción como ISAPI.
12. Seleccione Permitir ejecución de la ruta de extensión.
13. Haga clic en Aceptar en la ventana Agregar restricciones ISAPI o CGI.
14. Expanda los sitios en la sección Conexión, seleccione Sitio web predeterminado y haga clic con el botón secundario del ratón en Agregar directorio virtual.
15. Introduzca el alias como "jakarta" e introduzca la ubicación del archivo isap_redirect.dll (c:\ajp) en la ruta física.
16. Haga clic en el botón Probar configuración:
    - Si la autenticación y autorización se han aceptado, haga clic en Aceptar.
    - Si se produce un error con la autorización, haga clic en el botón de conectarse como.
17. Seleccione el usuario específico y proporcione el nombre de usuario y la contraseña del administrador.
18. Vuelva a hacer clic en el botón Probar configuración. Esta vez la autorización se acepta.
19. Haga clic en Sitio web predeterminado a la izquierda y haga doble clic en el filtro ISAPI.
20. Haga clic en el botón Agregar en el panel derecho.
21. Introduzca el nombre y proporcione la ubicación del archivo isapi_redirect.dll.
22. Haga clic en OK.
23. Expanda Sitio web predeterminado y haga clic en el directorio virtual de jakarta.
24. Haga doble clic en Asignaciones de controlador.
25. Seleccione ISAPI-dll y haga clic en Modificar permisos de características.

26. Verifique que todos los permisos (Lectura, Script, Ejecutar) están seleccionados.
27. Haga clic en OK.

Actualización del agente web

Después de configurar IIS 7.x, haga los cambios siguientes en el agente web:

1. Haga clic en Grupos de aplicaciones y cambie la agrupación de aplicaciones predeterminada al modo clásico.
2. Haga clic en Enviar.
3. Asegúrese de que el agente esté más arriba en la lista de prioridades de los filtros ISAPI que el complemento para el servidor de aplicaciones que utiliza CA Identity Manager.

El complemento de JBoss está configurado.

Instalación y configuración de un complemento de aplicaciones de JBoss (IIS 6.0)

Esta integración supone que SiteMinder autentica y autoriza a un usuario antes de llegar a CA Identity Manager. Se requiere que un usuario tenga una cookie SMSESSION antes de llegar a CA Identity Manager. Utilice un complemento de la aplicación (redirección de proxy) protegido por un agente Web de SiteMinder. Mediante esta configuración, SiteMinder autentica a un usuario y, a continuación, se le redirige a CA Identity Manager después de que se haya creado una cookie SMSESSION.

Este procedimiento es para la implementación y configuración del complemento de Apache de JBoss para IIS 6.0:

Siga estos pasos:

1. Implemente y actualice el filtro ISAPI en el sistema de archivos.

   Asegúrese de implementar la carpeta ISAPI en la raíz de la unidad C.
2. Edite el archivo jakarta.reg que se encuentra en la carpeta descomprimida.

   Si se colocó la carpeta ISAPI en la raíz de C:\, no cambie este archivo. Si se coloca en una carpeta diferente, especifíquela en las líneas 9, 11 y 12.
3. Guarde los cambios y, a continuación, haga doble clic para actualizar el registro.
4. Edite el archivo workers.properties especificando la ubicación del servidor de aplicaciones JBoss. El puerto y el tipo no deben cambiar.
5. Implemente el filtro ISAPI en IIS.
6. Abra Administrador de Internet Information Services en Herramientas administrativas.
7. Aumente los niveles hasta pueda verse Sitio web predeterminado. Haga clic con el botón secundario del ratón en Nuevo, Directorio virtual.

8. Introduzca *jakarta* como el alias.
9. Haga referencia a la ruta donde se instaló el complemento de ISAPI.
10. Seleccionar Leer, Ejecutar scripts (por ejemplo, ASP), y Ejecutar (por ejemplo, aplicaciones ISAPI o CGI).
11. Haga clic en Siguiente para continuar y finalizar al asistente.
12. Haga clic con el botón secundario del ratón en Sitio web predeterminado y seleccione propiedades, seleccione la ficha Filtros ISAPI y haga clic en Agregar.
13. Introduzca *jakarta* para el nombre del filtro y, a continuación, haga clic en la opción de examinar para seleccionar isapi_redirect.dll. A continuación, haga clic en Aceptar dos veces.
14. Para IIS 6.0, active este filtro en Extensiones de servicio web.
15. Seleccione la carpeta Extensiones de servicio web. Haga clic en el vínculo azul a la izquierda para agregar una extensión de servicio web nueva.
16. Proporcione Jakarta-Tomcat para el nombre. Haga clic en Agregar y busque el mismo dll anterior. Haga clic en Aceptar, haga clic en el estado Establecer la extensión en Permitido y, a continuación, haga clic en Aceptar.
17. Reinicie el servidor IIS.

Con el proxy en su lugar, ahora se puede acceder a CA Identity Manager mediante IIS. Por ejemplo, a continuación se muestran los vínculos para acceder a CA Identity Manager antes y después de la configuración del proxy:

Antes

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

Transcurridos

http://smserver.forwardinc/idmmanage http://smserver.forwardinc/idmmanage

Nota: Puede que se necesite una barra diagonal "/" al final de esta dirección URL para que el proxy funcione. Se debe hacer referencia a los registros del proxy si no se redirige al usuario a la Consola de gestión.

Instalación del complemento del proxy en WebLogic

Cuando el agente Web autentique y autorice una solicitud para un recurso de CA Identity Manager, el servidor Web enviará la solicitud al servidor de aplicaciones que hospeda el servidor de CA Identity Manager.

1. Instale el complemento del proxy de WebLogic para su servidor Web como se describe en la documentación de WebLogic.

   Nota: Para usuarios de IIS, cuando se instala el complemento del proxy, es necesario asegurarse de configurar las conexiones de proxy mediante extensión de archivo y ruta. Cuando se configuran las conexiones de proxy mediante extensión de archivo, se debe agregar una asignación de la aplicación en la ficha correspondiente con las propiedades siguientes:
   Archivo ejecutable: IISProxy.dll
   Extensión: .wlforward

2. Configure el complemento del proxy para CA Identity Manager como se describe en una de las siguientes secciones:

   - Complemento del proxy de IIS (en la página 329)
   - Complemento del proxy de iPlanet (en la página 330)
   - Complemento del proxy de Apache (en la página 333)

Configuración del complemento del proxy para IIS (7.x)

El procedimiento siguiente guía durante toda la implementación y configuración del complemento del proxy de WebLogic para IIS 7.x.

Nota: Estas instrucciones son para entornos operativos de 32 bits. Se aplican las mismas instrucciones a los entornos operativos de 64 bits. La ubicación del archivo .dll de instalación es diferente:

- %WL_HOME%server\plugin\win\32\
- %WL_HOME%server\plugin\win\64\

Siga estos pasos:

1. Instale el agente Web y configúrelo en IIS 7.
2. Cree una carpeta con el nombre ‘plugin’ en la unidad ‘C’.
3. Copie los siguientes archivos en la carpeta de complemento:

   - lisforward.dll
   - lisproxy.dll
   - iisproxy.ini

   Se pueden encontrar estos archivos en \\lodimmaple.ca.com\RegressionHarness\thirdparty\weblogic\Weblogic_Proxy_Files_IIS7.

4. Instale los servicios de rol Desarrollo de aplicaciones y Herramientas de administración en IIS 7.
5. Abra Inet Manager y seleccione Sitio web predeterminado.
6. Haga clic en Asignaciones de controlador.
7. Haga doble clic en la opción del archivo estático y modifique la ruta de solicitud a *.*.
8. Haga clic en el botón Restricciones de solicitudes.
9. En la ficha Asignaciones, seleccione Invocar controlador sólo si la solicitud está asignada a un archivo o carpeta.
10. En el cuadro de diálogo Asignaciones de controlador, haga clic en Agregar asignación de script en las opciones del menú derecho. Introduzca los siguientes valores:
    - Ruta de acceso de solicitudes: *
    - Archivo ejecutable: iisProxy.dll
    - Nombre: proxy
11. Haga clic en el botón Restricciones de solicitudes.
12. Anule la selección de la casilla Invocar controlador sólo si la solicitud está asignada a.
13. Haga clic en Sí a la petición de permitir esta extensión IASPI.
14. Haga clic en el nodo raíz (nombre del equipo) del árbol del gestor de IIS y haga clic en Restricciones de ISAPI y CGI.
15. Haga clic en Agregar en panel Acciones e introduzca los valores siguientes:
    - Ruta de ISAPI o CGI: C:\plugin\ iisproxy.dll.
    - Descripción: WebLogic
    - Seleccione Permitir ejecución de la ruta de extensión.
16. Haga clic en el nodo raíz (nombre del equipo) del árbol del gestor de IIS y haga clic en Restricciones de ISAPI y CGI. Seleccione la opción WebLogic y haga clic en Modificar configuración de característica en el panel derecho.
17. Seleccione Permitir módulos ISAPI no especificados y Permitir módulos CGI no especificados.
18. Haga lo mismo con Webagent.
19. En la vista Funciones, en el Sitio web predeterminado, haga doble clic en Asignaciones de controlador.

20. En la página Asignaciones de controlador, en el panel Acciones, haga clic en Agregar asignación de script y los valores siguientes:
    - Ruta de la solicitud: .jsp
    - Archivo ejecutable: iisproxy.dll
    - Nombre: JSP
21. Haga clic en Restricciones de solicitudes.
22. En la ficha Asignación, seleccione Invocar controlador sólo si la solicitud está asignada al archivo.
23. Haga clic en OK.
24. Haga clic en Agregar asignación de script y agregue los valores siguientes:
    - Ruta de la solicitud: .do
    - Archivo ejecutable: C:\plugin\iisproxy.dll
25. Haga clic en Restricciones de solicitudes. Los parámetros de configuración son los mismos del .jsp.
26. Haga clic en OK.
27. Haga clic en Agregar asignación de script y especifique los valores siguientes:
    - Ruta de la solicitud: .wlforward
    - Archivo ejecutable: C:\plugin\iisproxy.dll
28. Haga clic en Restricciones de solicitudes. Los parámetros de configuración son los mismos que los de .jsp.
29. Haga clic en Sitio web predeterminado y haga doble clic en Filtros ISAPI.
30. Haga clic en la lista de orden de vista en el panel derecho.
31. Coloque el archivo ejecutable del agente de SiteMinder en segundo lugar en la lista. Después de esta entrada, solamente el archivo ejecutable de WebLogic estará en la lista.

    Nota: Si el archivo ejecutable del agente de SiteMinder aparece después del archivo ejecutable de WebLogic, se debe mover el agente de SiteMinder usando la acción Mover hacia arriba.
32. Haga clic en Grupos de aplicaciones y cambie la agrupación de aplicaciones predeterminada al modo clásico.

El complemento de WebLogic está configurado.

Configuración del complemento del proxy de WebLogic para IIS 6.0

Este procedimiento se aplica a las configuraciones del complemento del proxy de WebLogic para IIS 6.0.x:

Siga estos pasos:

1. Cree una carpeta en el sistema donde esté instalado el agente web. Por ejemplo: c:\weblogic_proxy.
2. Inicie sesión en el sistema donde se esté ejecutando el servidor de CA Identity Manager.
3. Vaya a esta carpeta: *Weblogic_Home*\wlserver_11\server\plugin
4. Copie los siguientes archivos en la carpeta del proxy de WebLogic creada en el paso 1.
   - iisforward.dll
   - iisproxy.dll
5. Cree un archivo llamado iisproxy.ini en la misma carpeta e incluya el siguiente contenido:

   ```
   # This file contains initialization name/value pairs
   # for the IIS/WebLogic plug-in.
   WebLogicHost=host-name
   WebLogicPort=7001
   ConnectTimeoutSecs=20
   ConnectRetrySecs=2
   WlForwardPath=/castylesr5.1.1,/iam,/im , /ca/Odata/
   WLLogFile= c:\weblogic_proxy \proxy.log
   DebugConfigInfo=ON
   ```

   Sustituya *host-name* por el nombre de host real.
6. Inicie el gestor de IIS.
7. Expanda los sitios web.
8. Haga clic con el botón secundario del ratón en Sitio web predeterminado.
9. Seleccione Propiedades.
10. Agregue un filtro como se muestra a continuación:
    a. Haga clic en Filtros ISAPI.
    b. Haga clic en Agregar y complete el cuadro de diálogo como se muestra a continuación:

       Para el nombre del filtro: WebLogic

       Para el archivo ejecutable: ruta de iisforward.dll

11. Proporcione la ubicación del archivo iisproxy.dll como se muestra a continuación:
    a. Haga clic en Directorio principal.
    b. Haga clic en Configuración.
    c. Haga clic en Agregar.
    d. Introduzca la ruta del archivo iisproxy.dll.
    e. Introduzca .jsp en el campo Extensión.
    f. Anule la selección de la opción Comprobar si el archivo existe.
12. Repita el paso 11 para las extensiones .do y .wlforward.
13. Agregue una extensión de servicio web para wlforward (todo en minúscula) apuntando a la ubicación de iisforward.dll.

