CA Identity Manager™

Guía de implementación

12.6.4

Referencias a productos de CA Technologies

En este documento se hace referencia a los siguientes productos de CA Technologies:

- Gestión de identidades de CA CloudMinder™
- CA Directory
- CA Identity Manager ™
- CA Identity Governance (anteriormente CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

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.

Contenido

Capítulo 1: Gestión de identidades y acceso

Esta sección contiene los siguientes temas:

Gestión de usuarios y acceso a la aplicación

Un departamento común de tecnologías de la información (TI) se enfrenta a una demanda constante de mantenimiento de las cuentas de usuario. Los administradores de TI deben abordar las necesidades urgentes de los usuarios, como restablecer contraseñas olvidadas, crear cuentas nuevas y proporcionar suministros y equipamiento para la oficina.

Al mismo tiempo, los administradores de TI deben proporcionar diversos niveles de acceso a aplicaciones a los usuarios. Por ejemplo, un gestor del departamento genera órdenes de compra y necesita una cuenta en una aplicación financiera.

Para abordar la creciente demanda de servicios de TI, CA Identity Manager proporciona un método integrado de gestión de usuarios y su acceso a aplicaciones, que incluye:

- Asignación de privilegios mediante roles. Descripción detallada:
  - Roles que permiten a los administradores crear y mantener cuentas de usuario.
  - Roles que aprovisionan cuentas adicionales a los usuarios existentes (requiere compatibilidad con aprovisionamiento).
- Delegación de la gestión de usuarios y acceso a la aplicación.
- Opciones de autoservicio para que los usuarios puedan gestionar sus propias cuentas.
- Integración de aplicaciones de negocio con CA Identity Manager.
- Opciones de personalizar y extender CA Identity Manager.

Autorizaciones basadas en roles

Se asignan privilegios a los usuarios asignando roles. Un *rol* contiene tareas que corresponden a funciones de la aplicación en CA Identity Manager, como por ejemplo la tarea Crear usuario, funciones en una aplicación, como por ejemplo la función Crear orden de compra o plantillas de cuenta que proporcionan las cuentas de usuario, como una cuenta de SAP. Cuando se asigna un rol a los usuarios, éstos reciben los privilegios correspondientes.

CA Identity Manager proporciona los tipos siguientes de roles:

- Roles de gestión de usuarios, que se llaman *roles de administrador*.

  Los roles de administrador pueden incluir también cualquier tarea que aparezca en la Consola de usuario.
- Roles de asignación de cuenta, que se llaman *roles de aprovisionamiento.*
- Roles de función de la aplicación, que se llaman *roles de acceso*.

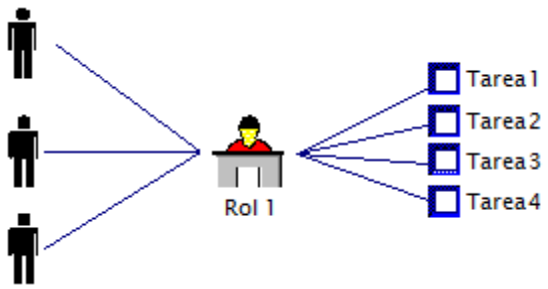
Si se elimina una tarea o plantilla de cuenta de un rol, el usuario no podrá realizar más esta tarea, utilizar una cuenta de punto final o utilizar una función de la aplicación.

Roles de administrador

Los roles de administrador controlan lo que puede hacer un usuario en CA Identity Manager. Un administrador del sistema asigna un rol a un usuario; ese rol define un conjunto de tareas que el usuario puede realizar. Los usuarios pueden realizar *tareas administrativas* en cuentas de usuario, como cambiar una contraseña o actualizar un cargo.

Los diversos usuarios tienen niveles distintos de acceso a estas tareas. Por ejemplo, un rol Empleado podría contener tareas que proporcionan a los usuarios la capacidad de modificar su nombre y dirección, mientras que el rol Gestor de recursos humanos contiene tareas para modificar el cargo y el salario del usuario.

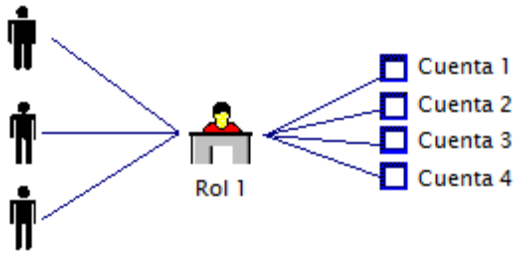
La ilustración siguiente muestra cuatro tareas que se combinan en un rol de administrador y se asignan a tres usuarios:



Roles de aprovisionamiento

Para conceder acceso a los usuarios a cuentas en aplicaciones adicionales, como por ejemplo un sistema de correo electrónico, se deben asignar roles de aprovisionamiento. Los roles de aprovisionamiento contienen plantillas de cuenta que definen los atributos que existen en un tipo de cuenta. Por ejemplo, una plantilla de cuenta para una cuenta de Exchange define atributos como el tamaño del buzón de correo. Las plantillas de cuenta también definen cómo los atributos de usuario de CA Identity Manager se asignan a las cuentas.

La ilustración siguiente muestra cuatro tareas que se combinan en un rol de aprovisionamiento y se asignan a tres usuarios: Cada usuario recibe cuatro cuentas cuando se asigna el rol de aprovisionamiento a ese usuario.



Roles de acceso

Los roles de acceso proporcionan una forma adicional de proporcionar autorizaciones en CA Identity Manager u otra aplicación. Por ejemplo, se pueden utilizar los roles de acceso para realizar las siguientes tareas:

- Proporcionar acceso indirecto a un atributo de usuario
- Crear expresiones complejas
- Establecer un atributo en un perfil de usuario, que otra aplicación utiliza para determinar las autorizaciones

Los roles de acceso son similares para identificar políticas de identidad ya que aplican un conjunto de cambios de negocio a un usuario o grupo de usuarios. Sin embargo, cuando se utiliza un rol de acceso para aplicar cambios de negocio, se puede consultar a qué usuarios se aplican los cambios visualizando los miembros del rol de acceso.

En la mayoría de los casos, los roles de acceso no están asociados a tareas.

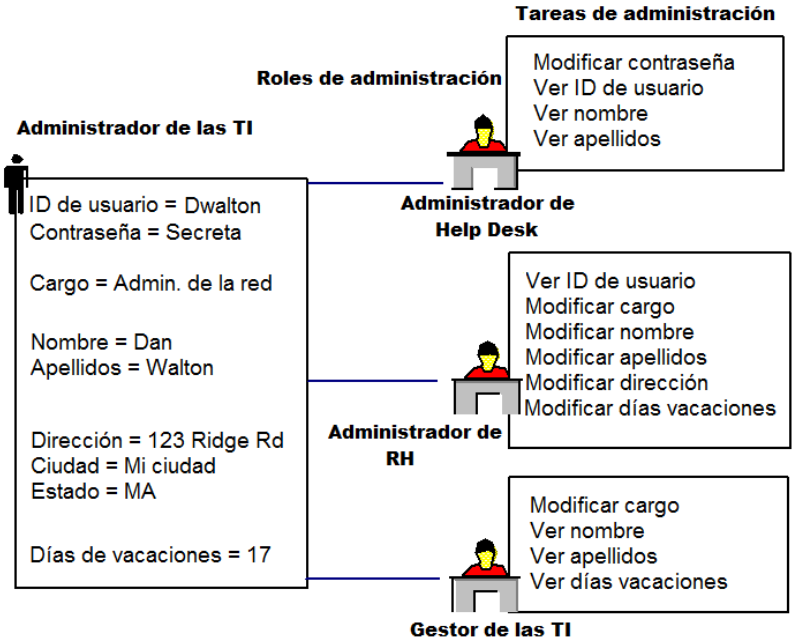
Nota: Cuando CA Identity Manager se integra con CA SiteMinder, los roles de acceso pueden proporcionar también acceso a aplicaciones que protege CA SiteMinder. En este caso, los roles de acceso incluyen tareas de acceso. Para obtener más información, consulte el capítulo sobre la integración de SiteMinder en la *Guía de configuración*.

Roles de administrador para la gestión de cuentas de usuario

En CA Identity Manager, los objetos de almacén de usuarios (usuarios, grupos y organizaciones) se gestionan mediante roles de administrador. También se utilizan roles de administrador para gestionar los roles y las tareas mediante los cuales se gestionan los objetos del almacén de usuarios. Por ejemplo, se utilizan roles de administrador para modificar atributos de perfil de usuarios, dar a los usuarios opciones para gestionar sus propias cuentas y aprobar tareas que utilicen flujo de trabajo.

Gestión de perfiles en el nivel del atributo

Se pueden crear roles de administrador para administradores diferentes que deban leer o escribir atributos de perfil diferentes. Por ejemplo, una compañía puede tener varios empleados que realizan operaciones en perfiles de usuario, cada uno mediante el acceso a atributos diferentes. La siguiente ilustración muestra tres roles y sus tareas asociadas. Cada rol tiene un acceso diferente a atributos de perfil.



En este ejemplo, tres roles pueden gestionar atributos diferentes para el mismo usuario, Dan Walton:

- Un administrador de Help Desk consulta nombres y direcciones de usuario y restablece contraseñas de usuario.
- Un administrador de recursos humanos modifica los ID de usuario, nombres de usuario, direcciones, títulos y número de días de vacaciones.
- Un gestor de TI modifica el título de usuarios y consulta su nombre y número de días de vacaciones.

Independientemente de los roles que se tengan al iniciar sesión en CA Identity Manager, aparecerán varias fichas, llamadas categorías, basadas en el rol de administrador asignado a la cuenta de CA Identity Manager. Para ver las tareas que se pueden realizar en una categoría, se hace clic en la ficha correspondiente como se muestra en la siguiente ilustración:

Los roles de administrador del usuario determinan las categorías y las tareas de esas categorías que ve un usuario.

Aprobación del flujo de trabajo de las tareas de administración

Para ayudar a automatizar los procesos de negocio, se puede diseñar una tarea de administración para generar un proceso de flujo de trabajo. Un *proceso de flujo de trabajo* automatiza un procedimiento bien definido que una compañía repite con frecuencia. CA Identity Manager incluye el motor del flujo de trabajo WorkPoint.

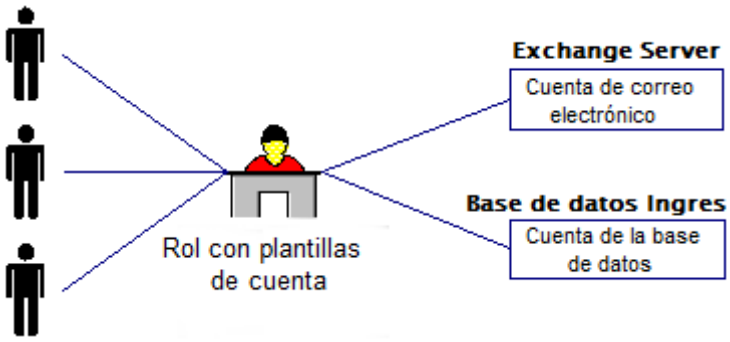
Los eventos de CA Identity Manager que forman parte de una tarea de administración activan procesos de flujo de trabajo. Por ejemplo, la tarea Crear usuario incluye los eventos llamados CreateUserEvent y AddToGroupEvent. Cuando se produce un evento, el motor del flujo de trabajo puede:

- Requerir aprobaciones: un aprobador debe aprobar un evento, como la modificación de un perfil de usuario, antes de que CA Identity Manager actualice un almacén de usuarios. Los aprobadores son administradores que tienen el rol de aprobador para una tarea determinada.
- Enviar notificaciones: el motor del flujo de trabajo puede notificar a los usuarios sobre el estado de un evento en etapas diferentes de un proceso, como el momento en que un usuario inicia un evento o en el que un evento se aprueba.
- Generar listas de trabajo: las listas de trabajo especifican las tareas que debe realizar un usuario concreto. El motor del flujo de trabajo actualiza las listas de trabajo de los administradores automáticamente.

Para eventos comunes, se pueden utilizar los procesos de flujo de trabajo que se facilitan con CA Identity Manager. De forma alternativa, se pueden crear procesos de flujo de trabajo personalizados.

Roles de aprovisionamiento para cuentas adicionales

En CA Identity Manager, se proporcionan cuentas adicionales a usuarios mediante roles de aprovisionamiento. Los roles de aprovisionamiento contienen plantillas de cuenta, que definen cuentas que existen en puntos finales gestionados, como un servidor de correo electrónico. Cuando se tienen usuarios en CA Identity Manager, se pueden asignar roles de aprovisionamiento a algunos de esos usuarios. El usuario recibe las cuentas definidas por las plantillas del rol.



Las plantillas de cuenta definen las características de la cuenta. Por ejemplo, una plantilla de cuenta para una cuenta de Exchange podría definir el tamaño del buzón de correo. Las plantillas de cuenta también definen cómo los atributos de usuario se asignan a las cuentas.

Para poder utilizar roles de aprovisionamiento, se debe instalar el servidor de aprovisionamiento con el servidor de Identity Manager. Después, se crean plantillas de cuenta en la Consola de usuario.

Gestión de contraseñas

Identity Manager incluye varias funciones para gestionar las contraseñas de los usuarios:

- Políticas de contraseñas: estas políticas gestionan las contraseñas de los usuarios mediante la aplicación de reglas y restricciones que controlan la caducidad, la composición y el uso de las contraseñas.

  Nota: Para políticas de contraseñas avanzadas, se debe configurar la integración con SiteMinder. Para obtener más información, consulte la *Guía de instalación*.

- Gestores de la contraseña: los administradores que tienen el rol Gestor de la contraseña pueden restablecer una contraseña cuando el usuario llama a Help Desk.

- Gestión de las contraseñas de autoservicio: Identity Manager incluye varias tareas de autoservicio que permiten a los usuarios gestionar sus propias contraseñas. Estas tareas incluyen:

  - Autorregistro: los usuarios especifican una contraseña cuando se registran en un sitio Web corporativo.
  - Cambiar Mi contraseña: los usuarios pueden modificar sus contraseñas sin ayuda del personal de TI o de Help Desk.
  - Contraseña olvidada: los usuarios pueden restablecer o recuperar una contraseña olvidada después de que Identity Manager verifique su identidad.
  - ID de usuario olvidado: los usuarios pueden recuperar un ID de usuario olvidado después de que Identity Manager verifique su identidad.

- Sincronización de contraseñas (solamente con aprovisionamiento): los cambios de las contraseñas se sincronizan en Identity Manager y en cuentas de sistemas de destino llamados puntos finales. Las nuevas contraseñas se verifican con respecto a las políticas de contraseñas de Identity Manager.

Opciones de autoservicio para usuarios

Para reducir más aún la carga de trabajo de TI, CA Identity Manager incluye funciones para registrar usuarios nuevos y proporcionar una contraseña olvidada. Estas funciones no requieren participación del administrador. El usuario obtiene acceso a CA Identity Manager mediante una *consola pública*, que no requiere ninguna cuenta de inicio de sesión. Mediante esta consola, un usuario se puede autorregistrar en un sitio o solicitar un recordatorio sobre una contraseña olvidada.

Para ahorrar tiempo a los administradores de TI, los usuarios de CA Identity Manager pueden gestionar sus propias cuentas. Dado que los usuarios tienen un rol de autogestión, pueden:

- Mantener información personal
- Cambiar su propia contraseña
- Unirse a grupos autosuscriptores

Personalización y extensibilidad de Identity Manager

Estas funciones de CA Identity Manager se pueden personalizar:

- El directorio de Identity Manager, que describe una estructura del almacén de usuarios a CA Identity Manager.
- El aspecto y funcionalidad de la interfaz de usuario.
- Las pantallas de entrada de usuario, que determinan los campos y el diseño de cada pantalla de tarea.
- La validación de la entrada de datos del usuario, mediante implementaciones de Java, JavaScript o expresiones regulares.
- El flujo de trabajo, que define los procesos de flujo de trabajo automatizados. Los procesos se crean o modifican vinculando aprobadores y acciones en el diseñador de procesos WorkPoint.
- Los mensajes de correo electrónico, que informan a los usuarios del estado de una tarea.
- El envío de la tarea, que puede enviar una aplicación de terceros al servicio Web de ejecución de tareas de Identity Manager (TEWS). TEWS procesa las solicitudes de tareas remotas. Las solicitudes de tareas remotas cumplen los estándares de WSDL.