    Establezca el estado de la extensión en Permitido.
14. Haga clic con el botón secundario del ratón en cada extensión del servicio web para cambiarlo al estado Permitido.
15. Reinicie el servidor web de IIS.

Configuración del complemento del proxy de iPlanet

Para configurar el complemento, se deben modificar los siguientes archivos de configuración de iPlanet:

- magnus.conf
- obj.conf

Los archivos de configuración de iPlanet tienen reglas estrictas sobre la ubicación del texto. Para evitar problemas, se deben tener en cuenta los siguientes puntos:

- Eliminar los espacios blancos iniciales y finales extraños. Un espacio blanco extra puede hacer que se produzca un error en el servidor de iPlanet.
- Si es necesario introducir más caracteres de los que se puedan ajustar en una línea, se debe colocar una barra inversa (\) al final de esa línea y continuar escribiendo en la línea siguiente. La barra inversa añade directamente el final de la primera línea al inicio de la línea siguiente. Si hace falta un espacio entre la palabra que termina la primera línea y la que empieza la segunda, es necesario asegurarse de utilizar un espacio al final de la primera línea (antes de la barra inversa) o al inicio de la segunda línea.
- No se deben dividir atributos en varias líneas.

Los archivos de configuración de iPlanet para su instancia de iPlanet se encuentran en la siguiente ubicación:

iplanet_home/https-*instance_name*/config/

donde *iplanet_home* es el directorio raíz de la instalación de iPlanet e *instance_name* es la configuración del servidor particular.

Siga estos pasos:

1. En el directorio *weblogic_home*/server/lib, copie el archivo libproxy.so que corresponde a la versión del servidor web de iPlanet en el sistema de archivos donde se instaló iPlanet.
2. En un editor de texto, modifique el archivo de iPlanet magnus.conf.

   Para hacer que iPlanet cargue el archivo libproxy.so como un módulo de iPlanet, agregue las líneas siguientes al inicio del archivo magnus.conf:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=path in file system from step 1/libproxy.so
   Init fn="wl_init"
   ```

   Por ejemplo:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   La función load-modules etiqueta la biblioteca compartida para la carga cuando se inicia iPlanet. Los valores wl_proxy y wl_init identifican las funciones que ejecuta el complemento.

3. En un editor de texto, modifique el archivo iPlanet obj.conf como se muestra a continuación:

   a. Después de la última línea que empieza con el texto siguiente:

      NameTrans fn=....

      Agregue la siguiente directiva de servicio a la sección Object name="default":

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      Nota: Puede agregar esta directiva en una línea después de las directivas de servicio existentes.

   b. Agregue el código siguiente al final del archivo:

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      ```

      donde *hostname* es el nombre del servidor y el dominio del sistema donde se instaló WebLogic y *portnumber* es el puerto de WebLogic (el valor predeterminado es 7001).

      Puede que haya más de una entrada Object.

      Por ejemplo:

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```

4. Guarde el archivo de configuración de iPlanet.
5. Reinicie la instancia del servidor Web.

IM_12.8: Configuración del complemento del proxy de Apache

La configuración del complemento del proxy de Apache requiere la edición del archivo http.conf.

Siga estos pasos:

1. Detenga el servidor Web de Apache después de haber instalado un agente Web en Solaris y copie el archivo mod_wl_20.so de la ubicación siguiente:

   weblogic_home/server/lib/solaris

   en

   apache_home/modules

2. Edite el archivo http.conf (ubicado en *apache_home*/conf) y realice los siguientes cambios:

   a. En la sección de carga del módulo, agregue el código siguiente:
   ```
   LoadModule weblogic_module      modules/mod_wl_20.so
   ```

   b. Edite el nombre del servidor con el nombre del sistema de servidor de Apache.

   c. Agregue un bloque If al final del archivo como se muestra a continuación:
   ```
   <IfModule mod_weblogic.c>
     WebLogicHost weblogic_server.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
     MatchExpression /ca/Odata
   </IfModule>
   ```

3. Guarde el archivo http.conf.

4. Reinicie el servidor web de Apache.

Asocie el agente de SiteMinder con un dominio de CA Identity Manager.

El administrador de políticas realiza esta tarea después de haber completado las tareas de CA Identity Manager. Mientras se cargan los entornos en CA Identity Manager, se debe hacer referencia al agente de 4.X. SiteMinder utiliza ese agente al crear el dominio o territorio en el servidor de políticas de SiteMinder. Este agente valida las cookies SMSESSION. Se debe actualizar el dominio o territorio y hacer referencia al agente en funcionamiento completo que está en el servidor web que se utiliza para acceder a CA Identity Manager. Este servidor web actúa como el punto de acceso a CA Identity Manager y crea cookies SMSESSION.

Siga estos pasos:

1. Inicie sesión en la interfaz de usuario administrativa de SiteMinder.
2. Vaya a Políticas, Dominios.
3. Modifique el dominio para el entorno.
4. En la ficha Territorios, edite el primer territorio que aparece: XXX_ims_realm.
5. Busque y seleccione el agente en su proxy.

   Nota: Si no se dispone de un agente de proxy (agente de servidor web), se deberá crear uno. Verifique que tiene un servidor Web y proxy en su lugar para dirigir CA Identity Manager.
6. Haga clic en Aceptar dos veces y, a continuación, repita este proceso para el territorio público XXX_pub_realm.
7. Después de actualizar los dos territorios, haga clic en Enviar.
8. Se debe esperar a que el agente se actualice o reiniciar el servidor Web donde se encuentra el agente de proxy.

Configuración del parámetro LogOffUrI de SiteMinder

Después de agregar SiteMinder al entorno, el cierre de sesión en CA Identity Manager no funciona. Para volver a activar esta funcionalidad, actualice el objeto de configuración del agente (ACO) correspondiente al agente en el proxy.

Siga estos pasos:

1. Inicie sesión en la interfaz de usuario administrativa de SiteMinder. Haga clic en la ficha Infraestructura, Agentes, Expand Agent Configuration (Expandir configuración del agente) y, a continuación, haga clic en Modificar configuración del agente.
2. Busque el ACO. Busque el parámetro #LogoffUri. Haga clic en el botón de reproducción (flecha derecha) a la izquierda de ese parámetro.

3. Elimine el signo de almohadilla (#) del nombre del campo Valor e introduzca /idm/logout.jsp.
4. Haga clic en Aceptar y, a continuación, en Enviar para actualizar el objeto configuración del agente.

   La próxima vez que el agente recupere su configuración del servidor de políticas, se propagará la nueva configuración.

Resolución de problemas

En los siguientes temas se describen los errores comunes que se pueden producir. Siempre que sea posible, se equiparará una resolución con su error con el fin de prestar asistencia con la integración.

Ausencia de DLL de Windows

Síntoma:

Ausencia de DLL de Windows (MSVCP71.dll)

Se ha observado que después de que la conexión de SiteMinder se active, se produce un error de Java en el que se indica que falta una DLL (MSVCP71.dll).

Nota: Es posible que no se muestre este error si JBoss se ejecuta como servicio. En la medida de lo posible, pruebe la configuración sin ejecutar JBoss como servicio.

Solución:

Siga estos pasos:

1. Busque MSVCP71.dll en el servidor de políticas de SiteMinder, si se está ejecutando en Windows.
2. Copie esta DLL (MSVCP71.dll) en la carpeta \Windows\system32.
3. Después de colocar este archivo en la ubicación adecuada, regístrelo con el SO.
4. En una ventana de comandos, ejecute el comando regsvr32. Debe ser correcto siempre y cuando el archivo esté cargado.
5. Reinicie el servidor de aplicaciones.

Ubicación del servidor de políticas de SiteMinder incorrecta

Síntoma:

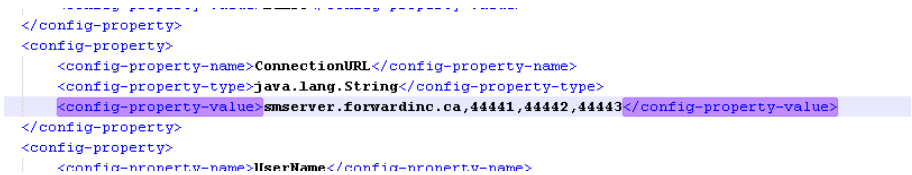
La ubicación del servidor de políticas de SiteMinder no es correcta.

Solución:

Se hace referencia a una ubicación incorrecta en ra.xml y se muestra el error Cannot connect to policy server: xxx (No se puede conectar al servidor de políticas: xxx).

Siga estos pasos:

1. Verifique el nombre de host que se ha proporcionado en ra.xml.



2. En la propiedad ConnectionURL, especifique el nombre de host del servidor de políticas de SiteMinder. Utilice un FQN (Nombre completo).

Nombre del administrador incorrecto

Síntoma:

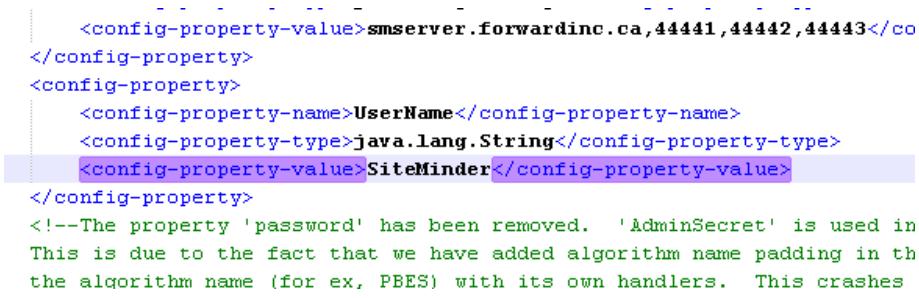
Nombre del administrador incorrecto

Solución:

Se hace referencia a un administrador incorrecto en ra.xml y se muestra el error Unknown administrator (Administrador desconocido).

Siga estos pasos:

1. Compruebe la propiedad UserName en ra.xml.



2. En la propiedad UserName, especifique la cuenta que se utiliza para comunicarse con CA SiteMinder. Por ejemplo, utilice la cuenta de SiteMinder (valor predeterminado).

Secreto de administrador incorrecto

Síntoma:

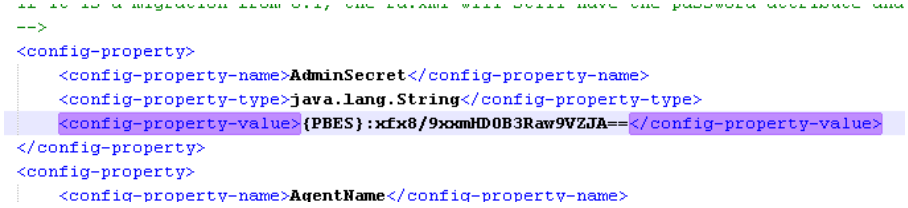
Secreto de administrador incorrecto

Solución:

Se utiliza un secreto de administrador incorrecto en ra.xml y se muestra el error Cannot connect to the policy server: Invalid credentials (No se puede conectar al servidor de políticas: credenciales no válidas).

Siga estos pasos:

1. Compruebe la propiedad AdminSecret en ra.xml.



2. En la propiedad AdminSecret, especifique la contraseña cifrada para el nombre de usuario al cual se hace referencia en la propiedad UserName.

Más información:

Modificación de un secreto compartido o una contraseña de SiteMinder (en la página 367)

Nombre de agente incorrecto

Síntoma:

Nombre de agente incorrecto

Solución:

Se utiliza un nombre de agente incorrecto en ra.xml y se muestra el error Cannot connect to the policy server: Failed to init Agent API: -1 (No se puede conectar al servidor de políticas: se ha producido un error al iniciar API de agente: -1).

Siga estos pasos:

1. Compruebe la propiedad AgentName en ra.xml.

```
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>idmagent</config-property-value>
</config-property>
<config-property>
```

2. Especifique el nombre de agente de 4.X creado durante el 3.º paso de la configuración de SiteMinder.

Secreto de agente incorrecto

Síntoma:

Secreto de agente incorrecto

Solución:

Se utiliza un secreto de agente incorrecto en ra.xml y se muestra el error Cannot connect to the policy server: Failed to init Agent API: -1 (No se puede conectar al servidor de políticas: se ha producido un error al iniciar API de agente: -1).

Siga estos pasos:

1. Compruebe la propiedad AgentSecret en ra.xml.

```
<config-property>
    <config-property-name>AgentSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
```

2. Especifique la contraseña cifrada que se ha utilizado al crear ese agente.

Más información:

Modificación de un secreto compartido o una contraseña de SiteMinder (en la página 367)

Ningún contexto del usuario en CA Identity Manager

Síntoma:

No existe ningún contexto del usuario en CA Identity Manager.

Si un usuario intenta acceder a CA Identity Manager sin una cookie SMSESSION, CA Identity Manager no podrá autenticar el usuario. En este caso, se mostrará la interfaz de usuario de CA Identity Manager vacía.

Si se tiene activado Flujo de trabajo para el entorno, se podrá ver un error como el siguiente:

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

Solución:

Pueden ser varias las causas de este error, pero normalmente es una de las siguientes:

- Se ha accedido directamente a CA Identity Manager.
- El agente de SiteMinder en el proxy está desactivado (es decir, no existe ningún elemento protegido). La cookie SMSESSION no se ha creado).
- El dominio de SiteMinder para el entorno de CA Identity Manager tiene una configuración errónea.

Las primeras dos causas son bastante directas. Es necesario asegurarse de que se accede a través del servidor web con el agente web completamente funcional activado. Sin embargo, si se accede a través del servidor web y el agente está activado; a continuación, se tendrá que modificar el dominio.

Siga estos pasos:

1. Inicie sesión en la interfaz de usuario administrativa de SiteMinder.
2. Busque el dominio de CA Identity Manager y haga clic en las capas para modificarlo. Haga clic en la ficha Territorio y, a continuación, seleccione el primer dominio de la lista.
3. La ubicación predeterminada de la barra diagonal es bajo el territorio. Suprímalo.
4. Haga clic en la regla bajo este territorio.

   El recurso efectivo predeterminado de la regla es un asterisco "*".
5. Agregue la barra diagonal "/" delante del asterisco.

   Se ha movido la barra diagonal del territorio a la regla. La protección es la misma, pero SiteMinder lo trata de forma diferente.

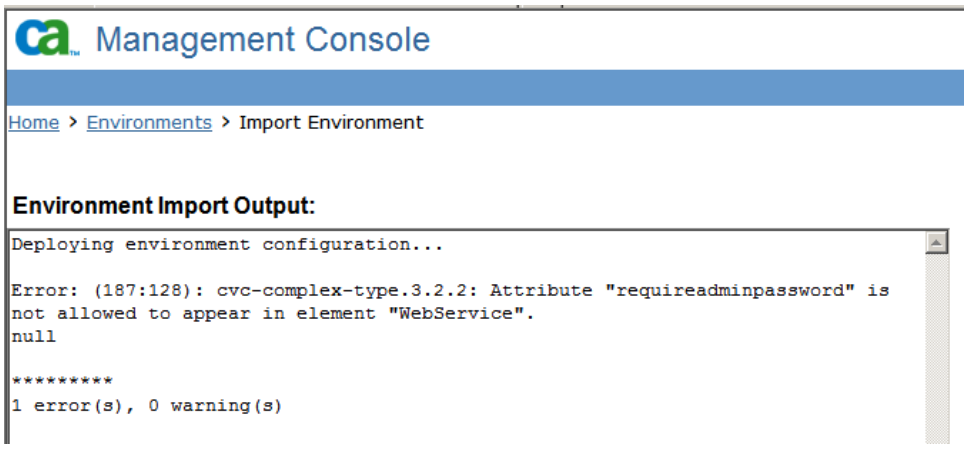
   Se puede iniciar sesión correctamente en CA Identity Manager a través de SiteMinder. Para validar la protección correcta, consulte los registros del agente de SiteMinder.

Error al cargar entornos

Síntoma:

Al volver a importar un entorno en CA Identity Manager después de integrarse con SiteMinder, se produce un error sobre el atributo requireadminpassword y el elemento WebService.

Nota: Esta incidencia puede producirse también cuando SiteMinder no forma parte de la implementación.



Solución:

Este error permite la implementación parcial del entorno. La implementación parcial puede crear elementos vacíos en el almacén de objetos de CA Identity Manager. Corrija uno de los XML de entorno y vuelva a importarlo.

Siga estos pasos:

1. Busque el archivo ZIP archivado y examínelo.
2. Cree una copia de XXX_environment_settings.xml.
3. Edite este archivo y busque el elemento WebService.
4. Suprima la etiqueta requireadminpassword=false.

   Nota: Elimine la etiqueta *y* el valor. No elimine solamente el valor.
5. Guarde los cambios y vuelva a colocar el archivo en el archivo ZIP.
6. Vuelva a importar el archivo ZIP de entorno archivado.

   No se tiene que suprimir el entorno que se ha creado a partir del intento erróneo. Al volver a importar un archivo corregido, se corrigen los errores del intento erróneo.

No se puede crear un directorio o entorno de CA Identity Manager

Síntoma:

No se puede crear un directorio o entorno de CA Identity Manager cuando se activa la integración de SiteMinder.

Solución:

Se puede producir esta incidencia debido a que falte una entrada en el registro.

Verifique que la configuración de registro siguiente existe en el equipo del servidor de políticas de SiteMinder:

- Solaris o Linux:

  Verifique que la entrada siguiente se encuentra en sm.registry:
  ImsInstalled=8.0; REG_SZ

- Windows:

  Verifique que la el parámetro de configuración ImsInstalled=8.0; REG_SZ se encuentra en la ubicación siguiente:
  HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

  Nota: Si la ruta de registro \Netegrity\SiteMinder\CurrentVersion no existe, créela manualmente.

Si se cambia el registro, es necesario asegurarse de reiniciar el servidor de políticas para que los cambios surtan efecto.

Importante: Antes de modificar el registro, se debe llevar a cabo una copia de seguridad completa del sistema.

El usuario no puede iniciar sesión

Síntoma:

Un usuario nuevo no puede iniciar sesión en un entorno con una contraseña no cifrada.

Solución:

Verifique que la siguiente clasificación de los datos no se incluya en la definición del atributo de contraseña del archivo de configuración del directorio (directory.xml):

<DataClassification name="AttributeLevelEncrypt"/>

En entornos que incluyan los componentes siguientes, al activar el cifrado de nivel de atributo se impide que los usuarios inicien sesión en:

- CA SiteMinder
- Una base de datos relacional

Cómo configurar parámetros de configuración del agente de CA Identity Manager

Cuando CA Identity Manager se integra con SiteMinder, CA Identity Manager utiliza un agente de CA Identity Manager integrado para comunicarse con el servidor de políticas de SiteMinder. Para ajustar el rendimiento, configure los parámetros de configuración de la conexión siguientes para el agente de CA Identity Manager.

1. Realice uno de los siguientes pasos:
   - Si CA Identity Manager se está ejecutando en un servidor de aplicaciones de WebLogic o WebSphere, edite el adaptador de recursos en el descriptor de conector de policyserver_rar de la consola del servidor de aplicaciones.
   - Si CA Identity Manager se está ejecutando en un servidor de aplicaciones de JBoss, abra policyserver-service.xml en <JBoss_home>\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.
2. Configure los siguientes parámetros de la siguiente forma:

   ConnectionMax

   Establece el número máximo de conexiones al servidor de políticas; por ejemplo, 20.

   ConnectionMin

   Establece el número mínimo de conexiones al servidor de políticas; por ejemplo, 2.

   ConnectionStep

   Establece el número de conexiones adicionales que se abrirán cuando todas las conexiones del agente estén en uso.

   ConnectionTimeout

   Especifica la cantidad de tiempo en segundos que se requiere para que el agente espere a conectarse a SiteMinder antes del tiempo de espera.
3. Reinicie el servidor de aplicaciones.

Configuración de alta disponibilidad de SiteMinder

Si se ha creado un clúster de servidor de políticas de SiteMinder, se puede configurar un clúster de servidor de aplicaciones con el fin de utilizarlo para equilibrio de carga y conmutación por error.

Siga estos pasos:

1. Edite el archivo ra.xml en esta ubicación:
   WebSphere:
   WAS_PROFILE/config/cells/*CELL_NAME*/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF
   Jboss:*jboss_home*/server/all/deploy/iam_im.ear/policyserver_rar/META-INF
   WebLogic: *wl_domain*/applications/iam_im.ear/policyserver_rar/META-INF
2. Modifique estos elementos, que se explican en las siguientes secciones:
   - Configuración de la conexión para el servidor de políticas
   - Número de servidores de políticas
   - La selección de equilibrio de carga o conmutación por error para el clúster.
3. Repita estos pasos para cada servidor de CA Identity Manager del clúster.
4. Reinicie el servidor de aplicaciones para que se apliquen los cambios.

Nota: Cuando se esté creando un directorio de CA Identity Manager o un entorno, o bien modificando un directorio o una configuración del entorno, se establecen los valores de conmutación por error de SiteMinder y FailoverServers en false. De lo contrario, el objeto del directorio se podría crear pero no replicarse a la vez que se utiliza. Por ejemplo, cree un directorio en el servidor 1. A continuación, cree un atributo mediante el ID de objeto de ese directorio en el servidor 2, pero el segundo directorio no existe todavía. Recibe el error No se ha encontrado el objeto.

Modificación de la configuración de la conexión del servidor de políticas

La Información de conexión del servidor de políticas debe reflejar el servidor primario para el entorno de producción. Esta información consta de ConnectionURL, el nombre de usuario y la contraseña correspondientes a la cuenta de administrador de SiteMinder, así como el nombre y el secreto compartido para el agente.

En el siguiente ejemplo, los valores editables aparecen en LETRAS MAYÚSCULAS.

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</co
nfig-
                property-value>
</config-property>
```

```
<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

Nota: Para los valores que requieren texto cifrado, utilice la herramienta de contraseña de CA Identity Manager. Para obtener más información, consulte la *Guía de configuración*.

Adición de más servidores de políticas

Para agregar más servidores de políticas a la instancia de instalación de CA Identity Manager, edite la entrada de FailoverServers en el archivo ra.xml.

Nota: Incluya el servidor de políticas primario y todos los servidores de conmutación por error en la entrada de FailoverServers.

Para cada servidor de políticas, introduzca una dirección IP y números de puerto para los servicios de autenticación, autorización y contabilidad. Utilice puntos y coma para separar entradas tal y como se muestra aquí:

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

Selección del equilibrio de carga o la conmutación por error

El comportamiento predeterminado de CA Identity Manager es utilizar el equilibrio de carga rotativo mediante los servidores que identifican ConnectionURL y FailoverServers. El equilibrio de carga se produce si se deja FailOver en false.

Para seleccionar la conmutación por error, establezca FailOver en true:

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

Eliminación de SiteMinder de una implementación de CA Identity Manager existente

En esta sección se proporcionan instrucciones detalladas para eliminar CA SiteMinder de un entorno de CA Identity Manager existente.

Siga estos pasos:

Importante: No se podrá acceder a la información del historial de contraseñas después de la migración.

1. Detenga el servidor de aplicaciones.
2. Desactive el servidor de políticas en el archivo ra.xml que se encuentra en \iam_im.ear\policyserver.rar\META-INF estableciendo el valor Activado de config-property en false
3. Edite el archivo web.xml que se encuentra en \iam_im.ear\User_console.war/WEB-INF y establezca la propiedad Activado de FrameworkAuthFilter en true.

   Nota: En WebSphere, el archivo web.xml se encuentra en *WebSphere_home*/AppServer/profiles/*Profile_name*/config/cells/*Cell_name*/applications/iam_im.ear/deployments/IdentityMinder/user_console.war/WEB-INF.

4. Inicie el servidor de aplicaciones.
5. (Solamente WebSphere) Actualice el objeto policyServer en la Consola de administración con mismo valores que en el archivo ra.xml.

Operaciones de la SiteMinder

En las secciones siguientes se explica cómo modificar las funciones de SiteMinder, incluidos los dominios de política y esquemas de autenticación, con el fin de que sean compatibles con CA Identity Manager:

Recolección de credenciales de usuario mediante un esquema de autenticación personalizado (en la página 348)

Cambia el método que CA Identity Manager utiliza para recolectar credenciales para los usuarios que intentan acceder a un entorno de CA Identity Manager.

Configuración de roles de acceso (en la página 349)

Proporciona acceso a las funciones de una aplicación.

Configuración de la dirección URL de cierre de sesión (en la página 364)

Impide el acceso no autorizado a un entorno de CA Identity Manager imponiendo un cierre de cierre de sesión completo.

Actualización de un alias en territorios de SiteMinder (en la página 365)

Actualiza los territorios que protegen un entorno de CA Identity Manager cuando se cambia el alias del entorno.

Contraseñas de SiteMinder (en la página 367)

Permite cambiar la contraseña de la cuenta de administrador que CA Identity Manager utiliza para comunicarse con SiteMinder, así como el secreto compartido para el agente de SiteMinder que protege un entorno de CA Identity Manager.

Configuración de parámetros de configuración del agente de CA Identity Manager (en la página 343)

Ajusta el rendimiento del agente de CA Identity Manager que se comunica con el servidor de políticas de SiteMinder.

Uso de directorios diferentes para autenticación y autorización (en la página 368)

Permite a los administradores que tienen perfiles en un directorio que gestionen usuarios en un directorio diferente.

Mejora del rendimiento de operaciones de directorio LDAP (en la página 370)

Aumenta el rendimiento de solicitudes de CA Identity Manager en el almacén de usuarios configurando SiteMinder para abrir varias conexiones en el mismo directorio.

Recolección de credenciales de usuario mediante un esquema de autenticación personalizado

SiteMinder utiliza un esquema de autenticación para recolectar credenciales de usuario y determinar la identidad de un usuario en el inicio de sesión. Una vez que se identifique un usuario, CA Identity Manager genera una Consola de usuario personalizada que se basa en los privilegios del usuario.