Se puede extender la funcionalidad de CA Identity Manager mediante las siguientes API:

- API de atributos lógicos: permite mostrar un atributo de forma diferente que como se almacena físicamente en un directorio de usuarios.
- API del identificador de tareas lógicas del negocio: permite realizar la lógica empresarial personalizada durante operaciones de transformación o validación de datos.
- API de flujo de trabajo: proporciona información a un script personalizado en un proceso de flujo de trabajo. El script evalúa la información y determina la ruta del proceso de flujo de trabajo en consecuencia.
- API de resolvedor del participante: permite especificar la lista de participantes que están autorizados a aprobar una actividad de flujo de trabajo.
- API de escucha de eventos: permite crear una escucha de eventos personalizada que escuche un evento de Identity Manager específico o grupo de eventos. Cuando se produce el evento, la escucha de eventos puede realizar la lógica empresarial personalizada.
- API de reglas de notificaciones: permite determinar los usuarios que deberían recibir una notificación de correo electrónico.
- API de plantilla de correo electrónico: incluye información específica del evento en una notificación de correo electrónico.

Nota: Para obtener más información sobre las API de CA Identity Manager, consulte la *Guía de programación para Java*.

Cuando CA Identity Manager incluye aprovisionamiento, también se puede extender la funcionalidad de aprovisionamiento como se muestra a continuación:

- Conectores personalizados: permiten la comunicación entre un servidor de aprovisionamiento y un sistema de punto final. El código que forma un conector puede incluir un complemento de la interfaz gráfica de usuario, un complemento de servidor y un complemento de agente.

  Un conector dinámico se puede generar mediante Connector Xpress y un conector estático personalizado se puede desarrollar en Java o C++.
- Salidas de programa: permite hacer referencia al código personalizado del flujo de proceso del servidor de aprovisionamiento.

Nota: Para obtener más información sobre la extensión de la funcionalidad de aprovisionamiento, consulte la *Guía de programación para aprovisionamiento*.

Integración de CA Identity Governance

CA Identity Governance es un producto de gestión del ciclo de vida de las identidades que permite desarrollar, mantener y analizar modelos de roles de forma rápida y precisa. También ofrece un control centralizado de la política de cumplimiento de identidad y automatiza los procesos asociados a la conformidad con las necesidades de cumplimiento y seguridad. CA Identity Governance le permite hacer lo siguiente:

- Validar que los privilegios de usuario de CA Identity Manager se conceden de acuerdo con las políticas de cumplimiento del negocio
- Obtener roles sugeridos y comprobación del cumplimiento al crear o modificar cuentas, roles y usuarios de CA Identity Manager
- Entender qué roles existen en su organización, establecer un modelo de roles que se ajuste a su organización y volver a crear el modelo de roles deseado dentro de CA Identity Manager
- Analizar y mantener el modelo de roles a medida que evolucione el negocio

CA Identity Manager se integra con CA Identity Governance de dos maneras diferentes:

- Conector de CA Identity Governance para CA Identity Manager

  Un tipo especial de conector que sincroniza automáticamente los datos de privilegios entre CA Identity Manager y CA Identity Governance. Mediante este conector, se pueden importar datos de CA Identity Manager a CA Identity Governance o exportar datos de CA Identity Governance a CA Identity Manager.

- Aprovisionamiento inteligente

  Cuando CA Identity Manager se integra con CA Identity Governance, se pueden configurar más funciones que permiten utilizar la información de roles y cumplimiento disponible en un modelo de roles, a fin de realizar las operaciones cotidianas de gestión de identidades. Los cambios realizados en CA Identity Manager actualizan de forma dinámica el modelo de roles de CA Identity Governance.

Nota: Para obtener más información sobre integración de CA Identity Governance con CA Identity Manager, consulte la *Guía de integración de CA Identity Manager* que se encuentra en la biblioteca de CA Identity Governance.

Integración de CA User Activity Reporting

Al empezar en CA Identity Manager r12.6, CA Enterprise Log Manager se llama CA User Activity Reporting (CA UAR).

CA UAR utiliza la Gramática de eventos comunes (CEG) para asignar los eventos que se producen en varios sistemas en un formato estándar y almacena todos los eventos (incluso los que no se han asignado aún) de modo que sea posible revisarlos y analizarlos. Además, CA UAR ofrece a los usuarios una solución de grandes volúmenes para gestionar y generar informes con los datos recopilados, a través de consultas a bases de datos configurables e informes en los que se pueden buscar distintos tipos de informaciones y eventos.

CA UAR ofrece una perspectiva mejor, más amplia y más profunda sobre los sistemas no gestionados y los sistemas ajenos al ámbito y el control de CA Identity Manager, además de permitir investigar en profundidad las identidades.

La integración con CA Identity Manager permite la visualización de informes centrados en la identidad de CA UAR y/o consultas dinámicas en la Consola de usuario de CA UAR mediante la Consola de usuario de CA Identity Manager. En la Consola de usuario se puede configurar cómo se deben visualizar y modificar los informes o consultas existentes de CA Identity Manager/CA UAR mientras investiga en profundidad una identidad específica.

Informes de CA UAR

Los siguientes informes de CA UAR se proporcionan con las definiciones de roles de CA UAR de forma predeterminada:

Tarea	Invoca el informe
Todos los eventos del sistema por usuario	CA Identity Manager: Todos los eventos del sistema filtrados por ID de usuario
Gestión de cuentas por host	Gestión de cuentas por host
Creaciones de cuentas por cuenta	Creaciones de cuentas por cuenta
Supresiones de cuentas por cuenta	Supresiones de cuentas por cuenta
Bloqueos de cuenta por cuenta	Bloqueos de cuenta por cuenta
Actividad de proceso de certificación por host	CA Identity Manager: Actividad de proceso por host
Actividad de modificación de política de contraseñas	CA Identity Manager: Actividad de modificación de política

Capítulo 2: Respuesta a las necesidades empresariales

Esta sección contiene los siguientes temas:

Procesamiento de los cambios del negocio

Se puede automatizar el procesamiento de ciertas tareas de gestión de identidades mediante políticas de identidad. Una política de identidad es un conjunto cambios empresariales que se producen cuando un usuario cumple una cierta condición o regla. Puede utilizar los conjuntos de políticas de identidad para:

- 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 (en la página 26). Por ejemplo, puede crear un conjunto de políticas de identidad que prohíba a los miembros del rol Comprobar firmante que tengan el rol Comprobar aprobador y que impida a cualquier persona de la empresa extender un cheque superior a 10.000 $.
- Imponer el cumplimiento. Por ejemplo, puede auditar a los usuarios que tengan un título determinado y ganen más de 100.000 $.

  Las políticas de identidad que imponen el cumplimiento se denominan *políticas de cumplimiento*.

Los cambios del negocio asociados con una política de identidad incluyen:

- La asignación o revocación de roles, incluidos los roles de aprovisionamiento (cuando CA Identity Manager incluye aprovisionamiento).
- La asignación o la revocación de una pertenencia a grupo
- La actualización de atributos en un perfil de usuario

Por ejemplo, una empresa puede crear una política de identidad que establezca que todos los vicepresidentes pertenezcan al grupo Miembro del club de campo y tengan el rol Aprobador de salario. Si el cargo de un usuario cambia a vicepresidente y dicho usuario está sincronizado con la política de identidad, CA Identity Manager agregará el usuario al rol y al grupo apropiados. Cuando un vicepresidente es ascendido a Jefe ejecutivo, ya no cumple la condición de la política de identidad de vicepresidente, de modo que los cambios aplicados por dicha política serán revocados y se pasarán a aplicar nuevos cambios basados en la política de Jefe ejecutivo.

Las acciones de cambio que se producen en función de una política de identidad contienen eventos que se pueden colocar bajo el control de flujo de trabajo y auditar. En el ejemplo anterior, el rol Aprobador de salario concede privilegios significativos a sus miembros. Para protegerlo, la empresa puede crear un proceso de flujo de trabajo que necesite un conjunto de aprobaciones antes de asignar el rol. Además, se puede configurar CA Identity Manager para que audite la asignación del rol.

Para simplificar la gestión de políticas de identidad, éstas se agrupan en un conjunto de políticas de identidad. Por ejemplo, las políticas de vicepresidente y jefe ejecutivo pueden formar parte del conjunto de políticas de identidad Privilegios ejecutivos.

Cumplimiento con las políticas del negocio

La conformidad es el gobierno corporativo que incluye una amplia variedad de procedimientos que garantizan que una compañía y sus empleados cumplan con las políticas del negocio. Esos procedimientos de conformidad suelen implicar la documentación, automatización y auditoría de la asignación de derechos a aplicaciones y sistemas.

CA Identity Manager incluye las siguientes características, que admiten la gestión del cumplimiento:

- **Aprovisionamiento inteligente**

  El aprovisionamiento inteligente es un conjunto de funciones que simplifica la asignación de roles de aprovisionamiento cuando CA Identity Manager se integra en CA Identity Governance. Entre estas funciones se incluyen las siguientes:

  - Roles de aprovisionamiento sugeridos

    CA Identity Manager puede proporcionar a los administradores una lista de roles de aprovisionamiento que puede ser conveniente asignar a un usuario. La lista de roles de aprovisionamiento se determina mediante CA Identity Governance, en función de los criterios especificados por el administrador.

    Los roles de aprovisionamiento sugeridos garantizan que los usuarios tengan los privilegios correctos, manteniendo al mismo tiempo el modelo de roles de la empresa.

- Mensajes de cumplimiento y modelo

  Los administradores de CA Identity Manager pueden validar cambios propuestos con un modelo de rol en CA Identity Governance antes de confirmar los cambios. La validación de los cambios antes de que confirmen ayuda a las empresas a mantener el modelo de rol que han definido para sus operaciones.

  Los usuarios pueden validar los cambios propuestos en los roles de aprovisionamiento (asignándolos o eliminándolos), así como en los atributos de usuario.

  CA Identity Manager lleva a cabo dos tipos de validaciones de políticas:

  - Conformidad

    Los cambios propuestos se validan con el modelo de rol de CA Identity Governance para ver si infringen las reglas de política de negocio explícitas predefinidas de CA Identity Governance.

  - Patrón

    Los cambios propuestos se comparan con el modelo de rol de CA Identity Governance para ver si transforman el asunto del cambio en "sin patrón". CA Identity Manager también comprueba que los cambios no alteren de forma significativa un patrón establecido del modelo de rol.

    Puede configurar CA Identity Manager para que lleve a cabo estas validaciones de forma automática cuando los usuarios realicen determinadas tareas, o permitir a los usuarios que inicien la validación de forma manual.

Puede implementar el aprovisionamiento inteligente en un entorno de CA Identity Manager, una vez se haya establecido un modelo de rol basado en datos de CA Identity Manager en CA Identity Governance.

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

- **Políticas de identidad**

  Se puede crear una política de conformidad (un tipo de política de identidad (en la página 21)), que prohíba a los usuarios tener determinados privilegios si ya tienen otros. Por ejemplo, puede prohibir la facultad de emitir cheques a los usuarios con capacidad para aprobarlos.

  Las políticas de conformidad imponen la segregación de funciones en el entorno.

- **Informes de cumplimiento**

  CA Identity Manager incluye informes de ejemplo que muestran el estado de cumplimiento de los usuarios del entorno. Mediante estos informes, se puede ver qué usuarios no cumplen las políticas empresariales.

Informes de cumplimiento

CA Identity Manager incluye los informes de ejemplo en la tabla siguiente que se puede utilizar para controlar el cumplimiento de las políticas de empresa corporativas.

Informe	Descripción
Miembros de roles	Muestra los roles en la base de datos de informe y enumera los miembros de esos roles.
Roles	Se muestra siguiente información de cada rol en la base de datos de informes: ■ Tareas asociadas con el rol ■ Políticas de miembros y miembros de rol ■ Políticas de administrador y administradores de roles ■ Políticas de propietario y propietarios de rol
Roles de tareas	Muestra las tareas de la base de datos de informes y los roles con los que están asociados.
Funciones de usuario	Muestra los usuarios de la base de datos de informes y enumera los roles de cada usuario.
Tendencia de las cuentas no estándar	Muestra las tendencias de las cuentas no estándar para cuentas huérfanas, del sistema y de excepción.
Cuentas no estándar	Muestra todas las cuentas huérfanas, del sistema y de excepción.
Cuentas huérfanas	Muestra todas las cuentas de puntos finales sin usuarios globales en el servidor de aprovisionamiento.
Políticas	Muestran todas las políticas de identidad.

Informe	Descripción
Perfil de usuario	Se muestra la siguiente información de usuarios: ■ Nombre ■ ID de usuario ■ Grupos de los que el usuario sea miembro o administrador ■ Roles de los que el usuario sea miembro, administrador o propietario
Cuentas de puntos finales	Muestra las cuentas por punto final (se puede elegir qué punto final ver).
Administradores del rol	Muestra los roles y sus administradores.
Propietarios de roles	Muestra los roles y sus propietarios.
Instantáneas	Muestra todas las instantáneas exportadas.
Cuenta de usuario	Muestra una lista de usuarios y sus cuentas.
Autorizaciones de usuario	Muestra roles de usuario, grupos y cuentas.
Estado de la sincronización de las políticas de usuario	Muestra el estado de usuario por política (qué políticas se deben adjudicar, desadjudicar o readjudicar).

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

Imposición de la segregación de requisitos de funciones

Los requisitos de la segregación de funciones (SOD) evitan que los usuarios reciban privilegios que puedan dar lugar a un conflicto de intereses o fraude. CA Identity Manager proporciona la siguiente funcionalidad para ser compatible con SOD:

- **Políticas de identidad preventivas**

  Estas políticas, que se ejecutan antes de que se envíe una tarea, permiten que un administrador compruebe si hay infracciones de política antes de asignar privilegios o cambiar atributos de perfil. Si las hubiera, el administrador podría borrar la infracción antes de enviar la tarea.

  Por ejemplo, una compañía puede crear una política de identidad preventiva que prohíba a los usuarios que posean el rol Gestor de usuarios tener el rol Aprobador de usuarios. Si un administrador usa la tarea Modificar usuario para darle al Gestor de usuarios el rol Aprobador de usuarios, CA Identity Manager muestra un mensaje sobre la infracción. El administrador puede cambiar las asignaciones de rol para borrar la infracción antes de enviar la tarea.

- **Validación de la política mediante el aprovisionamiento inteligente**

  Los administradores de CA Identity Manager pueden validar los cambios propuestos en los roles de aprovisionamiento y los atributos de usuario con respecto a las reglas de la política del negocio (BPR) en CA Identity Governance antes de realizar los cambios. Las BPR representan diversas restricciones sobre los privilegios. Por ejemplo, una BPR puede impedir que los usuarios que tengan el rol de departamento de compras, que permite a los miembros pedir material a los subcontratistas, tengan también el rol de pago a subcontratista. Un gestor del sistema, gestor del negocio, auditor o ingeniero de roles crea las BPR en CA Identity Governance.

  Nota: Para obtener más información acerca de las BPR, consulte *CA Identity Governance Sage DNA User Guide*.

Nota: Para obtener más información sobre las políticas de identidad preventivas y el aprovisionamiento inteligente, consulte la *Guía de administración* de *CA Identity Manager*.

Transformación de los datos del almacén de usuarios

En algunos casos, se puede desear que CA Identity Manager transforme los datos antes almacenarlos en el almacén de usuarios. Por ejemplo, se puede desear almacenar la información en un formato diferente del que se introduce o que los cambios se apliquen cuando ciertos tipos de información estén presentes.

CA Identity Manager incluye las siguientes funciones para transformar datos:

- Políticas de identidad
- Identificadores de atributos lógicos

Nota: También se pueden utilizar políticas de identidad e identificadores de atributos lógicos para implementar la lógica del negocio personalizada.

Identificadores de atributos lógicos

Los identificadores de atributos lógicos son código de Java personalizado que transforman los valores de atributos de usuarios utilizados en las pantallas de tarea de CA Identity Manager. Al usar identificadores de atributos lógicos, se puede controlar cómo se muestra un atributo físico en una pantalla de tarea. También se pueden utilizar identificadores de atributos lógicos para transformar un valor de visualización en la pantalla de tarea, como el coste, en uno o varios atributos físicos, como el precio por unidad y cantidad, que se almacenan en el almacén de usuarios.

Nota: Para obtener más información sobre los identificadores de atributos lógicos, consulte la *Guía de programación para Java*.