Se puede implementar cualquier esquema de autenticación de SiteMinder para proteger un entorno de CA Identity Manager.

Por ejemplo, se puede implementar un esquema de autenticación de formularios HTML, que recolecta credenciales en un formulario HTML. Al utilizar un formulario HTML, se permite crear una página de inicio de sesión que puede incluir elementos de marca, como un logotipo de la compañía, y que se vincula a las páginas de contraseña olvidada y autorregistro.

Nota: Para obtener información sobre los esquemas de autenticación, consulte la *Guía de configuración del servidor de políticas de SiteMinder de CA*.

Siga estos pasos:

1. Inicie sesión en una de las interfaces siguientes:
   - Para CA SiteMinder Web Access Manager r12 o posterior, inicie sesión en la interfaz de usuario administrativa.
   - Para CA eTrust SiteMinder 6.0 SP5, inicie sesión en la interfaz de usuario del servidor de políticas.

   Nota: Para obtener información sobre el uso de estas interfaces, consulte la documentación de la versión de SiteMinder que esté utilizando.
2. Cree un esquema de autenticación tal y como se describe en la *Guía de configuración del servidor de políticas de SiteMinder de CA*.
3. Modifique el territorio que protege el entorno de CA Identity Manager adecuado para utilizar el esquema de autenticación creado en el paso 1.

   El nombre de territorio utiliza el formato siguiente:

   *Identity Manager-environment*_ims_realm

   Nota: Si se ha configurado la compatibilidad con tareas públicas, verá un territorio adicional *Identity Manager-environment*_pub_realm. Este territorio utiliza un esquema de autenticación anónimo para permitir que los usuarios desconocidos utilicen las funciones de autorregistro y de contraseña olvidada sin proporcionar credenciales. No modifique los esquemas de autenticación para estos territorios.

Importación de definiciones de datos en el almacén de políticas

Se puede controlar el acceso de un usuario a funciones de la aplicación mediante políticas de SiteMinder. Entre la instalación del servidor se incluyen las definiciones de datos obligatorias para permitir este control. Importe el archivo IdmSmObjects.xdd de esta ubicación:

siteminder_home\xps\dd

siteminder_home es la ruta de instalación del servidor de políticas.

Planificación de roles de acceso

Para controlar el acceso a las aplicaciones, cree roles de acceso y tareas. Una tarea de acceso proporciona acceso a una función de una aplicación. Un rol de acceso contiene una o más tareas de acceso a una o más aplicaciones. Cuando a un usuario se le ha asignado un rol de acceso, este puede utilizar las funciones que existen en ese rol.

Los roles de acceso para acceso a aplicaciones proporcionan más detalles sobre la finalidad de los roles de acceso.

Los roles de acceso requieren configuración en Identity Manager y SiteMinder. En el proceso, participan dos administradores:

- Administrador de Identity Manager: debe ser capaz de crear roles de acceso y tareas en Identity Manager. Entre los roles de gestor del sistema y el gestor de roles de acceso predeterminados se incluyen estas tareas.
- Administrador de SiteMinder: debe tener el ámbito Sistema y poder gestionar objetos de sistema y dominio. Consulte la sección de *diseño de políticas de CA eTrust SiteMinder* para obtener más información.

Nota: La interfaz de usuario de diseño de políticas utiliza el *entorno de Identity Manager* de término para hacer referencia a lo que se denomina ahora *"entorno de Identity Manager"*. Además, en la documentación de SiteMinder que se proporciona con este producto, se le denomina *"Identity Manager"*. A partir de la versión r8.1, el nuevo nombre de producto nuevo es *"Identity Manager"*.

El procedimiento siguiente describe los pasos para crear un rol de acceso:

1. Un administrador de Identity Manager con el rol de gestor de rol de acceso:
   a. Crea tareas de acceso.
   b. Crea un rol de acceso.
   c. Comunica la información de roles y tareas al administrador de SiteMinder.

2. Un administrador de SiteMinder crea una política de control de acceso basada en roles de la siguiente forma:

   a. Asignando un directorio de usuarios asociado a uno o más entornos de Identity Manager a un dominio de la política.

   b. Asociando uno o más entornos de Identity Manager con el dominio de la política en el paso 1.

   c. Creando territorios y reglas en el dominio de la política (si no existen aún). Los territorios y las reglas se deben corresponder con los recursos a los cuales los roles de acceso concederán acceso.

   d. Creando políticas y enlazándolas a roles del entorno de Identity Manager.

   e. (opcional) Especificando respuestas que proporcionan información de autorización para acceder a los recursos protegidos.

   Consulte la sección de *diseño de políticas de CA eTrust SiteMinder* para obtener instrucciones sobre los anteriores pasos.

Activación de roles de acceso para utilizarlos con SiteMinder

Para utilizar roles de acceso con CA SiteMinder, CA Identity Manager refleja todos los objetos del almacén de objetos de CA Identity Manager relacionados con esos roles de acceso en el almacén de políticas de SiteMinder. Para permitir que esto suceda, configure una propiedad en la Consola de gestión de CA Identity Manager.

Para activar roles de acceso para utilizarlos con SiteMinder

1. Abra la Consola de gestión.
2. Seleccione Environment (Entorno), *Your Environment (Su entorno)*, Advanced Settings (Configuración avanzada), Miscellaneous (Opciones varias).
3. Agregue una nueva propiedad proporcionando la siguiente información:
   - En el campo Property (Propiedad) , introduzca lo siguiente:

     EnableSMRBAC
   - En el campo Value (Valor), introduzca lo siguiente:

     true

4. Haga clic en Agregar. A continuación, haga clic en Guardar.

   Se muestra un mensaje en el que se indica que se debe reiniciar el entorno.

5. Haga clic en Restart Environment.

   CA Identity Manager ahora es compatible con los roles de acceso y las tareas para utilizarlos con CA SiteMinder.

Una vez que se activan roles de acceso para utilizarlos con CA SiteMinder, se debe tener en cuenta lo siguiente:

- Si se han utilizado roles de acceso en CA Identity Manager r8x, es necesario realizar un paso de migración adicional para gestionar esos roles de acceso en la versión actual de CA Identity Manager. Para obtener más información, consulte la *Guía de actualización*.
- Para desactivar la compatibilidad con los roles de acceso en SiteMinder, suprima el rol de acceso de CA Identity Manager y los objetos de tarea del almacén de políticas de SiteMinder. A continuación, elimine la propiedad EnableSMRBAC de la lista Miscellaneous Properties (Propiedades de opciones varias) y reinicie el entorno.

Adición de tareas de acceso a roles de administrador

De forma predeterminada, las tareas de Tareas de acceso no se muestran en la ficha de roles y tareas; es necesario agregar las tareas de acceso al rol de administrador del usuario que ha iniciado sesión.

Siga estos pasos:

1. Inicie sesión en una cuenta de CA Identity Manager con un rol que incluya permisos para una tarea de crear roles de acceso.
2. Haga clic en Roles y tareas, Modificar rol de administrador.
3. Seleccione el rol del administrador de usuario que ha iniciado sesión.
4. Haga clic en la ficha Tareas, en el campo Filtrar por categoría y seleccione los roles y las tareas del menú desplegable.
5. Seleccionar Crear tarea de acceso del menú desplegable Agregar tarea.
6. Haga clic en Enviar.

Creación de una tarea de acceso

Una tarea de acceso es una única acción que puede realizar un usuario en una aplicación de negocio, como generar una orden de compra en una aplicación de finanzas. Los usuarios pueden realizar esa acción cuando se les asigne un rol de acceso que incluya la tarea de acceso.

Importante: Para crear tareas de acceso, es necesario agregar las tareas de acceso (en la página 351) a un rol de administrador del usuario que ha iniciado sesión.

Siga estos pasos:

1. Seleccione Roles y tareas, Tareas de acceso, Crear tarea de acceso.
2. Seleccione una de las siguientes opciones:
   - Creación de una tarea de acceso.
   - Creación de copias de una tarea de acceso.
3. Complete estos campos:

   Nombre

   Un nombre único que se puede asignar a la tarea, como "generar orden de compra"

   Etiqueta

   Una etiqueta única para la tarea. La etiqueta debe comenzar con una letra o guión bajo y contener sólo letras, números o guiones bajos.

   Descripción

   Una nota opcional sobre la finalidad de la tarea.

   ID de aplicación

   Un identificador para una aplicación; por ejemplo, el nombre de la aplicación asociado a la tarea. El ID de la aplicación no puede contener espacios ni caracteres que no sean alfanuméricos.

   Anotar este ID; se necesitará cuando se active el rol en SiteMinder.
4. Para completar la tarea de acceso, haga clic en Enviar.

Cómo crear un rol de acceso

Un rol de acceso contiene tareas de acceso, que proporcionan acceso a las funciones de una aplicación. Por ejemplo, un rol puede contener tareas que permitan que los miembros del rol coloquen una orden en una aplicación de compra y actualicen las cantidades en una aplicación de control de inventario.

Complete los siguientes pasos para crear un rol de acceso:

1. Inicie la creación del rol de acceso. (en la página 353)
2. Defina las propiedades básicas para el rol de acceso en la ficha Perfil. (en la página 353)
3. Seleccione las tareas de acceso para el rol. (en la página 354)
4. Defina políticas de miembros para el rol. (en la página 355)
5. Defina las políticas de administración para el rol. (en la página 355)
6. Defina las reglas de propietarios para el rol. (en la página 356)

Inicio de la creación de la función de acceso

1. Inicie sesión en una cuenta de Identity Manager con una función que incluya una tarea para crear funciones de acceso.
2. Haga clic en Funciones de acceso, Crear función de acceso.

   Seleccione la opción para crear una nueva función o una copia de una función. Si selecciona Copiar, busque la función.
3. Continúe con la siguiente sección, Definición del perfil de la función de acceso.

Definición del perfil de la función de acceso

Para definir el perfil de la función de acceso

1. Introduzca el nombre, la descripción y complete los atributos personalizados definidos para la función.

   Nota: Puede especificar atributos personalizados en la ficha Perfil que especifica información adicional acerca de los roles de acceso. Esta información adicional se puede usar para simplificar la búsqueda de roles en entornos que incluyan un gran número de roles.
2. Seleccione Activado si está listo para dejar la función disponible para ser utilizada en cuanto la haya creado.
3. Continúe con la siguiente sección, Definición de las políticas de miembros de la función de acceso.

Selección de las tareas de administración para el rol

En la ficha Tareas:

1. Seleccione las tareas que se incluirán en este rol. En primer lugar, seleccione las aplicaciones y, a continuación, la tarea. Se pueden incluir tareas de acceso desde diferentes aplicaciones:

   Nota: Si otro rol tiene las tareas que necesita, haga clic en Copiar tareas de otro rol. Se puede editar la lista que se muestra.

   Al crear un rol o una tarea, se mostrarán iconos para agregar, editar o eliminar elementos:

   Continúe o seleccione el elemento actual para ver o editarlo.

   Si JavaScript se desactiva, haga clic en el botón de avance para seleccionar elementos de una lista desplegable.

   Vuelva o deshaga una selección anterior.

   Inserte un elemento; por ejemplo, una tarea o una regla.

   Suprima la tarea actual o, en una regla, la expresión que sigue.

   Mueva el elemento actual hacia arriba en la lista.

   Mueva el elemento actual hacia abajo en la lista.

2. Continúe con la siguiente sección, Definición de las políticas de miembros de la función de acceso.

Definición de las políticas de miembros de la función de acceso.

Una política de miembros define una regla de miembros y reglas de ámbito para un rol. Se pueden definir varias políticas de miembros para un rol. Para cada política, los usuarios que cumplen la condición en la regla de miembros tienen el alcance para utilizar el rol que se define en la política.

Siga estos pasos:

1. Seleccione la ficha Miembros.
2. Haga clic en Agregar para definir más políticas de miembros.
3. (Opcional) En la página de política de miembros, defina si lo desea una regla de miembro para que quien vaya a utilizar este rol.

   Al definir una regla de miembro, se asigna automáticamente el rol a los usuarios que coinciden con los criterios en la política de miembros.

   Nota: Defina políticas de miembros que utilizan solamente atributos de directorio; por ejemplo: title=Gestor. Si se definen políticas de miembros que hacen referencia a los objetos que no se encuentran almacenados en el directorio de usuarios como roles de administración, SiteMinder no puede ser capaz de resolver la referencia.
4. Verifique que la política de miembros se muestra en la ficha Miembros.

   Para editar una política, haga clic en el símbolo de flecha a la izquierda. Para eliminarla, haga clic en el icono con el signo menos.
5. En la ficha Miembros, permita que los administradores puedan agregar y eliminar miembros de esta casilla de verificación de roles.

   Una vez que se activa esta función, defina la acción Agregar y la acción Eliminar. Estas acciones definen lo que sucede cuando un usuario se agrega o se elimina como miembro del rol.

Definición de las políticas de administración de la función de acceso.

Una política de administración define reglas de administración, reglas de ámbito y privilegios de administrador para un rol. Se pueden definir varias políticas de administración para un rol. Cada política indica que si un administrador cumple la condición en la regla de administración, tendrá el alcance y los privilegios de administrador que se han definido para la política.