Aplicación de la lógica empresarial personalizada

Se puede personalizar CA Identity Manager para implementar la lógica empresarial que requiere una compañía. CA Identity Manager incluye las siguientes opciones para implementar la lógica empresarial personalizada:

- Políticas de identidad: se pueden utilizar políticas de identidad para definir un conjunto de cambios de negocio que se producen cuando un usuario cumple una cierta condición o regla. Por ejemplo, las políticas de identidad pueden automatizar ciertas tareas de gestión de identidades, como la asignación de roles o la imposición de reglas de negocio, como evitar que los usuarios firmen y aprueben cheques superiores a 20000 $.

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

- Identificadores de atributos lógicos: se pueden asociar estos identificadores con pantallas de tarea de CA Identity Manager para controlar la visualización y la modificación de los valores de atributos.

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

- Identificadores de tareas lógicas del negocio: permiten realizar la lógica empresarial personalizada, como se muestra a continuación, durante las operaciones de validación de datos para una tarea de CA Identity Manager:

  - Imposición de reglas de negocio personalizadas (por ejemplo, un administrador no puede gestionar más de cinco grupos).
  - Validación de campos de pantalla de tarea específicos del cliente (por ejemplo, el valor de un campo de ID de empleado debe existir en la base de datos principal de recursos humanos).

  Los identificadores de tareas lógicas del negocio se pueden implementar en Java o JavaScript.

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

- Flujo de trabajo: permite crear definiciones del proceso personalizadas, que se asocian a un evento de CA Identity Manager.

Nota: Antes de decidir si implementar la lógica empresarial en un identificador de tareas lógicas del negocio o un proceso de flujo de trabajo, consulte las siguientes secciones:

- Consideraciones de los identificadores de tareas lógicas del negocio (en la página 29)
- Consideraciones del proceso de flujo de trabajo (en la página 29)

Consideraciones de los identificadores de tareas lógicas del negocio

Los identificadores de tareas lógicas del negocio realizan la validación de la lógica del negocio durante la fase de procesamiento sincrónica de la tarea, que tiene lugar antes de la generación del evento. Esto permite:

- Realizar la validación en el nivel de tareas Por ejemplo, se pueden agregar o eliminar miembros de un grupo en función de la ubicación de su oficina, que se especifica en la pantalla de perfil de usuario.
- Evitar que una tarea se envíe si se produce un error con la validación.
- Transformar automáticamente toda la información en una pantalla de tarea para que se encuentre conforme a las políticas de la empresa antes del envío de la tarea.

Nota: No se deben implementar actividades que tardan mucho tiempo completarse en un identificador de tareas lógicas del negocio. Las actividades que utilizan mucho tiempo de ejecución retrasan el envío de la tarea y no son adecuadas para la fase sincrónica en la que tiene lugar la interacción del usuario. En su lugar, se debe utilizar un proceso de flujo de trabajo, que se ejecuta durante la fase asincrónica de la tarea.

Consideraciones del proceso de flujo de trabajo

Los procesos de flujo de trabajo se convocan durante la fase asincrónica de la tarea y se asocian con la ejecución de pruebas individuales. Esto permite:

- Ejecutar actividades de aprobación según los datos del evento individual
- Ejecutar actividades de lógica del negocio personalizadas con un tiempo de ejecución largo

Aunque la API de flujo de trabajo permite obtener datos de nivel de tarea de una actividad de flujo de trabajo, normalmente se trabaja en el contexto de ese evento específico del flujo de trabajo.

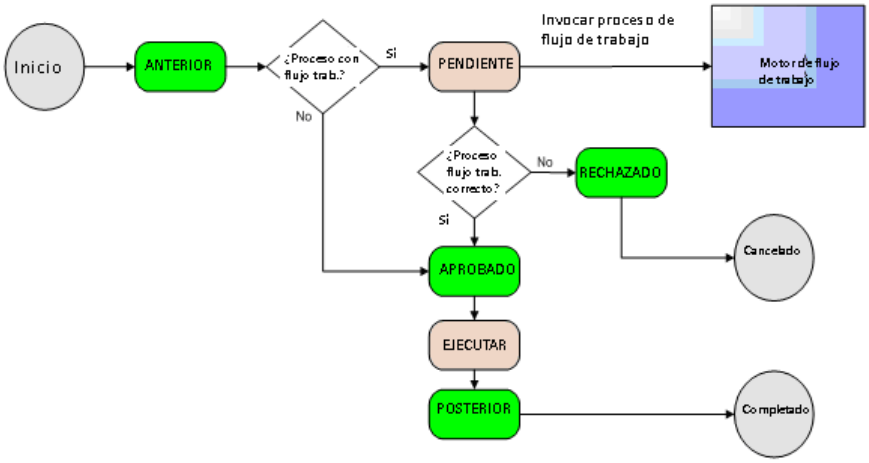
Aprobación de cambios de negocio

El flujo de trabajo describe un proceso formado por uno o varios pasos que se deberán realizar para lograr algún objetivo de negocio, como la ejecución de un proceso de contratación o la obtención del resultado del crédito de un usuario de un sistema externo. Normalmente, uno de los pasos de un proceso de flujo de trabajo implica la aprobación o el rechazo del cambio empresarial.

En CA Identity Manager, un proceso de flujo de trabajo está asociado con un evento, una acción que tiene lugar durante el procesamiento de la tarea. Cuando un evento introduce el estado Pendiente en su ciclo de vida, CA Identity Manager invoca todos los procesos de flujo de trabajo asociados y detiene la ejecución del evento hasta que el proceso se complete. CA Identity Manager a continuación realiza o rechaza el evento en función de los resultados del proceso de flujo de trabajo.

Esta secuencia se muestra en el siguiente diagrama:

Ciclo de vida del evento y procesamiento del flujo de trabajo



CA Identity Manager incluye el motor del flujo de trabajo WorkPoint de InSession para crear y gestionar procesos de flujo de trabajo.

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

Capítulo 3: Arquitectura de CA Identity Manager

Esta sección contiene los siguientes temas:

Componentes de CA Identity Manager

Una implementación de CA Identity Manager puede incluir algunos o todos los componentes siguientes:

- Servidores
- Almacenes de usuarios
- Bases de datos
- Conectores

Servidores

Una implementación de CA Identity Manager incluye uno o varios tipos de servidores, según la funcionalidad que se necesite.

Servidor de CA Identity Manager (obligatorio)

Ejecuta tareas en CA Identity Manager. La aplicación de J2EE de CA Identity Manager incluye la Consola de gestión y la Consola de usuario.

Servidor de aprovisionamiento de CA Identity Manager

Gestiona las cuentas de sistemas de puntos finales.

Este servidor es obligatorio si la instalación de CA Identity Manager será compatible con el aprovisionamiento de cuentas.

Nota: El directorio de aprovisionamiento se debe instalar de forma remota (o de forma local para entornos de demostración solamente) en un servidor de CA Directory antes de instalar el servidor de aprovisionamiento.

Servidor de políticas de SiteMinder

Proporciona autenticación avanzada para CA Identity Manager y acceso a funciones de SiteMinder, como Password Services y Single Sign-On.

Este servidor es opcional.

Directorio de aprovisionamiento y almacén de usuarios

CA Identity Manager coordina dos almacenes de usuarios:

- El *almacén de usuarios de CA Identity Manager*, el almacén de usuarios que mantiene CA Identity Manager. Normalmente, se trata de un almacén existente que contiene las identidades del usuario que debe gestionar una compañía.

  El almacén de usuarios puede ser un directorio LDAP o una base de datos relacional.

  En la Consola de gestión, se crea un objeto de directorio de CA Identity Manager para conectarse al almacén de usuarios y describir los objetos del almacén de usuarios que CA Identity Manager mantendrá.

- El *directorio de aprovisionamiento*, el almacén de usuarios que mantiene el servidor de aprovisionamiento.

  Es una instancia de CA Directory e incluye usuarios globales, que asocian usuarios del directorio de aprovisionamiento con cuentas de puntos finales como Microsoft Exchange, Active Directory y SAP.

  Solamente algunos usuarios de CA Identity Manager tienen un usuario global correspondiente. Cuando un usuario de CA Identity Manager recibe un rol de aprovisionamiento, el servidor de aprovisionamiento crea un usuario global.

Almacén de usuarios y directorio de aprovisionamiento independientes

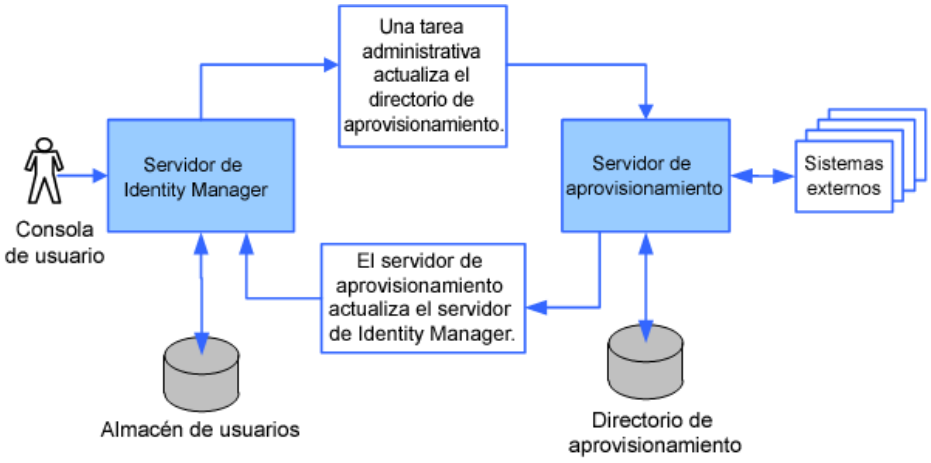
En la imagen siguiente se muestra un almacén de usuarios y un directorio de aprovisionamiento independientes, es decir, el escenario compatible para una instalación nueva de CA Identity Manager. En esta ilustración:

- Un administrador de CA Identity Manager utiliza una tarea de administración que edita un usuario en el almacén de usuarios, lo que afecta al directorio de aprovisionamiento.

  Este cambio también puede actualizar un punto final (como un servidor de correo electrónico) que tenga un conector al servidor de aprovisionamiento.

  Un cambio realizado en el servidor de aprovisionamiento (o un punto final con un conector en el servidor de aprovisionamiento) actualiza el directorio de aprovisionamiento y el almacén de usuarios de CA Identity Manager.

Por ejemplo, un punto final, como una aplicación de recursos humanos, podría actualizar las direcciones de correo electrónico de los usuarios.



Bases de datos

CA Identity Manager utiliza orígenes de datos para conectarse a bases de datos que almacenan la información necesaria para admitir la funcionalidad de CA Identity Manager. Estas bases de datos pueden residir en una instancia física única de una base de datos o en instancias separadas.

Base de datos de objetos (obligatoria)

Contiene información de la configuración de CA Identity Manager.

Base de datos de persistencia de la tarea (obligatoria)

Mantiene información acerca de las actividades de CA Identity Manager y sus eventos asociados gradualmente. Esto permite al sistema realizar un seguimiento con precisión de las actividades de CA Identity Manager, aunque se reinicie el servidor de CA Identity Manager.

Base de datos de archivado (obligatoria)

Datos de archivado de la base de datos de persistencia de la tarea.

Base de datos de flujo de trabajo

Almacena las definiciones del flujo de trabajo, trabajos, scripts y otros datos que necesita el motor del flujo de trabajo.

Base de datos de auditoría

Proporciona un registro del historial de las operaciones que se producen en un entorno de CA Identity Manager.

Nota: Se puede configurar la cantidad y el tipo de información que CA Identity Manager almacena en la base de datos de auditoría. Para obtener más información, consulte la *Guía de configuración*.

Base de datos de informes

Almacena los datos de la instantánea, que reflejan el estado actual de los objetos de CA Identity Manager en el momento en que se hace la instantánea. Se pueden generar informes de esta información para ver la relación entre objetos, como usuarios y roles.

Cuando se utiliza el instalador, CA Identity Manager configura una conexión a una base de datos única, la base de datos de CA Identity Manager, que contiene las tablas para cada tipo de base de datos.

Nota: Se puede crear un almacén de datos para persistencia de la tarea, flujo de trabajo, auditoría o generación de informes en una base de datos independiente y configurar CA Identity Manager para que se conecte a ella. Para obtener más información, consulte la *Guía de instalación*.

Componentes del conector

Un conector es la interfaz de software para un punto final. El servidor de aprovisionamiento utiliza el conector para comunicarse con el punto final. Traduce las acciones del servidor de aprovisionamiento a cambios en el punto final, como “Crear una cuenta de correo electrónico nueva en un punto final de Microsoft Exchange”.

Algunos ejemplos de puntos finales son estaciones de trabajo de UNIX, PC de Windows o una aplicación como Microsoft Exchange (para el correo electrónico).

Servidores de conectores

Un servidor de conectores es un componente del servidor de aprovisionamiento que gestiona conectores. Se puede instalar en el sistema del servidor de aprovisionamiento o en un sistema remoto.

Un servidor de conectores funciona con varios puntos finales. Por ejemplo, si se dispone de muchos puntos finales de estaciones de trabajo de UNIX, se podría tener un servidor de conectores que manejase todos los conectores que gestionen cuentas de UNIX. Otro servidor de conectores podría manejar todos los conectores que solicitasen cuentas de Windows.

El servidor de conectores distribuido funciona con varios servidores de conectores. Proporciona equilibrio de carga cuando un servidor de conectores está ocupado y disponibilidad alta cuando un servidor de conectores está inactivo.

Existen dos tipos de servidores de conectores:

- El servidor de conectores de CA IAM (Servicios de la nube de CA IAM) gestiona conectores escritos en Java.
- El servidor de conectores de C++ (CCS) gestiona conectores escritos en C++.

Servidor de conector de C++

El *servidor de conectores de C++* es un servidor de conectores que gestiona conectores de C++. Se puede instalar en el servidor de aprovisionamiento o en un sistema remoto. El servidor de conectores de C++ proporciona un marco de la aplicación orientado al objeto que simplifica el desarrollo de conectores, que son los responsables de la comunicación entre el servidor de conectores de C++ y el punto final.

Servicios de la nube de CA IAM

Servicios de la nube de CA IAM es un componente del servidor que maneja el hospedaje y la gestión de conectores de Java, así como el enrutamiento a éstos. Servicios de la nube de CA IAM proporciona una alternativa de Java al servidor de conectores de C++. Su arquitectura y funcionalidad son similares a las del servidor de conectores de C++, excepto en que tiene una API de Java en lugar de una API de C++, lo que permite implementar los conectores en Java. Además, Servicios de la nube de CA IAM se controla mediante datos más que mediante código, lo cual permite que el contenedor (o Servicios de la nube de CA IAM) aborde una mayor funcionalidad, en lugar de los propios conectores.

El servidor de aprovisionamiento maneja el aprovisionamiento de usuarios y delega a los conectores (mediante el servidor de conectores de C++ o Servicios de la nube de CA IAM) la gestión de cuentas de puntos finales, y se agrupa.

Conectores y agentes

Los conectores de CA Identity Manager se ejecutan como parte de la arquitectura de servidor de aprovisionamiento más amplia y se comunican con los sistemas gestionados en su entorno. Un conector sirve de puerta de enlace a un tecnología de sistema de tipo de punto final nativa. Por ejemplo, se pueden gestionar equipos que ejecutan servicios de Active Directory (ADS) solamente si el conector de servicios de Active Directory está instalado en un servidor de conectores con el cual se puede comunicar el servidor de aprovisionamiento. Los conectores gestionan los objetos que residen en los sistemas. Los objetos gestionados incluyen cuentas, grupos y, opcionalmente, objetos específicos de tipo de punto final.

Los conectores se instalan en el servidor de conectores y algunos componentes se instalan en el servidor de aprovisionamiento (por ejemplo, un complemento de servidor) o gestor de aprovisionamiento (complementos de interfaz de usuario).

Algunos conectores requieren un agente en los sistemas que gestionan para completar el ciclo de comunicación, en cuyo caso, se pueden instalar mediante el instalador de aprovisionamiento. Los agentes se pueden dividir en las categorías siguientes:

Agentes remotos

Instalados en los sistemas de puntos finales gestionados

Agentes de entorno

Instalados en sistemas como CA ACF2, CA Top Secret y RACF

Determinados componentes funcionan con UNIX y Windows, incluidas las siguientes opciones basadas en el servidor de conectores de C++:

- UNIX (ETC, NIS)
- Access Control (ACC)

  Nota: El conector de ACC de UNIX puede gestionar solamente puntos finales de ACC de UNIX. El conector de ACC de Windows se requiere para gestionar los puntos finales de ACC de Windows pero también puede gestionar puntos finales de ACC de UNIX.
- CA-ACF2
- RACF
- CA Top Secret

Se puede acceder a los demás conectores basados en el servidor de conectores de C++ desde el servidor de aprovisionamiento de Solaris basándose en el marco del servidor de conector (CSF). El CSF permite a un servidor de aprovisionamiento en Solaris comunicarse con conectores que se ejecutan en Windows.

Nota: El CSF se deberá ejecutar en Windows para usar estos conectores.

Connector Xpress

Connector Xpress es una utilidad de CA Identity Manager para gestionar conectores dinámicos, asignar conectores dinámicos a puntos finales y establecer reglas de enrutamiento para puntos finales. Se puede utilizar para configurar conectores dinámicos para permitir el aprovisionamiento y la gestión de bases de datos SQL y directorios LDAP.

Connector Xpress permite crear e implementar conectores personalizados sin la competencia técnica que se necesita generalmente al crear conectores gestionados por el gestor de aprovisionamiento.

También se puede configurar, editar y eliminar la configuración de un servidor de conectores (tanto Java como C++) mediante Connector Xpress.

La entrada principal a Connector Xpress es el esquema nativo de un sistema de punto final. Por ejemplo, se puede utilizar Connector Xpress para conectarse a RDBMS y recuperar el esquema de SQL de la base de datos. Entonces, se puede utilizar Connector Xpress para crear asignaciones de las partes del esquema nativo que sean relevantes para la gestión y el aprovisionamiento de identidades. Una asignación describe cómo representa la capa de aprovisionamiento un elemento del esquema nativo.

Connector Xpress genera metadatos que describen, a un conector dinámico, las asignaciones de tiempo de ejecución a un sistema de destino.

El resultado de Connector Xpress es un documento de metadatos que se genera cuando se completan las asignaciones. Los metadatos es un archivo XML que describe la estructura de su conector a Servicios de la nube de CA IAM.

Describe las clases del servidor de aprovisionamiento y los atributos y cómo se asignan al esquema nativo.

Los metadatos se utilizan para crear tipos de puntos finales dinámicos en uno o varios servidores de aprovisionamiento.

Nota: Para obtener más información sobre el uso de Connector Xpress, consulte la *Guía de Connector Xpress*, en la *biblioteca de CA Identity Manager*.

Componentes adicionales

CA Identity Manager incluye algunos componentes adicionales, que son compatibles con la funcionalidad de CA Identity Manager. Algunos de estos componentes se instalan con CA Identity Manager y algunos se deberán instalar por separado.

Flujo de trabajo de Workpoint

El motor del flujo de trabajo WorkPoint y el diseñador del punto de trabajo se instalan automáticamente cuando se instala CA Identity Manager.

Estos componentes permiten colocar una tarea de CA Identity Manager en el control del flujo de trabajo y modificar definiciones del proceso de flujo de trabajo existentes o crear definiciones nuevas.

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

Gestor de aprovisionamiento

El gestor de aprovisionamiento de CA Identity Manager gestiona el servidor de aprovisionamiento mediante una interfaz gráfica. Se utiliza para tareas administrativas como la gestión de opciones del servidor de aprovisionamiento. En algunos casos, también se puede utilizar el gestor de aprovisionamiento para gestionar ciertos atributos de punto final, que no se pueden gestionar en la Consola de usuario de CA Identity Manager.

El gestor de aprovisionamiento está instalado como parte de las herramientas administrativas de CA Identity Manager.

Nota: Esta aplicación se ejecuta en sistemas de Windows solamente.

Para obtener más información sobre el gestor de aprovisionamiento, consulte la *Guía de referencia de aprovisionamiento*.

Servidor de informes de IAM

CA Identity Manager proporciona informes que se pueden utilizar para controlar el estado de un entorno de CA Identity Manager. Para utilizar los informes proporcionados con CA Identity Manager, se instala el servidor de informes de IAM, que se incluye con CA Identity Manager.

El servidor de informes de IAM utiliza la tecnología de Business Objects Enterprise XI. Si se dispone de un servidor de Business Objects, se puede utilizar en lugar del servidor de informes de IAM para generar informes de CA Identity Manager.

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

Instalaciones de CA Identity Manager de ejemplo

Con CA Identity Manager, se pueden controlar identidades del usuario y su acceso a aplicaciones y cuentas en sistemas de punto final. Según la funcionalidad que se necesite, se selecciona qué componentes de CA Identity Manager se instalan.

En todas las instalaciones de CA Identity Manager, el servidor de CA Identity Manager se instala en un servidor de aplicaciones. El instalador de CA Identity Manager se utiliza para instalar los demás componentes que se necesiten.

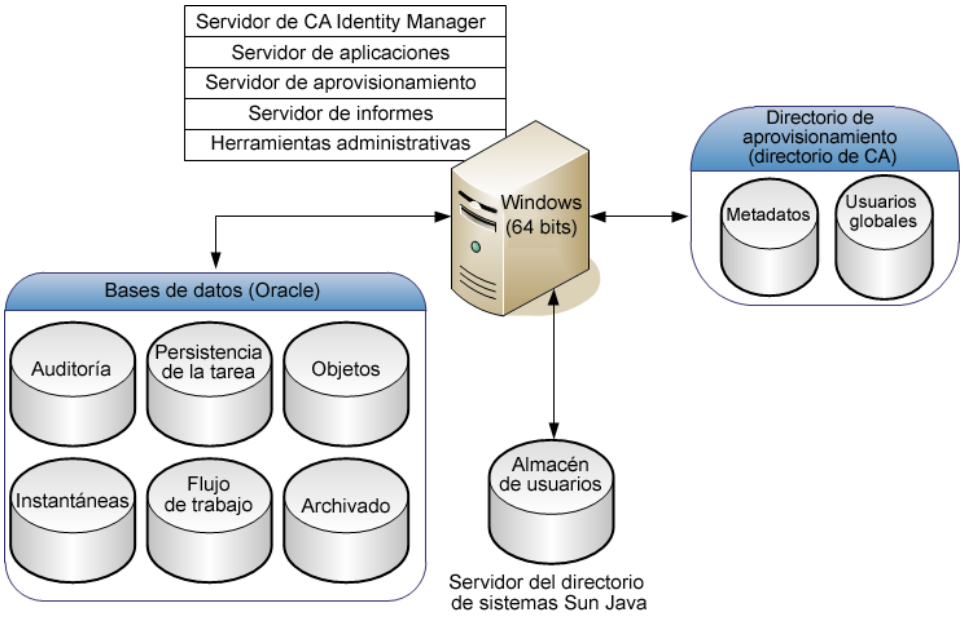
En las siguientes secciones se ilustran algunos ejemplos de implementaciones de CA Identity Manager a un nivel alto.

Instalación con componentes de aprovisionamiento

El aprovisionamiento de CA Identity Manager permite crear un entorno que se conecte a un servidor de aprovisionamiento para cuentas de aprovisionamiento a diversos sistemas de puntos finales. Se pueden asignar roles de aprovisionamiento a los usuarios que se creen mediante CA Identity Manager. Los roles de aprovisionamiento son roles con plantillas de cuenta que definen las cuentas que los usuarios pueden recibir en sistemas de puntos finales. Las cuentas proporcionan a los usuarios el acceso a recursos adicionales, como una cuenta de correo electrónico.

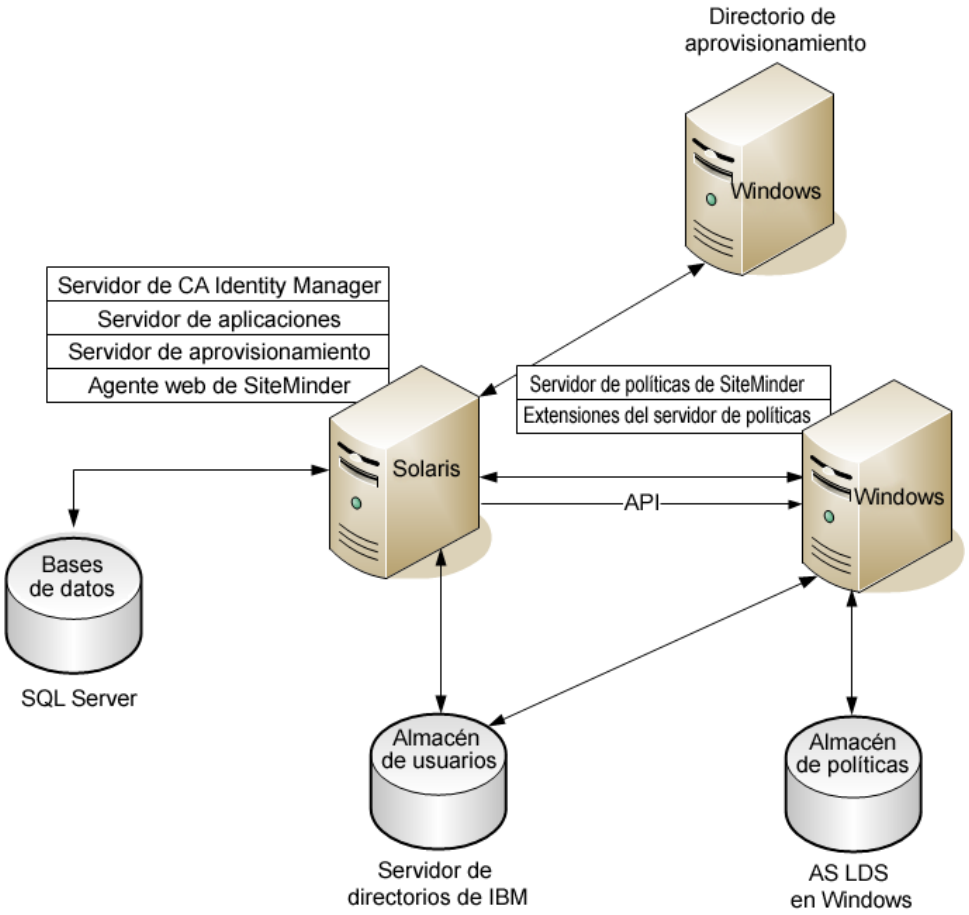
Cuando se asigna un rol de aprovisionamiento a un usuario, dicho usuario recibe las cuentas definidas por las plantillas de cuenta en el rol. Las plantillas de cuenta también definen cómo los atributos de usuario se asignan a las cuentas. Las cuentas se crean en puntos finales gestionados definidos por las plantillas de cuenta.

La siguiente ilustración es un ejemplo de una instalación de CA Identity Manager con aprovisionamiento:



Instalación con el servidor de políticas SiteMinder

Un servidor de políticas SiteMinder proporciona una autenticación avanzada y una protección para su entorno de CA Identity Manager. La siguiente ilustración es un ejemplo de una instalación de CA Identity Manager con un servidor de políticas de SiteMinder:



Una implementación de CA Identity Manager que incluye SiteMinder incluye todos los componentes de la instalación básica o la instalación con aprovisionamiento, más estos componentes adicionales:

Agente Web de SiteMinder

Funciona con el servidor de políticas de SiteMinder para proteger la Consola de usuario. 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, y otras funciones como Password Services y Single-Sign On.

Extensiones para el servidor de políticas SiteMinder

Permite que un servidor de políticas de SiteMinder sea compatible con CA Identity Manager. Las extensiones se deben instalar en cada sistema de servidor de políticas de SiteMinder de la implementación de CA Identity Manager.

Almacén de políticas de SiteMinder

Almacena información que SiteMinder necesita para gestionar el acceso a los recursos Web.

Cuando CA Identity Manager se integra con SiteMinder, el almacén de políticas también incluye información sobre entornos y directorios de CA Identity Manager para que SiteMinder pueda proporcionar autenticación avanzada.

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.

Capítulo 4: Planificación de la implementación

Para planificar una implementación de CA Identity Manager, se decide cómo CA Identity Manager gestionará los usuarios y qué funciones se necesitan para lograr los objetivos de negocio. Algunas cuestiones que se deben tener en cuenta son las siguientes:

- ¿Cómo se gestionan usuarios?
- ¿El aprovisionamiento de cuentas es necesario?
- ¿Cuáles son los requisitos personalizados de mi negocio y debería implementarlos mediante el flujo de trabajo?

Según las decisiones que se tomen, se puede determinar la mejor forma de implementar CA Identity Manager para su entorno.

Esta sección contiene los siguientes temas:

Decisión de qué gestionar

La decisión que lo que se desea gestionar ayudará a determinar qué componentes se desean instalar. El uso de CA Identity Governance permite gestionar lo siguiente:

- Identidades de usuarios
- Acceso a cuentas en sistemas de puntos finales

Identidades de usuarios

Las identidades de usuarios representan a las personas que debe gestionar una compañía, como empleados, contratistas y proveedores, entre otros.

Para gestionar identidades de usuarios, es necesario instalar solamente el servidor de CA Identity Manager y las herramientas administrativas.

Cómo configurar la compatibilidad con la gestión de usuarios

En CA Identity Manager, se gestionan los usuarios con roles de administrador, que determinan las tareas de CA Identity Manager que los administradores pueden realizar.

Nota: Antes de implementar la gestión de usuarios en CA Identity Manager, se debe determinar qué funcionalidad se necesita y desarrollar un plan (en la página 58) para implementarla en etapas.

Para configurar la compatibilidad de la gestión de usuarios, complete los siguientes pasos de alto nivel:

1. Instale el servidor de CA Identity Manager y las herramientas administrativas.

   Si se necesita aprovisionar cuentas para usuarios gestionados, también será necesario instalar compatibilidad para el aprovisionamiento (en la página 45).

   Nota: Consulte la *Guía de instalación* para obtener instrucciones.

2. Cree lo siguiente en la Consola de gestión de CA Identity Manager:

   - **Directorio de CA Identity Manager**

     Describe un almacén de usuarios para CA Identity Manager. Incluye la siguiente información:

     - 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 se representan en CA Identity Manager.

   - **Entorno de CA Identity Manager**

     Proporciona un espacio de nombres de gestión que permite a los administradores de CA Identity Manager gestionar objetos como usuarios, grupos y organizaciones, con un conjunto de roles asociados y tareas. El entorno de CA Identity Manager controla la presentación gráfica y la gestión de un directorio.

   Para obtener más información sobre entornos y directorios de CA Identity Manager, consulte la *Guía de configuración*.

3. Modifique las tareas y los roles de administrador predeterminados para que se adapten a los requisitos del negocio.

   Entre las modificaciones de roles más habituales se incluyen la adición o eliminación de tareas predeterminadas de roles de administrador existentes, o la creación de roles de administrador nuevos, que estén basados en los roles predeterminados.

Entre las modificaciones de tareas más habituales se incluyen la personalización de las fichas de perfil de usuario predeterminadas para incluir solamente la información de que se desea gestionar. (Las fichas de perfil predeterminadas incluyen todos los atributos definidos para los usuarios).

Para obtener información acerca de la modificación de tareas y roles de administrador predeterminados, consulte la *Guía de diseño de la Consola de usuario*.

4. Asigne los roles de administrador a los usuarios que realizarán tareas de gestión de usuarios.

Aprovisionamiento de cuentas desde otras aplicaciones

La decisión de implementar el aprovisionamiento depende del tipo de información que se necesite gestionar. Si se está gestionando un directorio de usuarios central y no se desea gestionar cuentas de usuario en otros sistemas, no se necesita aprovisionamiento. Si se desea gestionar cuentas de usuario en varios sistemas, se deberá implementar compatibilidad para el aprovisionamiento.

Las capacidades de aprovisionamiento las proporciona el servidor de aprovisionamiento, que está integrado con CA Identity Manager. El servidor de aprovisionamiento proporciona las siguientes funcionalidades para el aprovisionamiento de cuentas:

- Gestión de puntos finales
- Sincronización de cuentas
- Plantillas de cuenta
- Funcionalidad Explorar y correlacionar

Nota: La información de aprovisionamiento se almacena en un directorio de aprovisionamiento. Si CA Identity Manager mantiene usuarios en otro tipo de directorio, la implementación incluirá un almacén de usuarios de CA Identity Manager y un directorio de aprovisionamiento.

Gestión de puntos finales

Para aprovisionar cuentas, se deben definir y gestionar puntos finales en la Consola de usuario de CA Identity Manager. Un *punto final* es un sistema para el cual los usuarios necesitan acceso. Entre algunos ejemplos de puntos finales se incluyen bases de datos de Oracle, servidores de UNIX NIS, servidores de Windows y servidores de Microsoft Exchange. Las *plantillas de cuenta* (en la página 46) se utilizan para crear cuentas y determinar las capacidades de los usuarios en los puntos finales gestionados.