Siga estos pasos:

1. Seleccione la ficha Administradores para el rol de acceso.
2. Si se desea poner disponible la opción Gestionar administradores, permita que los administradores puedan agregar y eliminar administradores de esta casilla de verificación de roles.

   Una vez que se activa esta función, defina las acciones correspondientes a cuando un usuario se agrega o se elimina como administrador del rol.

3. En la ficha Administradores, agregue políticas de administración que incluyan privilegios de administrador y reglas de ámbito. Cada política necesita como mínimo un privilegio (Gestionar miembros o Gestionar administradores).

   Se pueden agregar varias políticas de administración con reglas y privilegios diferentes para los administradores que cumplen la regla.

   Nota: Defina políticas de administración que utilizan solamente atributos de directorio; por ejemplo: title=Gestor. Si se definen políticas de miembros que hacen referencia a los objetos que no se encuentran almacenados en el directorio de usuarios como roles de administración, SiteMinder no puede ser capaz de resolver la referencia.

4. Para editar una política, haga clic en el símbolo de flecha a la izquierda. Para eliminarla, haga clic en el icono con el signo menos.

5. Continúe con la siguiente sección, Definición de las reglas de propietarios de la función de acceso.

Definición de las reglas de propietarios de la función de acceso.

Una regla de propietarios define quién puede modificar un rol. Se pueden definir varias reglas de propietarios para un rol.

Siga estos pasos:

1. Seleccione la ficha Propietarios para el rol de acceso.

2. Defina reglas de propietario, que determinan qué usuarios pueden modificar el rol.

   Nota: Defina reglas de propietarios que utilicen solamente atributos de directorio; por ejemplo: title=Gestor. Si se definen reglas de propietarios que hacen referencia a los objetos que no se encuentran almacenados en el directorio de usuarios como roles de administración, SiteMinder no puede ser capaz de resolver la referencia.

3. Haga clic en Enviar.

   Se muestra un mensaje para indicar que se ha enviado la tarea. Se puede producir un retraso momentáneo antes de que un usuario pueda utilizar el rol.

Activación de roles de acceso en SiteMinder

Un administrador de SiteMinder enlaza roles con políticas de seguridad que definen cómo interactúan los usuarios con los recursos. Las políticas pueden vincularse a los objetos siguientes:

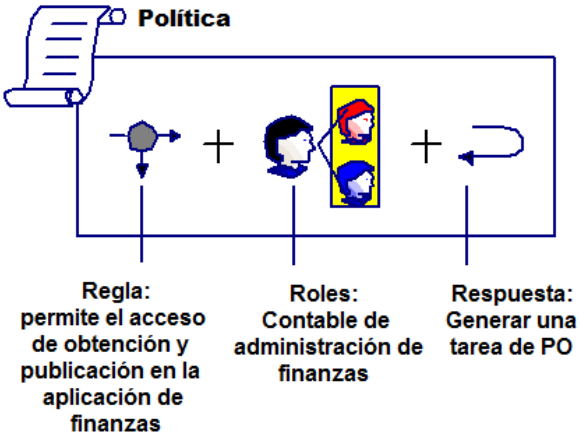
- Usuarios y grupos de usuarios: identifican un conjunto de usuarios a los que le afecta una política.
- Roles: identifican usuarios a los que se les ha asignado un conjunto de privilegios en Identity Manager.
- Reglas: identifican un recurso y las acciones que se permiten o se deniegan para el recurso. El recurso es normalmente una dirección URL, una aplicación o un script.

- Respuestas: determinan la reacción a una regla. Cuando se activa una regla, se devuelven respuestas a un agente de CA SiteMinder.

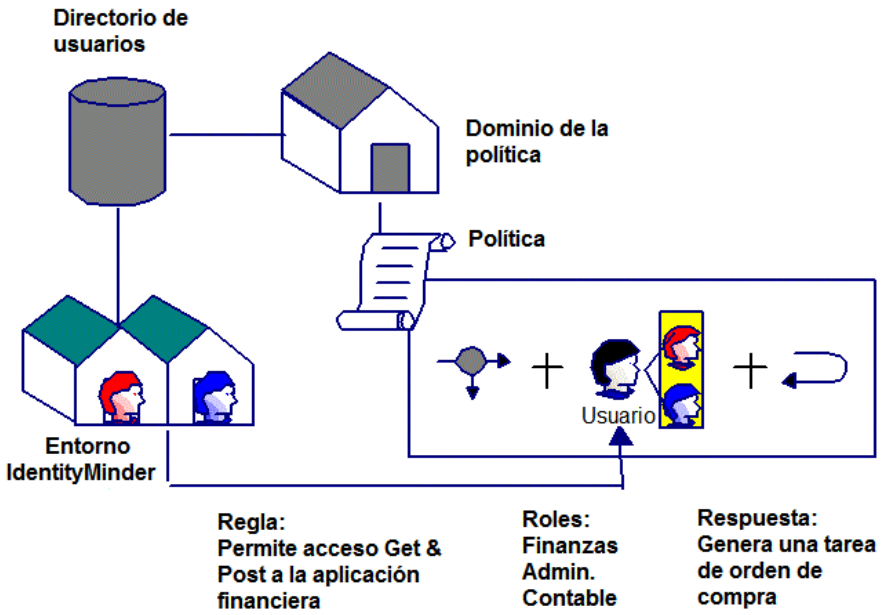
  Identity Manager utiliza respuestas de SiteMinder para proporcionar información de tareas y roles específicas para un recurso protegido.

Se pueden enlazar políticas de SiteMinder con usuarios, con roles, o bien con usuarios *y* roles. Cuando un usuario o miembro del rol intenta acceder a un recurso protegido, SiteMinder utiliza la información de la política para determinar si conceder acceso y activar las respuestas.

En la siguiente ilustración se muestra la relación de los objetos de política en una política basada en roles.



Las políticas de SiteMinder se crean en dominios de política, que vinculan de forma lógica directorios de usuarios con recursos protegidos. En la siguiente ilustración se muestra la relación de los objetos de política en una política basada en roles.



Para proporcionar autorizaciones de usuario a una aplicación protegida, un administrador de SiteMinder empareja una regla en la política de la aplicación con una respuesta. La respuesta contiene un atributo de respuesta que genera SiteMinder y que recupera la información de autorización de Identity Manager.

Cuando SiteMinder autoriza un miembro del rol a un recurso protegido, se producen los siguientes eventos:

1. La regla de la política se ejecuta en SiteMinder, por lo que se activa la respuesta emparejada.
2. El servidor de políticas obtiene la información de autorización de Identity Manager para que se incluya en una respuesta.
3. El servidor de políticas transfiere el atributo de respuesta al Agente Web.
4. El Agente Web pone la información de autorización disponible para la aplicación como una variable del encabezado HTTP o una cookie.

Atributos de respuesta que genera SiteMinder

Identity Manager transfiere la información de autorización a las aplicaciones mediante las respuestas del Agente Web de SiteMinder. Estas respuestas contienen variables de encabezado HTTP en atributos de respuesta, que puede utilizar la aplicación para determinar los privilegios de acceso de un usuario. Las respuestas se incluyen en las políticas de SiteMinder, que determinan cómo interactúan los usuarios con un recurso protegido.

Los administradores de SiteMinder pueden configurar una respuesta que incluya dos tipos de atributos de respuesta para transferir la información a una aplicación:

- SM_USER_APPLICATION_ROLES[:*application id*]: devuelve una lista de roles asignados a un usuario.
- SM_USER_APPLICATION_TASKS[:*application id*]: devuelve una lista de tareas que puede realizar un usuario según los roles que se les haya asignado.

El ID de la aplicación limita el conjunto solicitado de roles y tareas a una aplicación específica. Por ejemplo, si se crea el atributo de respuesta siguiente:

SM_USER_APPLICATION_ROLES:Finance_application

SiteMinder devuelve los roles que tienen tareas en la aplicación de contabilidad al agente web, que a continuación transfiere la información a la aplicación de finanzas.

Nota: El *ID de la aplicación* proporcionado debe coincidir con un *ID de la aplicación* proporcionado al utilizar Crear tarea de acceso en Identity Manager. Si no se ha creado todavía la tarea, el ID de la aplicación puede ser cualquier nombre que seleccione, pero no puede contener espacios o caracteres que no sean alfanuméricos.

Se pueden especificar varios ID de aplicación en una lista delimitada por comas con objeto de devolver el conjunto de roles y tareas desde varias aplicaciones en un atributo de respuesta único. Por ejemplo, para devolver la lista de roles que un usuario tiene en la aplicación de compra y finanzas, especifique lo siguiente

SM_USER_APPLICATION_ROLES:Finance, Purchasing

Lista de comprobación para activar roles de acceso en SiteMinder

Nota: Durante los siguientes pasos se asume que SiteMinder protege ya la aplicación a la cual aplica el rol de acceso que se va a crear. Si va a crear un rol de acceso para una aplicación que SiteMinder no protege, consulte la guía *CA eTrust SiteMinder Policy Design* para obtener instrucciones sobre cómo configurar la aplicación en SiteMinder.

✓	Paso	Consulte...
	1. En la Interfaz de usuario del servidor de políticas, asigne el directorio de usuarios que se asocia al entorno de Identity Manager a un dominio de la política.	*Diseño de políticas de CA eTrust SiteMinder*
	2. Agregue el entorno de Identity Manager al dominio de SiteMinder que protege la aplicación en la que se aplica el rol de acceso.	*Diseño de políticas de CA eTrust SiteMinder*
	3. En el dominio de la política, cree dominios y reglas (si no existen aún) que se correspondan con los recursos a los cuales el rol de acceso concederá acceso.	*Diseño de políticas de CA eTrust SiteMinder*
	4. Creae una respuesta para transferir información de autorización al recurso.	Creación de una respuesta de SiteMinder (en la página 361)
	5. Cree una política y asóciela a lo siguiente: ■ El rol creado en Identity Manager. ■ Los territorios y las reglas creadas en el paso 2. ■ Las respuestas creadas en el paso 4.	*Diseño de políticas de CA eTrust SiteMinder*

Adición de entornos de Identity Manager a un dominio de la política

Para activar SiteMinder con el fin de que sea compatible con roles de acceso, asocie un entorno de CA Identity Manager a un directorio de usuarios y un dominio de la política en SiteMinder.

Nota: Agregue el almacén de usuarios asociado al entorno de CA Identity Manager al dominio de la política *antes* de poder agregar el entorno de CA Identity Manager al dominio de la política.

Para agregar un entorno de CA Identity Manager a un dominio de la política

1. En el cuadro de diálogo Dominio de la política en la interfaz de usuario del servidor de políticas, agregue el almacén de usuarios asociado al entorno de CA Identity Manager con un dominio de la política tal y como se muestra a continuación:
   a. Seleccione la ficha Directorios de usuarios.
   b. En el cuadro de lista desplegable del final de la ficha, seleccionar el directorio de usuarios que se incluirá en el dominio de la política.
   c. Haga clic en el botón Agregar.

      La Interfaz de usuario del servidor de políticas agrega el directorio a la lista que se muestra en la ficha Directorios de usuarios.
   d. Haga clic en Apply (Aplicar).
2. Agregue el entorno de CA Identity Manager al dominio de la política tal y como se muestra a continuación:
   a. Seleccionar la ficha Entornos de CA Identity Manager.
   b. Seleccione el entorno de CA Identity Manager que se desea asociar al dominio de la política de la lista desplegable en la parte superior de la ficha.
   c. Haga clic en Agregar.

      La Interfaz de usuario del servidor de políticas agrega la selección a la lista de entornos de CA Identity Manager en la parte superior de la ficha.
3. Haga clic en Aceptar para guardar las selecciones y cierre el cuadro de diálogo.

   Los entornos de CA Identity Manager seleccionados están disponibles al crear políticas.

Creación de una respuesta de SiteMinder

1. Inicie sesión en la interfaz de usuario del servidor de políticas.
2. En función de los privilegios administrativos, realice una de las siguientes tareas:
   - Si se tiene el privilegio Gestionar objetos del sistema y dominio:
     a. En el panel Objeto, haga clic en la ficha Dominios.
     b. Seleccione el dominio de la política a la que desee agregar una respuesta.
   - Si se tiene el privilegio Manage Domain Objects (Gestionar objetos de dominio), seleccione el dominio de la política en el que se desea agregar una respuesta en el panel Objeto.
3. En la barra de menús, seleccione Editar, <nombre de dominio>, Crear respuesta.

   Se abrirá el cuadro de diálogo de respuesta de SiteMinder (consulte el cuadro de diálogo de respuesta).
4. Introduzca un nombre y una descripción para la nueva respuesta.

5. En el cuadro de grupo Tipo de agente, seleccione el botón de opción de SiteMinder.
6. Seleccione la opción Agente Web en la lista desplegable en el cuadro de grupo Tipo de agente y haga clic en Aplicar para guardar los cambios.
7. Haga clic en Crear.

   Se abrirá el cuadro de diálogo de editor de atributos de respuesta de SiteMinder.
8. En la lista desplegable de atributos, seleccione el atributo de respuesta WebAgent-HTTP-Header-Variable.
9. En la ficha de configuración de atributos, seleccione el botón de opción Atributo de usuario.
10. En el campo Variable, introduzca el nombre de la variable que se transferirá a la aplicación.

    Por ejemplo, si se especifica la variable TASKS, se devuelve el encabezado siguiente a la aplicación:

    HTTP_TASKS
11. En el campo Nombre del atributo, especifique el atributo de respuesta como se muestra a continuación:

    - SM_USER_APPLICATION_ROLES[:*application id1, application_id2, ...application_idn*]: devuelve una lista de roles asignados a un usuario.
    - SM_USER_APPLICATION_TASKS[:*application id1, application_id2, ...application_idn*]

    Se proporciona más información en Atributos de respuesta que genera SiteMinder (en la página 359).
12. Haga clic en Aceptar para guardar los cambios y volver a la ventana de administración de SiteMinder.

Adición de roles a una política de SiteMinder

Cuando un usuario al que se le ha asignado el rol de acceso adecuado intenta acceder a un recurso protegido, el servidor de políticas de SiteMinder verifica que al usuario se le ha asignado el rol de acceso y, a continuación, desencadena las reglas incluidas en la política para ver si al usuario se permite acceder al recurso.

Para agregar roles de acceso a una política de SiteMinder

1. En el cuadro de diálogo de políticas de SiteMinder, haga clic en la ficha Usuarios.

   La ficha Usuarios contiene fichas para cada directorio de usuarios y entorno de CA Identity Manager incluido en el dominio de la política.
2. Seleccione el entorno de CA Identity Manager que contenga los roles que se desean agregar a la política.

3. Haga clic en el botón Agregar/Eliminar.

   Se abrirá el cuadro de diálogo del rol de Identity Manager de la política de SiteMinder.

4. Para agregar roles a la política, seleccione una entrada en la lista de miembros disponibles y muévala a la lista de miembros actuales.

5. Haga clic en Aceptar para guardar los cambios y vuelva al cuadro de diálogo de políticas de SiteMinder.

Exclusión de roles en una política

Además de utilizar roles de acceso para conceder acceso a aplicaciones, también se pueden utilizar roles de acceso para evitar que los miembros de roles de acceso accedan a una aplicación. Para evitar que los miembros de un rol de acceso accedan a una aplicación, se excluyen los roles de las políticas de SiteMinder. Cuando un usuario al cual se le ha asignado el rol de acceso excluido en CA Identity Manager intenta acceder a un recurso protegido, el servidor de políticas verifica la exclusión del rol de CA Identity Manager del usuario asignado. Al realizar la verificación, se bloquea el acceso al recurso.