Nota: También se puede utilizar el gestor de aprovisionamiento para definir y gestionar puntos finales. Aunque se recomienda el uso de la Consola de usuario para la mayor parte de las tareas de gestión de puntos finales, hay algunas tareas que requieren el uso del gestor de aprovisionamiento, como la gestión de ciertos atributos de punto final y la de objetos de punto final que no sean cuentas. Para obtener más información sobre el gestor de aprovisionamiento, consulte la *referencia de aprovisionamiento*.

Sincronización de cuentas

Se pueden sincronizar cuentas de usuario de diversos puntos finales gestionados. Cuando se activa la sincronización de cuentas, al hacer un cambio en un perfil de usuario en el servidor de aprovisionamiento, éste se propaga a todos los puntos finales donde el usuario tenga una cuenta.

Nota: En la ficha Perfil, se especifica la configuración de la sincronización de cuentas para una tarea de CA Identity Manager. Para obtener más información acerca de la configuración de la sincronización de cuentas, consulte la *Guía de administración*.

Plantillas de cuenta

En las plantillas de cuenta se define cómo se representa un usuario en un punto final gestionado. Por ejemplo, una plantilla para una cuenta de Exchange podría definir el formato de la dirección de correo electrónico de un usuario, como <primera inicial><apellido>@miempresa.com.

Las plantillas de cuenta también determinan los privilegios que un usuario tiene dentro de un sistema gestionado. Por ejemplo, además de definir el formato de una dirección de correo electrónico, puede que una plantilla para una cuenta de Exchange también limite el tamaño del buzón de correo de un usuario.

Las plantillas de cuenta se crean y gestionan en la Consola de usuario.

Funcionalidad Explorar y correlacionar

Las funciones de Explorar y correlacionar simplifican la gestión de puntos finales, ya que detectan y sincronizan los cambios de sistemas gestionados.

La función de exploración busca objetos, incluidas cuentas, en puntos finales y almacena referencias a ellos en el directorio de aprovisionamiento. Se puede utilizar la función exploración para detectar los objetos nuevos que se deban gestionar. Por ejemplo, si se aprovisionan cuentas en un directorio LDAP y se agregan organizaciones nuevas en dicho directorio, se puede utilizar la función de exploración para introducir esas organizaciones nuevas para que se utilicen en plantillas de cuenta.

La función de correlación asocia una cuenta de un punto final gestionado a un usuario global en el directorio de aprovisionamiento. Cuando se hace un cambio en la cuenta mediante el punto final, la función de correlación puede sincronizar dichos cambios con la cuenta de usuario global.

Nota: Para obtener más información acerca de la funcionalidad Explorar y correlacionar, consulte la *Guía de administración*.

Cómo configurar la compatibilidad con el aprovisionamiento

Si decide implementar el aprovisionamiento, complete los siguientes pasos de alto nivel.

1. Utilice el instalador del servidor de CA Identity Manager para instalar el servidor de CA Identity Manager, el servidor de aprovisionamiento, la inicialización del directorio de aprovisionamiento y las herramientas administrativas.

   Nota: Para obtener más información acerca de la instalación de componentes de CA Identity Manager, consulte la *Guía de instalación*.

2. Configure el gestor de aprovisionamiento para conectarse al servidor de CA Identity Manager.

3. Configure el aprovisionamiento en la Consola de gestión de CA Identity Manager:

   a. Active el aprovisionamiento.

   b. Configure un entorno para el aprovisionamiento completando lo siguiente:

      - Importación de definiciones de roles personalizadas
      - Configuración de un administrador de entrada
      - Conexión del entorno al servidor de aprovisionamiento.

   Nota: Para obtener más información, consulte la *Guía de configuración*.

4. Cree puntos finales en la Consola de usuario.

   Esto permite que CA Identity Manager gestione el punto final.

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

5. Exploración y correlación del punto final.

   Al explorar un punto final, CA Identity Manager busca los objetos en el punto final y almacena instancias de ellos en el directorio de aprovisionamiento. Esta acción rellena el directorio de aprovisionamiento con cuentas y otros objetos que se encuentran en el punto final.

   Cuando se correlacionan cuentas en un punto final, CA Identity Manager las asocia con un usuario global en el directorio de aprovisionamiento. Se puede elegir si la función de correlación crea usuarios globales que no están presentes o si asocia cuentas que no coincidan con ningún usuario global al usuario global [usuario predeterminado].

6. Cree y mantenga cuentas de puntos finales mediante plantillas de cuenta, que contienen los atributos que se utilizan para crear cuentas.

7. Asocie las plantillas de cuenta con roles de aprovisionamiento.

   Cuando se asignan roles de aprovisionamiento a usuarios, CA Identity Manager crea cuentas en los puntos finales asociados para esos usuarios.

   Nota: Para obtener información acerca de las plantillas de cuenta y los roles de aprovisionamiento, consulte la *Guía de administración*.

Determinación de requisitos de la auditoría

CA Identity Manager incluye capacidades de auditoría que permiten controlar actividades en un entorno de CA Identity Manager.

Esta información se almacena en una base de datos de auditoría. La cantidad y el tipo de información que se almacena en la base de datos de auditoría se puede configurar.

Los datos de auditoría se pueden consultar en la Consola de usuario mediante la tarea Ver tareas enviadas. Esta tarea permite a los administradores buscar y ver tareas que se produzcan en el sistema. Los administradores pueden consultar la información de la tarea a un nivel alto o ver detalles del evento y la tarea.

Consideraciones de auditoría de CA Identity Manager

Los datos de auditoría proporcionan un registro del historial de operaciones que se producen en un entorno de CA Identity Manager. Para realizar una auditoría de datos en CA Identity Manager, se necesita lo siguiente:

- Una base de datos de auditoría
- Un archivo de configuración de auditoría

Base de datos de auditoría

Cuando se utiliza el instalador de CA Identity Manager, CA Identity Manager configura una conexión a una base de datos única (base de datos de CA Identity Manager) y crea un origen de datos para conectarse a las tablas de base de datos para la auditoría.

Nota: La base de datos de CA Identity Manager también incluye datos que utiliza otra funcionalidad de CA Identity Manager, entre los que se incluyen la persistencia de la tarea, el flujo de trabajo y la generación de informes. Con fines de escalabilidad, se puede crear una instancia nueva independiente de una base de datos para auditar.

Nota: Para obtener más información acerca de las bases de datos para auditorías, consulte la *Guía de instalación*.

Configuración de la auditoría

Las auditorías se configuran en un archivo de configuración de auditoría. Un archivo de configuración de auditoría determina la cantidad y tipo de información que CA Identity Manager audita. Se puede configurar un archivo de configuración de auditoría para realizar lo siguiente:

- Activar la auditoría para un entorno 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, 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.

Nota: Para obtener más información acerca de la configuración de auditorías, consulte la *Guía de configuración*.

Consideraciones de CA Audit

CA Audit es un sistema de gestión de auditorías que permite recopilar y almacenar datos relacionados con la seguridad de la auditoría, la generación de informes, la verificación de la conformidad y el control de eventos.

Para integrarse con CA Audit, se debe instalar el componente de iRecorder cuando se instala el servidor de CA Identity Manager. El componente iRecorder recupera eventos de CA Identity Manager. En función de las políticas del gestor de políticas de CA Audit, el iRecorder ignora el evento o lo enruta mediante CA Audit.

Decisión de los requisitos del almacén de usuarios

Una implementación de CA Identity Manager debe incluir un almacén de usuarios que contenga las identidades del usuario que mantiene CA Identity Manager. Normalmente es un almacén de usuarios existente que una empresa utiliza para almacenar información acerca de sus usuarios, como empleados y clientes.

Si la implementación incluye aprovisionamiento, CA Identity Manager también requiere un directorio de aprovisionamiento que incluya usuarios globales, que se asocia a cuentas en puntos finales como Microsoft Exchange, Active Directory y Oracle.

Gestión de varios almacenes de usuarios

Una empresa puede mantener varios almacenes de usuarios. En cada almacén de usuarios, la identidad del usuario permite acceder a distintos recursos corporativos. Se puede utilizar uno de los métodos siguientes para gestionar varios almacenes de usuarios:

- Utilice CA Identity Manager para gestionar de forma directa el directorio de aprovisionamiento y utilice el servidor de aprovisionamiento para gestionar de forma indirecta los usuarios y las cuentas de los distintos almacenes de usuarios.

  Este enfoque permite:

  - Gestionar de forma centralizada los usuarios a los que se les pueden asignar diversos recursos empresariales de una ubicación.
  - Implementar la seguridad habitual y reglas de negocio mediante recursos de la empresa. Esto puede incluir lo siguiente:
    - Control de acceso basado en los roles
    - Administración delegada
    - Tareas y pantallas personalizadas en función del tipo de identidades corporativas que gestionan

- Políticas de identidad para la gestión de identidades basada en reglas
- Personalización y extensibilidad

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

- Cree un entorno de CA Identity Manager independiente para gestionar cada almacén de usuarios.

  Con este método, la información no se comparte entre entornos.

Selección de los componentes de la instalación

La siguiente tabla muestra los componentes que se deben instalar para que se admita la funcionalidad que se desea implementar.

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

Si desea...	Instale estos componentes
Gestionar identidades de usuarios en un almacén de usuarios corporativo existente	■ Servidor de CA Identity Manager
Aprovisionar cuentas en sistemas de punto final	■ Servidor de aprovisionamiento ■ Directorio de aprovisionamiento ■ Gestor de aprovisionamiento ■ Conectores ■ Servidores de conectores **Nota**: Para obtener instrucciones sobre la instalación de conectores, consulte la *Guía del conector* del tipo de conectores que desee instalar.

Si desea...	Instale estos componentes
Implemente una o varias de las siguientes funciones: ■ Autenticación avanzada ■ Políticas de contraseñas avanzadas ■ Máscaras de consola diferentes para conjuntos de usuarios diferentes ■ Preferencias de configuración regional para los usuarios	■ Servidor de políticas de SiteMinder ■ Almacén de políticas ■ Agente Web de SiteMinder ■ Extensiones de CA Identity Manager al servidor de políticas **Nota**: Para obtener instrucciones sobre la instalación del almacén de políticas y el servidor de políticas de SiteMinder, consulte la *Guía de instalación del servidor de políticas del gestor de acceso Web de CA SiteMinder.* Para obtener instrucciones sobre la instalación del agente Web, consulte la *Guía de instalación del agente Web del gestor de acceso Web de CA SiteMinder.*
Generación de informes sobre la actividad de CA Identity Manager	Servidor de informes de IAM

Decisión de los requisitos de hardware

El hardware necesario para una instalación de CA Identity Manager depende de la funcionalidad que se desea implementar y del tamaño de la implementación.

En las siguientes secciones se describen implementaciones habituales de CA Identity Manager y el hardware que requieren.

Tipos de implementación

Al planear el hardware necesario para una implementación de CA Identity Manager, se deben tener en cuenta las funciones que se desean implementar y el tamaño inicial de la implementación. Las siguientes categorías permiten calcular el tamaño de la implementación.

Nota: El tipo de implementación que se selecciona determina el tamaño del archivo DxGrid que utiliza el directorio de aprovisionamiento. Se especifica el tipo de implementación cuando se instala el servidor de CA Identity Manager.

Demostración

Una implementación de servidor única para utilizar en demostraciones o pruebas básicas en un entorno de desarrollo. Una implementación de demostración admite hasta 10000 cuentas de aprovisionamiento.

Nota: Este tipo de implementación no es compatible con implementaciones de producción.

Básico:

Una implementación de alta disponibilidad adecuada para la mayor parte de las implementaciones de tamaño mediano o pequeño. Una implementación básica admite hasta 400000 cuentas de aprovisionamiento.

Este tipo de implementación requiere dos servidores para ejecutar la aplicación de CA Identity Manager y sus componentes y dos servidores para ejecutar la base de datos de CA Identity Manager y el almacén de usuarios.

Intermedio

Una implementación de alta disponibilidad adecuada para las implementaciones de tamaño mediano. Una implementación intermedia admite hasta 600000 cuentas de aprovisionamiento.

Gran empresa

Una implementación de alta disponibilidad que incluye clústeres de servidor adicionales para dirigir usuarios adicionales y un mayor número de transacciones. Una implementación grande admite más de 600000 cuentas de aprovisionamiento.

Nota: Para obtener más información sobre las implementaciones de alta disponibilidad, consulte la *Guía de instalación*.

Requisitos adicionales para el aprovisionamiento

Además de los componentes necesarios para una implementación de CA Identity Manager básica, se requieren los siguientes componentes adicionales cuando CA Identity Manager incluye aprovisionamiento:

- Servidor de aprovisionamiento

  Se puede instalar en el mismo equipo que el servidor de CA Identity Manager.

- Inicialización del directorio de aprovisionamiento

  Importante: La inicialización del directorio de aprovisionamiento se deberá instalar en CA Directory.

- Gestor de aprovisionamiento

  Se puede instalar en cualquier equipo Windows que pueda acceder al servidor de aprovisionamiento.

Nota: En un entorno de desarrollo, estos componentes se pueden instalar en un equipo que también incluya los componentes de instalación básicos.

Requisitos adicionales para integración de SiteMinder

Cuando CA Identity Manager se integra con SiteMinder, la implementación debe incluir los componentes de la instalación de CA Identity Manager básica, más los siguientes componentes adicionales:

- **Servidor de políticas**

  Proporciona servicios de cuentas, gestión de políticas, autenticación y autorización.

  El servidor de políticas se puede instalar en el mismo equipo que el servidor de CA Identity Manager, si el servidor de políticas es para CA Identity Manager. Si el servidor de políticas está protegiendo otras aplicaciones, se recomienda su instalación en un equipo independiente para garantizar un mejor rendimiento.

- **Almacén de políticas**

  Contiene todos los datos del servidor de políticas. Se puede configurar un almacén de políticas en un LDAP compatible o base de datos relacional. En implementaciones de disponibilidad alta, se recomienda la instalación del almacén de políticas en un servidor independiente.

- **Extensiones al servidor de políticas**

  Permite que un servidor de políticas de SiteMinder sea compatible con CA Identity Manager. Las extensiones se deben instalar en cada sistema de servidor de políticas de SiteMinder de la implementación de CA Identity Manager.

- **Agente Web de SiteMinder**

  Funciona con el servidor de políticas de SiteMinder para proteger la Consola de usuario. Se instala en el sistema con el servidor de CA Identity Manager.

Elección de un método para importar usuarios

Si es necesario importar usuarios en un almacén de usuarios existente, el método que se seleccione debe estar basado en los requisitos del negocio.

Las siguientes secciones describen opciones para importar usuarios.

Cómo importar usuarios en un almacén de usuarios nuevo

Tras decidir cómo almacenar los datos de los usuarios, puede ser necesario importar usuarios de un almacén a otro. En función de la implementación, se pueden utilizar métodos diferentes para importar usuarios.

Nota: Después de haber importado usuarios a un almacén de usuarios nuevo, se pueden utilizar políticas de identidad (en la página 56) para aplicar cambios los a usuarios importados.

Importación de usuarios mediante CA Identity Manager

CA Identity Manager proporciona los siguientes métodos para agregar usuarios a un almacén de usuarios que gestiona directamente.

Método	Características	Limitaciones
Cargador masivo	Permite utilizar la tarea del cargador masivo en la Consola de usuario para cargar archivos del alimentador que se utilizan para manipular grandes cantidades de objetos gestionados simultáneamente. La ventaja del método del cargador masivo es que permite automatizar el proceso de manipulación de una gran cantidad de objetos gestionados con un archivo de información (del alimentador). La tarea Cargador masivo también se puede asignar a un proceso de flujo de trabajo.	Si se está utilizando el cargador masivo, puede que se observen excepciones que no se encuentran en la memoria en función del número de usuarios que se estén importando. Para abordar esta incidencia, se deben aumentar los valores de configuración de memoria de JVM.
Invocación de tarea remota mediante servicio Web de ejecución de tareas (TEWS)	Permite la ejecución de cualquier tarea de CA Identity Manager que esté activada para servicios Web, incluida la tarea Crear usuario. Si la tarea se configura para la sincronización de usuarios, CA Identity Manager ejecutará cualquier política de identidad aplicable.	Es posible que las características del rendimiento de modelo de servicio Web no sean adecuadas para requisitos de alto rendimiento de operaciones de importación masiva.

API de IM	■ Proporciona API basadas en el usuario que se pueden invocar directamente para crear usuarios mediante un cliente Java. ■ Proporciona las capacidades de rendimiento más altas.	■ Omite los mecanismos de seguridad y auditoría que proporciona el servidor de la tarea. ■ No es compatible con la ejecución de políticas de identidad.

Nota: Para obtener más información sobre el cargador masivo, consulte la *Guía de administración*. Para obtener más información sobre TEWS y la API de IM, consulte la *Guía de programación para Java*.

Ejecución de políticas de identidad en usuarios importados

Una *política de identidad* es un conjunto de cambios empresariales que se producen cuando un usuario cumple una cierta condición o regla. Estos cambios pueden incluir la asignación o revocación de roles (incluidos los roles de aprovisionamiento para usuarios en el directorio de aprovisionamiento), la asignación o revocación de pertenencia a grupos y la actualización de atributos en un perfil de usuario.

Se pueden utilizar políticas de identidad para aplicar cambios a cuentas de usuario después de que se hayan importado a un almacén de usuarios nuevo.

En esta sección se describen métodos para ejecutar políticas de identidad en usuarios importados en uno o dos pasos.

Procedimiento en un paso

Se pueden utilizar los siguientes métodos de importación para ejecutar políticas de identidad en usuarios que importe a un almacén de usuarios nuevo en un paso único:

- Cargador masivo en la Consola de usuario
- Ejecución de la tarea Crear usuario mediante TEWS
- Sincronización de entrada

Procedimiento en dos pasos

Mediante un procedimiento en dos pasos, primero se importan los usuarios y, a continuación, se ejecutan políticas de identidad para esos usuarios. Se puede utilizar este método cuando CA Identity Manager gestiona los usuarios en el servidor de aprovisionamiento. Este método puede proporcionar más flexibilidad, en función de los requisitos de la importación.

1. Utilizar una de las herramientas de importación para agregar usuarios al directorio de aprovisionamiento.
2. Invocar la tarea de sincronizar usuario de CA Identity Manager mediante TEWS en cada uno de los usuarios importados.

Importación de usuarios mediante el servidor de aprovisionamiento

El servidor de aprovisionamiento incluye opciones de importación masiva para agregar y gestionar usuarios en el directorio de aprovisionamiento. En las siguientes tablas se describen los métodos para importar usuarios en el directorio de aprovisionamiento.

Método	Características	Limitaciones
Utilidad por lotes (etautil)	Una utilidad de interfaz de línea de comandos que permite gestionar objetos en el directorio de aprovisionamiento.	■ Actualmente sólo es compatible con sistemas Windows.
Explorar y correlacionar	■ Detecta objetos nuevos que el servidor de aprovisionamiento puede gestionar en un punto final conocido (incluidos usuarios). ■ Proporciona capacidades de correlación para instancias de objeto que existen en el punto final y el servidor de aprovisionamiento. Se puede obtener información adicional en Funcionalidad Explorar y correlacionar.	■ De forma predeterminada, la funcionalidad Explorar y correlacionar está disponible para los conectores compatibles actualmente. Se puede extender con conectores personalizados. ■ La opción de correlación puede afectar a la escalabilidad al trabajar con grandes cantidades de usuarios. Si se selecciona esta opción de importación, es necesario asegurarse de evaluar las implicaciones de rendimiento y escalabilidad.

Sincronización de los usuarios globales con el almacén de usuarios de CA Identity Manager

Después de importar los usuarios en el servidor de aprovisionamiento, se pueden utilizar los siguientes métodos para agregar dichos usuarios al almacén de usuarios de CA Identity Manager:

- **Sincronización de entrada**

  La sincronización de entrada mantiene a los usuarios de CA Identity Manager actualizados con los cambios que se produzcan en el directorio de aprovisionamiento. En los cambios en el directorio de aprovisionamiento se incluyen los que se realicen mediante el gestor de aprovisionamiento o sistemas con conectores al servidor de aprovisionamiento.

  Debe tenerse en cuenta lo siguiente al utilizar la sincronización de entrada para importar usuarios:

  - En la Consola de gestión de CA Identity Manager, se puede personalizar cómo se asignan los atributos de la solicitud de entrada a los atributos de la tarea de CA Identity Manager.

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

  - Debe tenerse en cuenta qué cambios del servidor de aprovisionamiento requieren sincronización con el almacén de usuarios corporativo. La sincronización de un gran número de cambios puede afectar al rendimiento y la escalabilidad.

- **Roles de aprovisionamiento y plantillas de cuenta**

  El servidor de aprovisionamiento puede gestionar cuentas en el almacén de usuarios de CA Identity Manager mediante roles de aprovisionamiento y plantillas de cuenta. Para esto es necesario haber adquirido un punto final gestionado, que apunte al almacén de usuarios de CA Identity Manager, y que existan los roles y las plantillas de cuenta adecuados. En este caso, a los usuarios globales creados mediante una de las opciones descritas en Importación de usuarios mediante el servidor de aprovisionamiento se les puede asignar un rol de aprovisionamiento que crea la cuenta de usuario en el almacén de usuarios de CA Identity Manager.

Desarrollo de un plan de implementación

Al planear una implementación grande, se debe implementar la funcionalidad de CA Identity Manager en etapas. El siguiente orden de implementación permite obtener rápidamente un valor significativo de CA Identity Manager, evaluar las necesidades cambiantes de su implementación de forma gradual y construir cuidadosamente el entorno para conseguir el mejor rendimiento y escalabilidad:

- Autoservicio y gestión de contraseñas
- Políticas de identidad

- Aprobaciones de flujo de trabajo
- Administración delegada los objetos de organización, grupo y usuario
- Administración delegada para la administración de roles

Después de cada etapa de la implementación, es necesario asegurarse de evaluar el rendimiento y realizar ajustes antes de continuar a la siguiente etapa. En Optimización de CA Identity Manager (en la página 69) se proporciona información sobre el rendimiento, la optimización y la escalabilidad.

Implementación de autoservicio y gestión de contraseñas

Se deben implementar las tareas de autoservicio y la gestión de contraseñas antes de implementar otras funciones de CA Identity Manager por los siguientes motivos:

- Las tareas de autoservicio y la gestión de contraseñas son fáciles de implementar y proporcionan rápidamente un valor significativo.
- Estas funciones son independientes del modelo de administración delegado y se pueden reconfigurar según sea necesario para abordar las necesidades empresariales cambiantes.
- Estas funciones normalmente generan el volumen más alto de tareas que CA Identity Manager procesa de forma regular. A causa de esto, proporcionan una forma de probar la escalabilidad de la implementación antes de implementar funciones adicionales.

Para implementar tareas de autoservicio, complete los pasos siguientes:

1. Configure la tarea de autorregistro.

   Esto es una tarea pública, que se activa de forma predeterminada durante la instalación. Para configurar esta tarea, agregue o elimine campos de la tarea de autorregistro predeterminada, según sea necesario.

2. Implemente el rol de autogestor.

   La regla de miembro para este rol se debe configurar para que se aplique a todos los usuarios o debe incluir una regla de miembro que asigne automáticamente el rol a los usuarios nuevos. Por ejemplo, se puede crear una regla de miembro que asigne el rol de autogestor a todos los empleados a tiempo completo. Cuando se autorregistre un usuario, CA Identity Manager podrá establecer el tipo de empleado como jornada completa (mediante un identificador de atributos lógicos o un identificador de tareas del negocio). El usuario cumple los criterios de la regla de miembro y recibe el rol de autogestor automáticamente.

   Nota: Cuando configure reglas de miembro para el rol de autogestor, no permita a los administradores agregar o eliminar miembros del rol. Dado que el rol se asigna automáticamente, no es necesario que un administrador lo asigne explícitamente.

Para implementar las capacidades de gestión de contraseñas, complete los siguientes pasos:

1. Configure las tareas de gestión de contraseñas públicas, como la tarea Contraseña olvidada.
2. Cree políticas de contraseñas que determinen cómo se crean y cuándo caducan las contraseñas.
3. Implemente el rol del gestor de contraseñas, que permite a los miembros del rol restablecer contraseñas de usuario.

Nota: Para obtener información acerca de roles, tareas y gestión de contraseñas, consulte la *Guía de administración*.

Implementación de políticas de identidad

Una política de identidad es un conjunto cambios empresariales que se producen cuando un usuario cumple una cierta condición o regla. Se pueden utilizar políticas de identidad para proporcionar autorizaciones controladas por el negocio antes de implementar un modelo de delegación completo. Por ejemplo, se puede crear una política de identidad que asigne el rol de aprovisionamiento Director de ventas, que concede acceso a las aplicaciones de ventas, a todos los usuarios cuyo título sea Director de ventas. Cuando un representante de ventas se asciende a director de ventas, recibe automáticamente acceso a todos los sistemas que necesita para trabajar sin tener que esperar la participación del administrador.

Para implementar políticas de identidad, complete los pasos siguientes:

1. Configure las políticas de identidad que se activen mediante cambios a atributos del perfil de usuario.
2. Configure el rol Gestor de usuarios para permitir que un pequeño número de administradores utilicen las tareas de usuario, como Crear usuario y Modificar usuario, para cambiar los atributos que activan las políticas de identidad.

   Asegúrese de configurar las reglas de ámbito en las políticas de miembros de Gestor de usuarios para determinar el conjunto de usuarios que los miembros del rol pueden gestionar.

Tenga en cuenta lo siguiente al implementar políticas de identidad:

- Al principio se debe considerar la posibilidad de crear políticas de identidad que concedan autorizaciones que *no* requieran aprobaciones del flujo de trabajo. Esto permite implementar políticas de identidad sin tener que definir los procesos de flujo de trabajo, los formularios de aprobación ni los modelos de aprobador.
- Antes de crear políticas de identidad, se deben conocer otros métodos de implementación de reglas de negocio en CA Identity Manager, como las reglas de validación de datos, los atributos lógicos, los identificadores de tareas lógicas del negocio y los procesos de flujo de trabajo, para determinar qué método proporciona la mejor solución.

  Nota: Para obtener más información sobre estos métodos, consulte la *Guía de administración* y la *Guía de programación para Java*.
- Las políticas de identidad son una forma eficaz de asignar autorizaciones en CA Identity Manager, sin embargo, puede que afecten al rendimiento de forma significativa (en la página 85).
- Para la implementación inicial de las tareas de usuario, se debe considerar la posibilidad de eliminar u ocultar las fichas de relación, como las fichas Roles, que gestionan las mismas autorizaciones que las políticas de identidad. Esto evita el riesgo de autorizaciones no permitidas e impide el impacto potencial en el rendimiento de roles creados de forma incorrecta.

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

Implementación de aprobaciones del flujo de trabajo

Las aprobaciones del flujo de trabajo pueden agregar un nivel adicional de seguridad y automatización a la implementación de CA Identity Manager.

Para realizar la implementación de aprobaciones del flujo de trabajo se requieren las siguientes tareas:

1. Decidir qué eventos o tareas requieren aprobaciones.
2. Definir el conjunto de aprobadores, llamados participantes, para cada proceso de flujo de trabajo.

   Nota: Los asignadores de participantes determinan todos los participantes de forma dinámica. Para mantener buen rendimiento, se debe limitar el número de participantes a treinta usuarios.
3. Configurar los formularios de aprobación.
4. Definir los procesos de flujo de trabajo personalizados, si es necesario.

Aprobaciones de flujo de trabajo de nivel de tarea y entorno

CA Identity Manager es compatible con dos tipos de aprobaciones: aprobaciones de nivel de entorno y aprobaciones de nivel de tarea. Las aprobaciones de nivel de entorno se definen para todas las instancias de un evento, independientemente de las tareas con las que estén asociadas. Las aprobaciones de nivel de tarea se definen para un evento específico asociado con una tarea específica. Las aprobaciones de nivel de tarea tienen prioridad sobre las aprobaciones de nivel de entorno.

La mayor parte de las aprobaciones se definen en el nivel del entorno para garantizar que se produzcan las mismas actividades de flujo de trabajo para un evento, independientemente de la tarea con la cual esté asociado. Sin embargo, en las siguientes situaciones, se debe considerar la posibilidad de implementar un flujo de trabajo de nivel tarea:

- Si se dispone de tareas especializadas que ejecutan cambios empresariales específicos que generan eventos, que no requieren aprobaciones.
- Si se dispone de acciones de cambios, activadas por políticas de identidad, que generan eventos que no requieren una aprobación del flujo de trabajo.
- Si se necesita la flexibilidad para asociar procesos de flujo de trabajo específicos con cambios específicos de tarea.

Puede que las aprobaciones de nivel de entorno requieran una cantidad significativa de recursos de sistema y procesamiento a medida que el volumen de transacciones aumente. Esto puede terminar por provocar incidencias de rendimiento y escalabilidad. El uso de aprobaciones de nivel de tarea, cuando sean adecuadas, puede reducir o eliminar estas incidencias.

Implementación de administración delegada para usuarios, grupos y organizaciones

La administración delegada es la gestión de usuarios y sus autorizaciones para que distintos usuarios de CA Identity Manager desempeñen las funciones de modificar, asignar y utilizar un rol.

Nota: Los modelos de delegación se deberán crear cuidadosamente para garantizar un buen rendimiento y escalabilidad en la implementación de CA Identity Manager.

Las reglas de ámbito, que se definen en las políticas de miembro y de administración para roles de administrador, imponen una delegación. Una regla de ámbito determina los objetos en los cuales un miembro del rol puede utilizar el rol. Por ejemplo, una regla de ámbito puede permitir que un gestor de usuarios gestione los usuarios de su departamento, pero no de otros departamentos.

Generalmente, las reglas de ámbito deben reflejar la estructura lógica del almacén de usuarios. Por ejemplo, en un almacén de usuarios de LDAP jerárquico, las organizaciones pueden definir el ámbito. En una base de datos relacional, el ámbito se puede definir mediante atributos como el ID de departamento.

Debe tenerse en cuenta lo siguiente al implementar la administración delegada para usuarios, grupos y organizaciones:

- Se debe limitar el acceso a las fichas de relación, como las fichas Roles de administrador y Roles de aprovisionamiento, en las tareas relacionadas con el usuario. Estas fichas de relación se incluyen en tareas de usuario predeterminadas, como Crear usuario y Modificar usuario. Se debe considerar la posibilidad de eliminarlos de las tareas predeterminadas y utilizarlos solamente en tareas especializadas que se asocian con un pequeño número de roles de administrador.
- CA Identity Manager evalúa cada regla de ámbito de forma dinámica; la información de ámbito no se almacena en la memoria caché. Se debe considerar la posibilidad de crear reglas de ámbito que contengan consultas de directorio simples para garantizar un buen rendimiento.
- Para evaluar el rendimiento de las reglas de ámbito se determina cuánto tiempo necesita CA Identity Manager para devolver los objetos que un administrador puede gestionar.

Implementación de la administración delegada para roles

La administración delegada de roles concede los privilegios más significativos en CA Identity Manager y puede tener el efecto más importante (en la página 70) en el rendimiento. Por estos motivos, se debe considerar la posibilidad de implementar la administración delegada para roles después de haber implementado todas las demás funcionalidades.

Al implementar la administración delegada para roles, se debe tener en cuenta lo siguiente:

- Para proteger el entorno y garantizar un buen rendimiento, se limita el número de roles de administrador, miembros de rol de administrador y administradores de rol de administrador.
- Después de implementar la administración delegada para roles, se llevan a cabo pruebas de rendimiento y escalabilidad. El entorno se optimiza según sea necesario.

Capítulo 5: Integración con 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:

Instalación con el servidor de políticas SiteMinder (en la página 41)

Autenticación SiteMinder

CA Identity Manager incluye las siguientes consolas, que se deben proteger:

Consola de usuario

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

Consola de gestión

Permite que los administradores de CA Identity Manager creen y configuren un directorio de CA Identity Manager, un directorio de aprovisionamiento y un entorno de CA Identity Manager.

CA Identity Manager incluye autenticación nativa, que protege la Consola de usuario de forma predeterminada. La Consola de gestión no está protegida de forma predeterminada, pero se puede configurar CA Identity Manager para protegerla. CA SiteMinder también se puede utilizar para proteger la Consola de gestión.

Para configurar otros tipos de autenticación para la Consola de usuario, como certificado o autenticación clave, CA Identity Manager se debe integrar con SiteMinder.

Nota: Para obtener más información, consulte la *Guía de configuración*.

Capítulo 6: Optimización de CA Identity Manager

Esta sección contiene los siguientes temas:

Rendimiento de CA Identity Manager

El rendimiento de CA Identity Manager depende del rendimiento individual de componentes y funciones diferentes.