Siga estos pasos:

1. En el cuadro de diálogo de políticas de SiteMinder, haga clic en la ficha Usuarios.

   La ficha Usuarios contiene fichas para cada directorio de usuarios y entorno de CA Identity Manager incluido en el dominio de la política.

2. Haga clic en el entorno de CA Identity Manager que contenga los roles que desee excluir de la política.

3. Haga clic en el botón Agregar/Eliminar.

   Se abre el cuadro de diálogo de rol de CA Identity Manager de políticas de SiteMinder.

4. Para agregar roles a la política, seleccione una entrada en la lista de miembros disponibles y haga clic en el botón de flecha izquierda, que apunta a la lista de miembros actuales.

   El procedimiento opuesto elimina los roles de la lista de miembros actuales.

5. En la lista de miembros actuales, seleccione los roles que se desean excluir y haga clic en el botón Excluir que se encuentra en la lista.

   Aparecerá un círculo rojo con una barra diagonal a la izquierda de los roles excluidos.

6. Haga clic en Aceptar para guardar los cambios y vuelva al cuadro de diálogo de políticas de SiteMinder.

Configuración del URI LogOff

Para proteger un entorno de CA Identity Manager, configure el agente Web de SiteMinder que protege el entorno para terminar una sesión de usuario después de que el usuario cierre sesión en CA Identity Manager.

El agente Web termina una sesión de usuario suprimiendo la sesión de SiteMinder y las cookies de autenticación del explorador Web y dando instrucciones al servidor de políticas de que elimine toda información de sesión.

Para terminar la sesión de SiteMinder, configure la funcionalidad de cierre de sesión en el campo LogOffURI del objeto de configuración del agente para el agente de SiteMinder que protege el entorno de CA Identity Manager.

Notas:

- Un agente de SiteMinder tiene un URI LogOff. Todas las aplicaciones protegidas por el agente usan la misma página de cierre de sesión.
- Cuando se configuran páginas de cierre de sesión personalizadas en la Consola de gestión como se describe en la sección acerca de la configuración de páginas de cierre de sesión personalizadas, CA Identity Manager envía la solicitud de cierre de sesión a la página de cierre de sesión personalizada *y* el URI LogOff. Sin embargo, CA Identity Manager muestra solamente la página de cierre de sesión personalizada al usuario.

Siga estos pasos:

1. Inicie sesión en una de las interfaces siguientes:
   - Para CA SiteMinder r12 o superior, inicie sesión en la interfaz de usuario administrativa.
   - Para CA eTrust SiteMinder 6.0 SP5, inicie sesión en la interfaz de usuario del servidor de políticas.

   Nota: Para obtener información sobre el uso de estas interfaces, consulte la documentación de la versión de SiteMinder que esté utilizando.

2. Modifique la propiedad #LogOffUri en el objeto configuración del agente para el agente que protege el entorno de CA Identity Manager como se muestra a continuación:
   - Elimine el signo de almohadilla (#).
   - En el campo Valor, especifique el URI siguiente:

     /iam/im/logout.jsp

   Nota: Se selecciona un objeto de configuración del agente cuando se instala el agente Web. Para obtener más información, consulte la *Guía de instalación del servidor de políticas del gestor de acceso Web de CA SiteMinder*.
3. Guarde los cambios.
4. Reinicie el servidor Web.

Alias en territorios de SiteMinder

Un *alias* es una cadena única que se agrega a la dirección URL para acceder a un entorno de CA Identity Manager. Por ejemplo, cuando el alias de un entorno es *employees*, la dirección URL para acceder a ese entorno es la siguiente:

`http://myserver.mycompany.org/iam/im/employees`

myserver.mycompany.org

Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager.

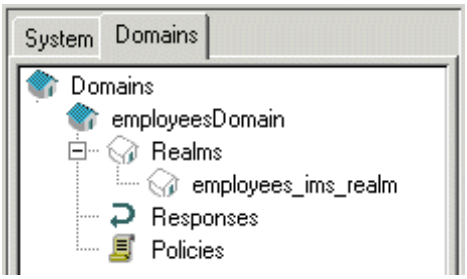
Especifica como mínimo un alias cuando se crea un entorno de CA Identity Manager en la Consola de gestión. (También se puede especificar un alias público).

SiteMinder utiliza el nombre del entorno para darle nombre a los objetos que protegen el entorno. Por ejemplo, cuando se especifica el nombre *employees*, SiteMinder crea objetos llamados *employeesobject_type*.

object_type

Define el objeto de SiteMinder, como employees_ims_realm.

La siguiente ilustración muestra dos de los objetos que crea SiteMinder:



Actualización de un alias en territorios de SiteMinder

Si se modifica el alias protegido o público en la Consola de gestión, CA Identity Manager intenta actualizar los nombres de alias en el servidor de políticas. Si CA Identity Manager no puede actualizar los nombres, se pueden actualizar manualmente en una de las interfaces siguientes:

- Para CA SiteMinder Web Access Manager r12 o posterior, se utiliza la interfaz de usuario administrativa.
- Para CA eTrust SiteMinder 6.0 SP5, se utiliza la interfaz de usuario del servidor de políticas.

Siga estos pasos:

1. Busque los territorios para el entorno de CA Identity Manager.

   Estos territorios se crean automáticamente (junto con otros objetos de SiteMinder obligatorios) cuando CA Identity Manager se integra con SiteMinder.

   Los territorios utilizan la convención de denominación siguiente:

   - *Identity Manager-environment*_ims_realm: protege la Consola de usuario.
   - *Identity Manager-environment*_pub_realm: permite la compatibilidad con tareas públicas, como las de autorregistro y contraseña olvidada. Este territorio aparece solamente si se ha configurado un alias público.

     Nota: Si se está utilizando la interfaz de usuario del servidor de políticas para modificar el territorio, busque el territorio de la política (*Identity Manager-environment*Domain) para el entorno de CA Identity Manager primero. Los territorios se encuentran bajo el dominio.

2. Modifique el recurso para el territorio como se muestra a continuación:

   /iam/im/*new_alias*

   No elimine la parte /iam/im/ que precede al alias en el filtro de recursos.

3. Guarde los cambios.

Nota: En Modify CA Identity Manager Properties se proporcionan instrucciones sobre los cambios de alias en la Consola de gestión.

Modificación de un secreto compartido o una contraseña de SiteMinder

Cuando se instalan las extensiones de CA Identity Manager en el servidor de políticas, se debe proporcionar la contraseña de la cuenta de administrador de SiteMinder que utiliza CA Identity Manager para comunicarse con el servidor de políticas.

Se puede cambiar la contraseña, sin embargo, se deberá cifrar. Para cifrar una contraseña, se utiliza la herramienta de contraseñas que se proporciona con CA Identity Manager.

Nota: Es necesario asegurarse de que la variable JAVA_HOME se define para el entorno antes de cambiar la contraseña de SiteMinder.

Siga estos pasos:

1. Cifre la contraseña como se muestra a continuación:
   a. En la línea de comandos, navegue a *admin_tools*\PasswordTool, donde *admin_tools* es la ubicación de la instalación de las herramientas administrativas, como en los siguientes ejemplos:
      - **Windows:** C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool
      - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/PasswordTool
   b. Escriba el comando siguiente:

      pwdtools *new_password*

      En este comando, *new_password* es la contraseña que se debe cifrar.

      Nota: Para obtener información acerca de opciones de la utilidad pwdtools, introduzca el comando siguiente:

      pwdtools help
   c. Copie la contraseña cifrada.
2. Complete el paso pertinente como se indica a continuación:
   - Si CA Identity Manager se está ejecutando en un servidor de aplicaciones WebLogic, realice las tareas siguientes:
     a. En la consola de WebLogic, edite el adaptador de recurso de WebLogic en el descriptor de conector de policyserver_rar.
     b. Agregue la contraseña cifrada como el valor de la propiedad de la contraseña.

- Si CA Identity Manager se está ejecutando en un servidor de aplicaciones JBoss, realice las tareas siguientes:

  a. Abra ra.xml en *JBoss_home*\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.

  b. Agregue la contraseña cifrada como el valor de config-property de contraseña.

- Si CA Identity Manager se está ejecutando en un servidor de aplicaciones WebSphere, complete las tareas siguientes:

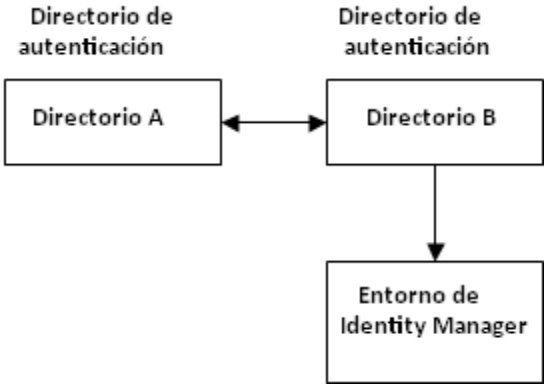
  a. En la consola de WebSphere, abra ra.xml.

  b. Agregue la contraseña cifrada como el valor de config-property de contraseña.

3. Reinicie el servidor de aplicaciones.

Configuración de un entorno de CA Identity Manager para usar directorios diferentes para su autenticación y autorización

Puede que un administrador deba gestionar usuarios cuyos perfiles existan en un almacén de usuarios diferente de aquél que se utiliza para autenticar al administrador. Dicho de otra manera, al iniciar sesión en el entorno de CA Identity Manager, el administrador se deberá autenticar mediante un directorio y se le deberá autorizar para gestionar usuarios en un segundo directorio, como se muestra en la ilustración siguiente:



Siga estos pasos:

1. Inicie sesión en una de las interfaces siguientes:
   - Para CA SiteMinder Web Access Manager r12 o posterior, inicie sesión en la interfaz de usuario administrativa.
   - Para CA eTrust SiteMinder 6.0 SP5, inicie sesión en la interfaz de usuario del servidor de políticas.

   Nota: Para obtener información sobre el uso de estas interfaces, consulte la documentación de la versión de SiteMinder que esté utilizando.
2. Cree dos directorios de usuarios.

   Un directorio hace referencia a los datos de autenticación (perfiles del administrador); el otro directorio hace referencia a los datos de autorización (perfiles de usuario).
3. En la Consola de gestión, cree un entorno de CA Identity Manager.

   Seleccione el directorio de autorizaciones como el directorio de CA Identity Manager.
4. En la interfaz de la versión de SiteMinder utilizada, se agrega el directorio de autenticación al dominio del entorno de CA Identity Manager creado en el paso anterior.

   El dominio y otros objetos necesarios para SiteMinder se crean automáticamente cuando se crea un entorno y SiteMinder se integra con CA Identity Manager.

   El dominio utiliza la convención de denominación siguiente:

   *Identity Manager-environment*Domain
5. Asegúrese de que este directorio aparece primero en la lista de directorios asociados con el dominio.
6. Busque *Identity Manager-environment*_ims_realm.
7. Asigne el directorio de autorización al directorio de autenticación en la sección Avanzada de la definición del territorio.
8. Busque la siguiente respuesta *Identity Manager-environment*response_ims.
9. Agregue los atributos de respuesta a las respuestas como se muestra a continuación:

Campo	Valor
Atributo	Web-Agent-HTTP-Header-Variable
Tipo de atributo	user attribute
Nombre de variable	sm_userdn

Campo	Valor
Nombre de atributo	SM_USERNAME

10. Guarde los cambios.

    CA Identity Manager ahora utiliza directorios diferentes para la autenticación y la autorización.

Cómo mejorar el rendimiento de operaciones de directorio LDAP

Las operaciones del directorio pueden necesitar más tiempo para procesarse porque todas las solicitudes de CA Identity Manager para el directorio de usuarios LDAP se enrutan mediante un conjunto fijo de conexiones.

Para aumentar el rendimiento de solicitudes de CA Identity Manager en el almacén de usuarios, se configura SiteMinder para abrir varias conexiones en el mismo directorio. Para llevar a cabo este procedimiento, se debe agregar el servidor LDAP varias veces en la conmutación por error del directorio LDAP y el cuadro de diálogo Configuración del equilibrio de carga en la interfaz de usuario del servidor de políticas.

El número de veces que se debe introducir el servidor LDAP (y el número de conexiones que se deben crear) depende de la carga de CA Identity Manager.

Apéndice A: Conformidad con FIPS 140-2

Esta sección contiene los siguientes temas:

Información general sobre FIPS

La publicación de los Estándares Federales de Procesamiento de la Información (FIPS) 140-2 es un estándar de seguridad para las bibliotecas criptográficas y los algoritmos que debería utilizar un producto para el cifrado. El cifrado FIPS 140-2 afecta la comunicación de todos los datos sensibles entre componentes de productos de CA, y entre productos de CA y productos de terceros. FIPS 140-2 especifica los requisitos para utilizar algoritmos criptográficos dentro de un sistema de seguridad que protege datos sensibles y sin clasificar.

CA Identity Manager utiliza un esquema de cifrado Estándar de cifrado avanzado (AES) que ha adaptado el gobierno de EE. UU. CA Identity Manager incorpora las bibliotecas criptográficas RSA Crypto-J v3.5 y Crypto-C ME v2.0, que se ha validado y cumple con los requisitos de seguridad para módulos criptográficos de FIPS 140-2.

Comunicaciones

El cifrado de FIPS cubre todas las comunicaciones de datos entre CA Identity Manager y los siguientes componentes:

- Servidor de CA Identity Manager
- Servidor de aprovisionamiento
- Gestor de aprovisionamiento y clientes
- Servidores de conectores de C++
- Puntos finales de servidor de conector de C++ (si admiten puntos finales)
- Servidores de conectores de CA IAM (Servicios de la nube de CA IAM)
- Puntos finales de Servicios de la nube de CA IAM (si admiten puntos finales)
- Connector Xpress (si admiten puntos finales)
- Agentes de sincronización de contraseñas de Windows
- Java Identity and Access Management (JIAM)

Instalación

El instalador de Identity Manager permite configurar CA Identity Manager para cumplir con FIPS 140-2.

Todos los componentes de un entorno de Identity Manager se deben activar para FIPS 140-2 con objeto de que Identity Manager sea compatible con FIPS 140-2. Se necesita una clave de cifrado FIPS para activar FIPS 140-2 durante la instalación. Se incluye una herramienta de contraseñas (pwdtools.bat/pwdtools.sh) para generar claves de FIPS en la siguiente ubicación:

```
C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity
Manager\PasswordTool\pwdtools.bat
```

Importante: Utilice la misma clave de cifrado FIPS 140-2 en todas las instalaciones. Además, asegúrese de guardar en una ubicación segura el archivo de clave que ha generado la herramienta de contraseñas.

Conexión a SiteMinder

Al conectar a CA SiteMinder durante la instalación de Identity Manager, sea consciente de que las configuraciones de la versión de producto y el modo FIPS solamente son compatibles de la manera que se muestra en la siguiente tabla:

Identity Manager r12	SiteMinder	SiteMinder Version
Modo FIPS-only	Modo FIPS-only	r12
Modo FIPS-only	Modo FIPS-compatible	r12
Modo Non-FIPS	Modo FIPS-compatible	r12
Modo Non-FIPS	Modo Non-FIPS	r6

Almacenamiento de archivos de clave

CA Identity Manager utiliza el sistema de archivos para el almacenamiento de claves de cifrado FIPS. El administrador de CA Identity Manager se encarga de proteger los archivos del acceso no autorizado estableciendo permisos de acceso al directorio para tipos de usuarios o grupos específicos, como el usuario que tiene autorización para ejecutar CA Identity Manager.

En la siguiente tabla se muestra la ubicación de los archivos de clave de FIPS para cada componente de CA Identity Manager.

Componente	Ubicación de instalación
Servidor de CA Identity Manager	*IdentityMinder.ear*\config\com\netegrity\config\keys\FIPSkey.dat *IdentityMinder.ear* es la ubicación en la que se instala CA Identity Manager en el servidor de aplicaciones.
Servidor de aprovisionamiento	*Instalación del servidor de aprovisionamiento*\data\tls\keymgmt\imps_datakey
Servidor de conector de C++	*Instalación del servidor de aprovisionamiento*\data\tls\keymgmt\imps_datakey

La herramienta de contraseña

La utilidad de herramienta de contraseña que cumple con los estándares de FIPS, pwdtools.bat (o pwdtools.sh), puede generar la clave de cifrado durante la instalación de CA Identity Manager, en la línea de comandos.

Se debe editar el archivo pwdtools.bat o pwdtools.sh antes de usar la herramienta de contraseña y establecer la variable JAVA_HOME como obligatoria.

Importante: CA Identity Manager no es compatible con la migración de datos ni el recifrado. Por lo tanto, es necesario asegurarse de que las claves de cifrado no se cambian después de la instalación.

Este comando presenta la siguiente sintaxis:

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <key file location>] [-f
<encrypting parameters file>]
```