Se pueden optimizar las siguientes funcionalidades en un entorno de CA Identity Manager:

- Roles
- Tareas
- Gestión y miembros de grupos
- Políticas de identidad

Para obtener un rendimiento adicional, también se pueden optimizar los siguientes componentes:

- Almacén de usuarios
- Componentes de aprovisionamiento
- Componentes de tiempo de ejecución, incluidas las bases de datos, como la base de datos de persistencia de la tarea y la configuración del servidor de aplicaciones.

Para garantizar un mejor rendimiento, se configura la funcionalidad de CA Identity Manager mediante las directrices de las siguientes secciones. A continuación, se mide el rendimiento y se optimizan los componentes, según sea necesario. Dado que los componentes funcionan de manera conjunta, puede que sean necesarias varias iteraciones antes de encontrar la configuración más optimizada para el entorno.

Optimizaciones de roles

CA Identity Manager incluye tres tipos de roles:

- Roles de administrador

  Determinan los privilegios que un usuario tiene en la Consola de usuario.

  Cuando un usuario inicia sesión en un entorno de CA Identity Manager, la cuenta del usuario tiene uno o varios roles de administrador. Cada rol de administrador contiene tareas, como Crear usuario, que un usuario puede completar en ese entorno de CA Identity Manager. Los roles de administrador que tiene un usuario determinan la presentación de la Consola de usuario, por lo tanto, los usuarios ven solamente las tareas que se asocian a sus roles.

- Roles de aprovisionamiento

  Proporcionan a los usuarios cuentas en puntos finales gestionados, como un sistema de correo electrónico.

- Roles de acceso

  Ofrecer una forma adicional de proporcionar autorizaciones en CA Identity Manager.

Los roles incluyen políticas que determinan lo siguiente:

- Quién puede utilizar el rol (solamente para roles de acceso y de administrador) y dónde lo puede utilizar.
- Quién puede gestionar los administradores y los miembros del rol.
- Quién puede modificar la definición del rol.

La evaluación de los roles y sus privilegios asociados puede tener un impacto significativo en el rendimiento de CA Identity Manager.

Cómo afecta la evaluación de roles al rendimiento en el inicio de sesión

Cuando un usuario de CA Identity Manager intenta iniciar sesión en la Consola de usuario, se producen las siguientes acciones:

1. CA Identity Manager pide al usuario que proporcione las credenciales, como un nombre de usuario y una contraseña.
2. Las credenciales del usuario se autentican mediante uno de los métodos siguientes:
   - Autenticación nativa de CA Identity Manager
   - Autenticación de SiteMinder, si la implementación de CA Identity Manager incluye SiteMinder

3. CA Identity Manager evalúa todas las políticas de miembros de todos los roles de administrador del entorno para determinar qué roles de administrador se aplican al usuario.

   Nota: Esta evaluación tiene lugar solamente una vez para un usuario determinado. Después de la evaluación inicial, CA Identity Manager almacena los resultados en la memoria caché. CA Identity Manager utiliza la información almacenada en la memoria caché hasta que se produce un cambio en el usuario o en el conjunto de políticas de miembros, que hace que CA Identity Manager actualice la información en la memoria caché.

4. La Consola de usuario de CA Identity Manager muestra las categorías que el usuario puede ver en función de sus roles.

Este proceso tiene lugar con todos los usuarios que inician sesión en la Consola de usuario. Si un entorno de CA Identity Manager contiene un gran número de roles o políticas de miembros ineficaces, la evaluación de la pertenencia a un rol puede afectar de forma significativa al rendimiento. En este caso, puede que la pantalla inicial que los usuarios ven cuando inician sesión en la Consola de usuario se muestre con lentitud.

Nota: CA Identity Manager no necesita evaluar las políticas de miembros cuando un usuario accede a una tarea pública para realizar un autorregistro o solicitar una contraseña olvidada. En estos casos, CA Identity Manager no necesita una lista de los roles del usuario porque no muestra la Consola de usuario completa.

Rendimiento y objetos de rol

Para ser compatible con cada rol, CA Identity Manager crea varios objetos en el almacén de objetos (en la página 33) de CA Identity Manager, en función de la configuración del rol.

CA Identity Manager crea un objeto base para cada rol. Además del objeto base, CA Identity Manager crea un objeto para cada política.

Una gran cantidad de objetos de rol puede afectar al rendimiento de las búsquedas de almacén de objetos y las evaluaciones de la política.

Rendimiento del almacén de objetos

CA Identity Manager almacena la información que necesita para gestionar usuarios y autorizaciones en un almacén de objetos. Disponer de una gran cantidad de objetos de rol en el almacén de objetos puede provocar las siguientes incidencias:

- Las búsquedas de objetos gestionados en pantallas de tareas de CA Identity Manager pueden llevar más tiempo.

  Para reducir el impacto en las búsquedas, se indexan los atributos que se utilizan en las búsquedas (en la página 90).

- Puede que las tareas de gestión de roles se ejecuten lentamente.

  A continuación se incluyen algunos ejemplos de tareas de gestión de roles que se ven afectadas por un gran almacén de objetos:

  - Una tarea Crear rol de administrador es lenta porque CA Identity Manager debe confirmar que el nombre del rol es único en el almacén de objetos.
  - La tarea Suprimir rol de administrador debe eliminar todos los objetos creados para ser compatible con el rol y la memoria caché del objeto se debe actualizar.

- CA Identity Manager tarda mucho tiempo en evaluar las políticas de rol.

CA Identity Manager almacena información en la memoria caché en el almacén de objetos para mejorar el rendimiento.

Optimización de la evaluación de la política de roles

Para cada rol de administrador, se pueden crear tres tipos de políticas:

- Políticas de miembros

  Definen una regla de miembro, que determina los usuarios que reciben el rol, y las reglas de ámbito, que determinan los objetos que los miembros del rol pueden gestionar.

- Políticas de administración

  Definen reglas de administración, reglas de ámbito y privilegios de administrador para un rol.

- Políticas de propietario

  Definen quién puede modificar un rol.

Para optimizar el rendimiento cuando CA Identity Manager evalúa las políticas de rol, se debe considerar la posibilidad de realizar las siguientes acciones:

- Limitar el número de roles de administrador en un entorno de CA Identity Manager.
- Seguir las directrices para crear reglas de la política (en la página 73).
- Ajustar el almacén de usuarios.
- Ajustar el almacén de políticas, si CA Identity Manager incluye SiteMinder.

Directrices para la creación de reglas de la política

Uno de los factores clave al determinar el rendimiento global de las evaluaciones de la política de roles es la cantidad de tiempo que lleva la evaluación de una única regla de la política. Para mejorar el tiempo de evaluación de una regla de la política, se debe tener en cuenta lo siguiente cuando se crea una política:

- Cuando es posible, se limita el número de objetos de política que crea CA Identity Manager y el número de búsquedas en el almacén de usuarios que realiza mediante la creación de reglas de la política con expresiones complejas.

  Una única regla con una expresión compleja es más eficaz que varias reglas con expresiones simples.

- Cuando es posible, se selecciona el tipo más eficaz y escalable de regla de la política.
- Se activa la opción de evaluación en memoria para reglas de la política.

  La opción de evaluación en memoria reduce de forma significativa el tiempo de evaluación de la política, ya que recupera la información del usuario que se tiene que evaluar del almacén de usuarios y almacena una representación de dicho usuario en memoria. CA Identity Manager utiliza la representación en memoria para comparar los valores del atributo con las reglas de la política.

  Nota: Para obtener más información sobre la opción de evaluación en memoria, consulte la *Guía de configuración*.

- Ajustar el almacén de usuarios.
- Ajustar el almacén de políticas, si la implementación de CA Identity Manager incluye SiteMinder.

Limitación de las búsquedas del almacén de usuarios y objetos de política

Cada regla de una política de rol requiere un conjunto de objetos en el almacén de objetos. Cuando CA Identity Manager evalúa una regla, carga estos objetos y realiza las búsquedas necesarias en el almacén de usuarios.

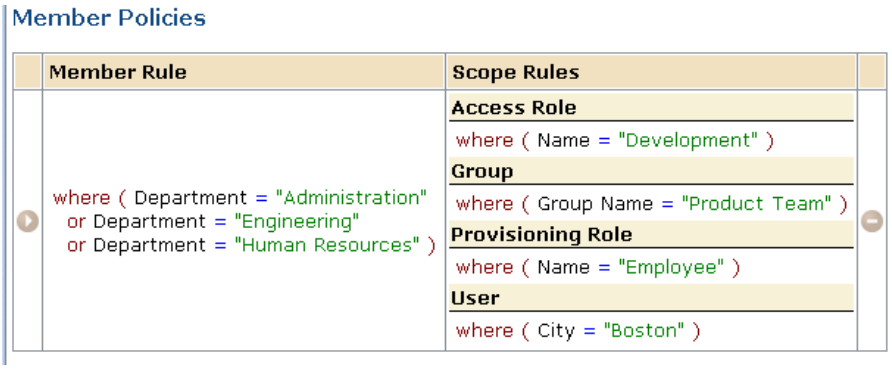
En el ejemplo siguiente se muestra una política de miembros que incluye tres reglas de miembro. Cada regla incluye cuatro reglas de ámbito.

En este ejemplo, CA Identity Manager crea los objetos y realiza las búsquedas en el almacén de usuarios descritas en la siguiente tabla al evaluar y al aplicar la política de miembros.

Regla	Objetos de política	Búsquedas en el almacén de usuarios potenciales
■ Regla de miembros: where (Department = "Administration") ■ Ámbito del usuario: City = "Boston" ■ Ámbito del grupo: Group Name = "Product Team" ■ Ámbito del rol de aprovisionamiento: Name = "Employee" ■ Ámbito de la tarea de acceso: Name = "Development"	5	5 (uno por cada objeto de definición de regla)
■ Regla de miembros: where (Department = "Engineering") ■ Ámbito del usuario: City = "Boston" ■ Ámbito del grupo: Group Name = "Product Team" ■ Ámbito del rol de aprovisionamiento: Name = "Employee" ■ Ámbito de la tarea de acceso: Name = "Development"	5	5
■ Regla de miembros: where (Department = "Human Resources") ■ Ámbito del usuario: City = "Boston" ■ Ámbito del grupo: Group Name = "Product Team" ■ Ámbito del rol de aprovisionamiento: Name = "Employee" ■ Ámbito de la tarea de acceso: Name = "Development"	5	5

En este ejemplo, CA Identity Manager crea 15 objetos y lleva a cabo 15 búsquedas de directorio para determinar los miembros y el ámbito.

Para limitar el número de objetos de política y búsquedas en el almacén de usuarios que realiza CA Identity Manager, se combinan las reglas en expresiones complejas. El siguiente ejemplo especifica las mismas autorizaciones del primer ejemplo como una regla de miembro.



En este ejemplo, CA Identity Manager crea solamente diez objetos de política y realiza solamente cinco búsquedas en el almacén de usuarios.

Regla	Objetos de política	Búsquedas en el almacén de usuarios potenciales
■ Regla de miembro: where (Department = "Administration") O where (Department = "Engineering") O where (Department = "Human Resources") ■ Ámbito del usuario: City = "Boston" ■ Ámbito del grupo: Group Name = "Product Team" ■ Ámbito del rol de aprovisionamiento: Name = "Employee" ■ Ámbito de la tarea de acceso: Name = "Development"	5	5

Selección de tipos de regla de política escalables

Además del número de reglas de política, el tipo de regla de política puede que también afecte al rendimiento. Normalmente, las reglas de política se crean en función de la estructura del almacén de usuarios y de la determinación de las atribuciones. Por ejemplo, se pueden crear reglas de política basadas en la pertenencia a un grupo, organización o atributos del usuario. Sin embargo, cuando hay varias formas de crear reglas de la política, se deben tener en cuenta las directrices de rendimiento de la siguiente tabla antes de decidir qué tipo de regla crear.

Nota: Los tipos de regla de política de la siguiente tabla se clasifican en orden de rendimiento, con el tipo de regla más eficaz en primer lugar.

Tipo de regla de la política	Notas sobre el rendimiento
Organización	■ Mejor rendimiento global. ■ No requiere una búsqueda en directorios LDAP. CA Identity Manager utiliza el nombre destacado del usuario que se evalúa y el nombre destacado de la organización de la regla de la política
Rol	■ CA Identity Manager almacena información del objeto de rol y evaluaciones anteriores en la memoria caché del almacén de objetos. ■ En la mayor parte de los casos, el rendimiento será equivalente a las reglas de la política de la organización.
Atributo de usuario	■ Proporciona el mejor rendimiento de búsqueda en el almacén de usuarios y es al que menos afectan las grandes cantidades de usuarios. ■ Permite activar la evaluación en memoria para obtener un rendimiento significativo.
Miembro del grupo	■ El rendimiento depende del tamaño del grupo y del tipo de almacén de usuarios.

Optimizaciones de tareas

En CA Identity Manager, las tareas que un usuario ve en la Consola de usuario dependen de los privilegios específicos de ese usuario. Para mostrar y ejecutar tareas, CA Identity Manager debe realizar varias evaluaciones de seguridad, que pueden tener un impacto significativo en el rendimiento cuando se apliquen a todos los usuarios de un entorno de CA Identity Manager.

CA Identity Manager realiza evaluaciones de seguridad cuando tienen lugar las siguientes acciones:

- Un usuario inicia sesión en la Consola de usuario.

  En este caso, CA Identity Manager debe evaluar los roles del usuario para determinar a qué tareas puede acceder ese usuario en la Consola de usuario.

- Un usuario invoca una tarea.

  Cuando se invoca una tarea, CA Identity Manager debe determinar qué objetos puede gestionar el usuario con esa tarea.

- Un usuario accede a una ficha de relación.

  Una ficha de relación es cualquier ficha donde un usuario puede ver o gestionar una relación de uno a muchos entre el asunto de la tarea y un conjunto de autorizaciones. Un ejemplo de una ficha de relación es la ficha Roles de administrador, que muestra los roles que tiene un usuario.

- Un usuario agrega objetos en una ficha de relación.

  Por ejemplo, CA Identity Manager realiza comprobaciones de seguridad adicionales cuando un usuario agrega roles adicionales a otro usuario en la ficha Roles de administrador.

Lo siguiente afecta al rendimiento de la tarea:

- Ámbito de la tarea, que determina dónde puede utilizar un administrador una tarea.
- Fichas de relación, que se muestran la relación de un objeto con otros objetos.

Rendimiento y evaluación del ámbito de una tarea

Cuando un administrador utiliza una tarea de administración que implica buscar un objeto gestionado, como un usuario, grupo, organización, tarea o rol, CA Identity Manager evalúa y aplica reglas de ámbito de la tarea. Estas reglas pueden afectar de forma significativa al tiempo que necesita CA Identity Manager para mostrar la lista de objetos que se pueden seleccionar para la tarea.

Nota: A diferencia de las evaluaciones de política de propietario, administrador y miembro, la información acerca de las evaluaciones de regla de ámbito no se almacena en la memoria caché.

El ámbito de la tarea lo determina lo siguiente:

- El tipo de objeto que gestiona la tarea.
- Reglas de ámbito que se aplican al rol de administrador que incluye la tarea. Las reglas de ámbito se definen en las políticas de administración, miembro y propietario.
- Cualquier criterio de búsqueda definido por el usuario.

Por ejemplo, la tarea Modificar usuario, que se incluye en el rol Gestor de usuarios. El rol Gestor de usuarios tiene una política de miembros con una regla de ámbito que permite a los gestores de usuarios gestionar usuarios en la organización Empleados. Un administrador abre la tarea Modificar usuario y especifica los criterios de búsqueda: Apellido empieza por A. En este caso, el ámbito de la tarea Modificar usuario es todos los usuarios de la organización Empleados cuyo apellido empiece por A.

Cómo representa CA Identity Manager las fichas de relación

Una ficha de relación permite a los usuarios ver y gestionar la relación que el asunto de una tarea tiene con un conjunto de autorizaciones. Por ejemplo, la ficha Roles de aprovisionamiento muestra los roles de aprovisionamiento que tiene un usuario.

Para determinar los objetos que aparecen en una ficha de relación, CA Identity Manager realiza numerosas evaluaciones de seguridad, que pueden afectar de forma significativa al rendimiento.

El siguiente ejemplo muestra los pasos que da CA Identity Manager para representar la ficha Roles de aprovisionamiento:

1. Un administrador hace clic en la ficha Roles de aprovisionamiento de la tarea Modificar usuario.
2. CA Identity Manager recupera los roles de aprovisionamiento de los que es miembro el usuario seleccionado.
3. Si la ficha está configurada para permitir la gestión de los administradores de rol, CA Identity Manager hace una segunda llamada para recuperar la lista de roles de aprovisionamiento de los que el usuario seleccionado es administrador.
4. CA Identity Manager evalúa cada rol de aprovisionamiento que tenga el usuario para averiguar si el administrador que inició la tarea puede gestionar los miembros de dicho rol.