JSAFE

Para cifrar un valor de texto no cifrado mediante el algoritmo PBE.

Ejemplo:

```
pwdtools -JSAFE –p mypassword
```

Nota: En las versiones anteriores, la contraseña para el administrador de arranque se almacena en texto no cifrado. Si se actualiza o migra a CA Identity Manager r12.6 SP1 o posteriores, será necesario cifrar manualmente la contraseña no cifrada. Garantice que la opción JSAFE esté especificada al utilizar la herramienta y siga estos pasos:

1. Después de actualizar o migrar a CA Identity Manager r12.6 SP1 y superiores, vaya a la base de datos de almacén de objetos de CA Identity Manager y busque la tabla siguiente:
   `IM_AUTH_USER`
2. Cifre la contraseña no cifrada mediante la herramienta de contraseña con JSAFE.
3. Reemplace el texto no cifrado por la contraseña cifrada de la tabla.

FIPSKEY

Para el instalador, se debe crear un archivo de claves de FIPS. La clave se genera antes de instalar CA Identity Manager.

Ejemplo:

```
pwdtools -FIPSKEY –k C:\keypath\FIPSkey.dat
```

Donde *keypath* es la ruta completa de la ubicación donde se desea almacenar la clave de FIPS.

La herramienta de contraseña crea la clave de FIPS en la ubicación especificada. Durante la instalación, se proporciona la ubicación del archivo de claves de FIPS al instalador.

Nota: Se debe asegurar la clave estableciendo los permisos de acceso al directorio para tipos concretos de grupos o usuario, como el usuario al que se autoriza a ejecutar CA Identity Manager.

FIPS

Para cifrar un valor de texto no cifrado mediante un archivo de claves de FIPS. FIPS utiliza el archivo de claves de FIPS existente.

Ejemplo:

```
pwdtools -FIPS –p firewall -k C:\keypath\FIPSkey.dat
```

Donde *keypath* es la ruta completa del directorio de claves de FIPS.

Nota: Se debe utilizar el mismo archivo de claves de FIPS especificado durante la instalación.

RC2

Para cifrar un valor de texto no cifrado mediante el algoritmo RC2.

Importante: CA Identity Manager utiliza el archivo de claves de FIPS para comprobar si la aplicación se iniciará en el modo FIPS o en el modo no FIPS. Por lo tanto, es necesario asegurarse de que el archivo de clave se llama FIPSKey.dat con la ruta de implementación del servidor de aplicaciones siguiente:

```
iam_im.ear\config\com\netegrity\config\keys\FIPSkey.dat
```

donde iam_im.ear está en el directorio de implementación del servidor de aplicaciones, por ejemplo:

```
jboss_home\server\default\deploy
```

Detección del modo FIPS

Para determinar si CA Identity Manager está operando en el modo FIPS o en el modo no FIPS, use la página de estado de entorno de CA Identity Manager.

Para ver la página de estado, introduzca la siguiente dirección URL en el explorador:

`http://server_name/idm/status.jsp`

server_name

Determina el nombre completo del dominio donde se ha instalado CA Identity Manager; por ejemplo, miservidor.miempresa.com. En este ejemplo, la dirección URL completa es la siguiente:

http://miservidor.miempresa.com/idm/status.jsp

El estado de FIPS se muestra en la parte inferior de la página.

Nota: Se puede comprobar también si CA Identity Manager está operando en el modo FIPS buscando el siguiente archivo de clave:

`/config/com/netegrity/config/keys/FIPSkey.dat`

Si este archivo existe, CA Identity Manager está operando en el modo FIPS.

La utilidad de herramienta de contraseñas, pwdtools.bat (o pwdtools.sh) crea el archivo de clave FIPSkey.dat. durante la instalación de <CA idmgr>.

Formatos de texto cifrado

El nombre del algoritmo se agrega al texto cifrado como prefijo e informa a CA Identity Manager sobre qué algoritmo se ha utilizado para el cifrado.

En el modo FIPS, el prefijo es {AES}. Por ejemplo, si se cifra el texto "password", el texto cifrado será similar al siguiente ejemplo:

{AES}:eolQCTq1CGPyg6qe++0asg==

En el modo no-FIPS (o modo de JSAFE), en función del algoritmo, el prefijo (etiqueta del algoritmo) es {PBES} o {RC2}. Por ejemplo, si se cifra el texto "password", el texto cifrado será similar al siguiente:

{PBES}:gSex2/BhDGzEKWvFmzca4w==

Se pueden crear claves dinámicas mediante la tarea Claves secretas en Sistema. Si se definen claves dinámicas, el ID de clave se inserta entre una etiqueta del algoritmo y delimitador de etiqueta (':'). La ausencia de un ID de clave en los datos cifrados indica que se utilizó una clave codificada para el cifrado. Esto se puede utilizar para la compatibilidad con versiones anteriores o si no se define ninguna clave dinámica para el algoritmo dado.

Información cifrada

La siguiente información de CA Identity Manager está cifrada:

- Contraseñas en la configuración de orígenes de datos para Jboss
- Información de la recuperación de contraseña olvidada
- Devolución de llamada secreta del servidor de aprovisionamiento
- Información de sesión de flujo de trabajo
- Información de conexión del servidor de políticas

Registro del modo FIPS

Los siguientes componentes de CA Identity Manager indican en los archivos de registro si se ha activado el modo FIPS:

- Servidor de Identity Manager
- Servidor de aprovisionamiento

- Servidor de conector de C++
- Servidor de conector de Java
- Gestor de aprovisionamiento
- Agente de sincronización de contraseñas

En todos los casos, la entrada de registro que indica que se ha activado el modo FIPS finaliza con la siguiente cadena:

FIPS 140-2 MODE: ON

Apéndice B: La sustitución de CA Identity Manager se certifica con certificados SSL firmados por SHA-2

El algoritmo de hash de certificado SSL de SHA-2 es un algoritmo criptográfico desarrollado por el Instituto nacional de normas y tecnología (NIST) y la Agencia de seguridad nacional (NSA). Los certificados de SHA-2 son más seguros que todos los algoritmos anteriores. En CA Identity Manager, se pueden configurar los certificados SSL firmados por SHA-2 en lugar de los certificados firmados con la función de hash SHA-1.

Nota: Para obtener más información sobre la configuración de certificados SSL, consulte la *Guía de instalación*.

En la tabla siguiente se muestra la ubicación de la ruta en el servidor de CA Identity Manager donde se pueden colocar los certificados firmados por SHA-2:

Certificados	Ubicación de instalación	Descripción
Certificado de servidor de aprovisionamiento	[Directorio de instalación del servidor de aprovisionamiento]/data/tls/server/eta2_servercert.pem [Directorio de instalación del servidor de aprovisionamiento]/data/tls/server/eta2_serverkey.pem *cs_install*/ccs/data/tls/server/eta2_servercert.pem *cs_install*/ccs/data/tls/server/eta2_serverkey.pem *cs_install*/jcs/conf/eta2_server.p12	Lo utiliza el servidor de aprovisionamiento en formato .pem y Servicios de la nube de CA IAM en formato .p12 (incluidos un certificado firmado, una clave privada y un certificado de CA raíz). **Nota**: Importe eta2_server.p12 en *cs_install*/jcs/conf/ssl.keystore con el alias eta2_server y eliminar la entrada existente. La contraseña de ssl.keystore es la contraseña del servidor de conectores que se proporciona durante la instalación.

Certificados	Ubicación de instalación	Descripción
Certificado de cliente de aprovisionamiento	[Directorio de instalación del servidor de aprovisionamiento]/data/tls/client/eta2_clientcert.pem [Directorio de instalación del servidor de aprovisionamiento]/data/tls/client/eta2_clientkey.pem [Directorio de instalación del gestor de aprovisionamiento]/data/tls/client/eta2_clientcert.pem [Directorio de instalación del gestor de aprovisionamiento]/data/tls/client/eta2_clientkey.pem *cs_install*/ccs/data/tls/client/eta2_clientcert.pem *cs_install*/ccs/data/tls/client/eta2_clientkey.pem *cs_install*/jcs/conf/eta2_client.p12	Lo utiliza el servidor de aprovisionamiento en formato .pem y Servicios de la nube de CA IAM en formato .p12 (incluidos un certificado firmado, una clave privada y un certificado de CA raíz).
Certificado de confianza del directorio de aprovisionamiento	*cadir_install*/config/ssld/impd_trusted.pem	Lo utiliza CA Directory en formato .pem. Debe incluir el contenido del certificado en la estructura siguiente: -----BEGIN CERTIFICATE----- Contenido del certificado -----END CERTIFICATE-----
Certificado de personalidad del directorio de aprovisionamiento	*cadir_install*/config/ssld/personalities/impd-co.pem *cadir_install*/config/ssld/personalities/impd-inc.pem *cadir_install*/config/ssld/personalities/impd-main.pem *cadir_install*/config/ssld/personalities/impd-notify.pem *cadir_install*/config/ssld/personalities/impd-router.pem	Lo utiliza CA Directory en formato .pem.

Certificados	Ubicación de instalación	Descripción
Certificado de CA raíz	[Directorio de instalación del servidor de aprovisionamiento]/data/tls/et2_cacert.pem [Directorio de instalación del gestor de aprovisionamiento]/data/tls/et2_cacert.pem *cs_install*/ccs/data/tls/ et2_cacert.pem *conxp_install*/lib/jiam.jar [Directorio de instalación del servidor de aplicaciones]/iam_im.ear/library/jiam.jar	Se importa el certificado en almacén de claves de Connector Xpress que se encuentra en [Directorio de instalación de Connector Xpress]/conf/ssl.keystore. El certificado también se deberá importar en el almacén de claves de jiam.jar. Para realizar la importación, se extrae el archivo .jar, se importa el certificado en admincacerts.jks y, a continuación, volver a empaquetar el contenido del .jar. La contraseña de almacén de claves de admincacerts.jks es "changeit". Verifique que todas las copias de jiam.jar se sustituyen.

Comandos útiles

El programa OpenSSL es una herramienta de línea de comandos para utilizar las diversas funciones de cifrado de la biblioteca OpenSSL. Esta herramienta se proporciona con IMPS que se encuentra en [Directorio de instalación del servidor de aprovisionamiento]/bin.

La tabla siguiente muestra algunos comandos útiles del programa OpenSSL para ejecutar diversos comandos relacionados con la gestión de certificados:

Comandos	Descripción
`openssl x509 –in cert.pem –text –noout`	Imprime el contenido de un certificado .pem.
`openssl.exe pkcs12 -in my.pkcs12 –info`	Imprime el contenido de un archivo .p12.
`openssl.exe pkcs12 -export -chain –inkey key.pem –in cert.pem -CAfile cacert.pem -out my.p12`	Convierte .pem cert/keypair en .p12.
`keytool –list –v -keystore my.keystore`	Imprime el contenido de un almacén de claves de java.
`keytool –list –v –alias myalias –keystore my.keystore`	Imprime el contenido de un alias específico de un almacén de claves de java.

Comandos		Descripción
	`keytool –delete –alias myalias –keystore my.keystore`	Suprime un alias de un almacén de claves de java.
	`keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias`	Importa un archivo .p12 en un almacén de claves de java.
	`keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore`	Importa un certificado de CA raíz .pem en un almacén de claves de java.