   Si el administrador puede gestionar los miembros del rol, CA Identity Manager muestra una casilla de verificación activa en la columna Pertenencia a para ese rol de la lista de roles de la ficha.
5. CA Identity Manager evalúa cada rol de aprovisionamiento que tenga el usuario para averiguar si el administrador que inició la tarea puede gestionar los derechos administrativos de dicho rol.

   Si el administrador puede gestionar los derechos administrativos, CA Identity Manager muestra una casilla de verificación activa en la columna Administrador para ese rol de la lista de roles de la ficha.

   CA Identity Manager debe completar los pasos del 2 al 5 para mostrar los roles de aprovisionamiento que el usuario tiene actualmente. Si el administrador necesita asignar un rol de aprovisionamiento nuevo, se requieren los siguientes pasos adicionales.
6. El administrador hace clic en el botón Agregar para encontrar los roles de aprovisionamiento nuevos que asignar.
7. CA Identity Manager muestra una pantalla de búsqueda que el administrador puede utilizar para buscar el rol que se desea agregar.
8. El administrador introduce un filtro de búsqueda para encontrar el rol para agregar.

9. CA Identity Manager devuelve la lista de roles de aprovisionamiento que cumplen los siguientes criterios:
   - Los roles coinciden con el filtro de búsqueda que introduce el administrador.
   - El administrador puede gestionar la pertenencia a los roles.
   - El usuario está en el ámbito administrativo del administrador de los roles.
   - El usuario no tiene ya los roles de aprovisionamiento.
10. CA Identity Manager repite el paso 9 para determinar los roles en los que el administrador puede gestionar los privilegios administrativos.

Fichas de relación y rendimiento

A causa del número de evaluaciones de seguridad que realiza CA Identity Manager, la representación de una ficha de relación puede afectar de forma significativa al rendimiento. Los factores que determinan el rendimiento varían en función del tipo de ficha.

En el caso de fichas de relación de rol, los siguientes factores pueden afectar al rendimiento:

- Número de roles en los que el asunto de la tarea es un miembro.
- Número de roles en los que el asunto de la tarea es un administrador.
- Número de objetos totales en el sistema que CA Identity Manager requiere para calcular los roles del asunto.
- Número de políticas de miembro o administración por rol.
- Complejidad de las reglas de ámbito de política de miembro o administración.
- La capacidad de mantener autorizaciones almacenadas en memoria caché para los invocadores de tarea para limitar el efecto de la imposición de la seguridad.

Para determinar pertenencia a un grupo y los privilegios administrativos en las fichas de relación del grupo, CA Identity Manager debe buscar en todos los grupos del almacén de usuarios. El rendimiento de estas búsquedas depende de los siguientes factores:

- Número de objetos de grupo en el almacén de usuarios.
- Número de miembros en cualquier grupo.
- Rendimiento de la base de datos o el directorio donde se encuentra el almacén de usuarios.

Rendimiento y procesamiento de la tarea

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 que crean el perfil del usuario, agregan el usuario a un grupo y asignan funciones.

Cuando CA Identity Manager procesa una tarea, procesa cada evento asociado con ésta. Durante el procesamiento de eventos, CA Identity Manager guarda cada evento cuatro veces. Esto permite que CA Identity Manager conserve las acciones en proceso, en caso de que se produzca un cierre del sistema inesperado.

Cuando CA Identity Manager procesa varios eventos al mismo tiempo, los eventos se agregan a una cola. Cuando el primer evento completa la primera etapa de su ciclo de vida, se guarda y, a continuación, se mueve al final de la cola para esperar a que empiece el procesamiento de la segunda etapa. CA Identity Manager a continuación completa la primera etapa de procesamiento del siguiente evento de la cola y ese evento se mueve al final de la cola. El proceso continúa hasta que todos los eventos de la cola hayan completado la primera etapa de procesamiento. A continuación, el primer evento de la cola empieza la segunda fase de procesamiento. Esto continúa hasta que todos los eventos de la cola completen las cuatro etapas de procesamiento.

En condiciones de carga normales, este comportamiento no afecta al rendimiento. Sin embargo, si el sistema está procesando un gran número de tareas y eventos, como durante una carga masiva de una gran cantidad de usuarios, cada evento y tarea deberán esperar más tiempo en la cola y, por lo tanto, necesitará más tiempo para la finalización.

Para evitar que se produzcan incidencias de rendimiento en condiciones de carga, se debe considerar la opción de realizar las siguientes acciones:

- Utilizar la opción de configuración Prioridad de la tarea de la ficha Perfil de una tarea.

  La opción de configuración Prioridad de la tarea permite establecer la prioridad de una tarea como Alta, Media o Baja.

  Las tareas que se deben procesar inmediatamente se deben establecer en la prioridad Alta. Las tareas implicadas en una carga masiva se deben establecer en la prioridad Baja.

  Si hay una prioridad de la tarea establecida, los eventos asociados con la tarea se procesarán con otras tareas que tengan la misma prioridad. Por ejemplo, si la tarea Modificar usuario está establecida en prioridad Alta y un administrador modifica un perfil de usuario, CA Identity Manager procesa esa tarea antes que otras tareas con una prioridad Media o Baja. Si hay otras tareas de prioridad Alta, CA Identity Manager completa la primera etapa de procesamiento para el primer evento de prioridad Alta y, a continuación, mueve ese evento al final de la lista de otros eventos de prioridad Alta.

- Instalar un servidor de CA Identity Manager separado y especializado para identificar operaciones de carga masiva.

Directrices para optimizar las tareas

Las tareas predeterminadas, que CA Identity Manager implementa cuando se crea un entorno de CA Identity Manager, se configuran para admitir una amplia gama de casos de uso de administración. La mayoría de las implementaciones de CA Identity Manager no requieren todas las funcionalidades que se proporcionan en las tareas predeterminadas. Después de haber creado un entorno de CA Identity Manager, estas tareas se modifican para adaptarse a las necesidades de administración específicas.

Los siguientes pasos proporcionan directrices para la modificación de tareas:

- **Crear tareas de gestión de usuarios especializadas**

  Las tareas predeterminadas Crear usuario, Modificar usuario y Ver usuario proporcionan plenas capacidades administrativas. En la mayoría de las implementaciones, solamente un pequeño número de administradores necesitan todas las capacidades disponibles.

  Se pueden crear tareas nuevas que incluyan solamente las capacidades obligatorias. Por ejemplo, si la mayor parte de las tareas de gestión de usuarios implican solamente la gestión de perfiles y grupos, se puede crear una nueva tarea Modificar usuario que incluya solamente las fichas Perfil y Grupo. Se pueden eliminar las fichas Roles de administrador, Roles de acceso y Roles de aprovisionamiento, que se encuentran disponibles en la tarea predeterminada Modificar usuario.

  Las fichas que no se utilicen pueden provocar una sobrecarga importante si se dejan en tareas que se utilicen con frecuencia. Esto ocurre especialmente al utilizar un cliente de servicio Web de ejecución de tareas (TEWS), en el que estas fichas se pueden activar involuntariamente mediante la ficha Clase de Java, que se proporciona con CA Identity Manager.

  Las tareas especializadas que se crean deben coincidir con el modelo de administración delegada (en la página 63) definido para el entorno.

- **Desactivar Gestionar administradores en las fichas de relación**

  De forma predeterminada, todas las fichas de relación proporcionan la capacidad de gestionar derechos administrativos para el objeto que la ficha gestiona, como roles y grupos. En la mayoría de las implementaciones, los administradores no necesitan esta funcionalidad.

Para eliminar la sobrecarga adicional que se produce cuando CA Identity Manager evalúa derechos administrativos, se puede borrar la opción Gestionar administradores en las siguientes fichas, si no se requiere esta funcionalidad:

- Roles de administrador
- Roles de aprovisionamiento
- Roles de acceso
- Grupos

Para permitir que los usuarios gestionen derechos administrativos en fichas específicas, se pueden crear copias de las fichas predeterminadas, activar la opción Gestionar administradores y desactivar la opción Gestionar miembros. Se pueden agregar fichas nuevas a las tareas especializadas, que solamente utilizan los administradores que las necesitan.

- **Activar búsquedas de ámbito en fichas de relación de rol**

  Se puede configurar cada ficha de rol para que incluya búsquedas que permitan a los administradores especificar criterios para los nuevos roles que se asignan a un usuario. Las búsquedas de rol limitan el número de reglas de la política de administración y miembro que CA Identity Manager debe evaluar para determinar qué roles puede asignar un administrador a un usuario.

- **Establecer opciones de sincronización de las tareas**

  Para cada tarea de CA Identity Manager, se puede especificar una opción de sincronización de usuarios, que sincroniza usuarios con políticas de identidad, y una opción de sincronización de cuentas de aprovisionamiento, que sincroniza usuarios con cuentas de aprovisionamiento. Las opciones permiten sincronizar usuarios cuando se completa una tarea o un evento.

  Para eliminar tiempo de evaluación y procesamiento, se puede establecer la sincronización para que tenga lugar cuando una tarea se complete, en lugar de cuando se completen los eventos.

Directrices para optimizaciones de administradores o miembros de grupo

Para mejorar rendimiento de las búsquedas de administradores y miembros de grupo, se debe considerar la posibilidad de realizar lo siguiente:

- Definir atributos conocidos en el archivo de configuración del directorio (directory.xml), que describe la estructura del almacén de usuarios y el contenido para CA Identity Manager.

  Un atributo conocido es un atributo que tiene un significado especial en CA Identity Manager.

  Para mejorar las búsquedas de administradores o miembros de grupo, se definen los siguientes atributos conocidos para el objeto de usuario:

  %MEMBER_OF%

  Identifica un atributo en el objeto de usuario que almacena una lista de grupos de los que el usuario es miembro.

  Cuando se define, este atributo puede evitar que CA Identity Manager busque en todos los miembros de todos los grupos del almacén de usuarios. Las búsquedas de grupos pueden afectar de forma significativa al rendimiento en grupos muy grandes.

  %ADMINISTRATOR_OF%

  Identifica un atributo en el objeto de usuario que almacena una lista de grupos de los que el usuario es administrador.

  Al igual que el atributo %MEMBER_OF%, este atributo conocido puede eliminar búsquedas de grupos largas.

- Especificar el tipo de grupo en el archivo de configuración del directorio

  CA Identity Manager admite tres tipos de grupos: grupos estándares, grupos anidados y grupos dinámicos.

  Cuando se define el objeto de grupo en el archivo de configuración del directorio, se pueden especificar los tipos de grupos con los que es compatible el almacén de usuarios. Si su implementación no es compatible con los grupos anidados o dinámicos, se establece el atributo Tipo de grupo como se muestra a continuación:

  GroupType = NONE

  El valor NONE especifica la compatibilidad con los grupos estándares.

  El valor predeterminado de Tipo de grupo es ALL, lo que puede afectar al rendimiento.

  Nota: Para obtener más información sobre los atributos conocidos y los tipos de grupo en el archivo de configuración del directorio, consulte la *Guía de configuración*.

- Establecer los índices de la memoria caché del directorio de aprovisionamiento para mejorar el rendimiento de GlobalGroup

  Para implementaciones de CA Identity Manager que incluyen un almacén de usuarios combinado y directorio de aprovisionamiento, la pertenencia a GlobalGroup se puede optimizar para la evaluación de regla de la política para roles y políticas de identidad.

  Para activar esta optimización, se indexan los siguientes atributos, que el servidor de aprovisionamiento utiliza para resolver la pertenencia a un grupo, en la memoria caché del directorio de aprovisionamiento:

  eTID

  El atributo de ID de objeto único. Para búsquedas de miembros del grupo, el valor es un usuario específico o grupo involucrado en la búsqueda.

  eTPID

  El ID principal del objeto utilizado al buscar relaciones de pertenencia.

  eTCID

  El ID secundario del objeto utilizado al buscar relaciones de pertenencia.

  Además, se pueden agregar las siguientes entradas de hash:

  eTSuperiorClass

  El tipo del objeto principal en una búsqueda de pertenencia.

  eTSubordinateClass

  El tipo del objeto secundario en una búsqueda de pertenencia.

  Nota: Para obtener más información sobre la memoria caché del directorio de aprovisionamiento, consulte la *Guía de instalación*.

Optimizaciones de la política de identidad

Una *política de identidad* es un conjunto cambios empresariales que se producen cuando un usuario cumple una cierta condición o regla. Estos cambios pueden incluir la asignación o revocación de roles o de pertenencia a grupos y la actualización de atributos de un perfil de usuario.

CA Identity Manager evalúa las políticas de identidad cuando tiene lugar la sincronización de usuarios.

Lo siguiente afecta al rendimiento de la política de identidad:

- La configuración de las políticas de identidad
- La frecuencia con la que se produce la sincronización de usuarios

Cómo sincronizar usuarios y políticas de identidad

Al utilizar políticas de identidad, es importante comprender cómo CA Identity Manager evalúa y aplica las políticas a los usuarios. Si no comprende al detalle el proceso de sincronización de usuarios, es posible que configure conjuntos de políticas de identidad que produzcan resultados inesperados.

El procedimiento siguiente describe cómo CA Identity Manager evalúa y aplica políticas de identidad:

1. El proceso de sincronización de usuarios comienza:
   - **Automáticamente**: puede configurar las tareas de CA Identity Manager para que activen automáticamente la sincronización de usuarios.
   - **Manualmente**: utilice la tarea Sincronizar usuario de la Consola de usuario para sincronizar un usuario.
2. CA Identity Manager determina el conjunto de políticas de identidad que se aplican a un usuario.
3. CA Identity Manager compara el conjunto de políticas de identidad que se aplican a un usuario con la lista de políticas que ya se han aplicado a ese usuario.

   Nota: La lista de políticas que se han aplicado a un usuario se almacena en el atributo conocido %IDENTITY_POLICY% del perfil de usuario. Para obtener información sobre la configuración de este atributo, consulte la *Guía de configuración*.
   - Si una política de identidad está en la lista de políticas aplicables *y* esa política *no* se ha aplicado previamente al usuario, CA Identity Manager la agregará a una lista de asignación.
   - Si una política de identidad está en la lista de políticas aplicables, se ha aplicado previamente al usuario y la opción Aplicar una vez está desactivada para esa política, CA Identity Manager agregará la política a una lista de reasignación.
   - Si una política de identidad no está en la lista de políticas aplicables y ha sido aplicada al usuario, el usuario ya no cumplirá la condición de la política. CA Identity Manager agregará estas políticas a una lista de anulación de asignación.
4. Una vez que CA Identity Manager ha evaluado todas las políticas de un usuario, las aplica en este orden:
   a. Políticas de identidad de la lista de anulación de asignación
   b. Políticas de identidad de la lista de asignación
   c. Políticas de identidad de la lista de reasignación

5. Tras aplicar las políticas de identidad, CA Identity Manager vuelve a evaluarlas para ver si se necesitan otros cambios en función de los cambios que tuvieron lugar en el primer proceso de sincronización (pasos 2-4).

   Esto se hace para asegurar que los cambios realizados al aplicar políticas de identidad no han desencadenado otras políticas de identidad.

6. CA Identity Manager continúa evaluando y aplicando políticas de identidad hasta que el usuario se sincroniza con todas las políticas aplicables, o hasta que CA Identity Manager alcanza el nivel de recursividad máximo. Este nivel se define en la Consola de gestión.

   Por ejemplo, una política de identidad puede cambiar el departamento de un usuario al asignar una función al usuario. El nuevo departamento inicia otra política de identidad. Sin embargo, si el nivel de repetición se establece en 1, el cambio posterior no se realiza hasta que el usuario se vuelve a sincronizar.

   Para obtener más información sobre la configuración del nivel de recursividad, consulte la Ayuda en línea de la consola de gestión.

Diseño de políticas de identidad eficaces

Cuando se crean políticas de identidad, se deben utilizar las siguientes directrices:

- **Limitar el número de objetos de política**

  CA Identity Manager crea objetos en el almacén de objetos que son compatibles con las políticas de identidad. Para reducir el número de objetos del almacén de objetos, se crean políticas de identidad con expresiones complejas.
  Se recomienda un procedimiento similar para las políticas de rol (en la página 74).

- **Limitar las iteraciones del conjunto de políticas de identidad**

  Se puede configurar el nivel de recursión de una política de identidad, que determina el número de veces que CA Identity Manager evalúa y aplica políticas de identidad cuando se sincroniza un usuario. Por ejemplo, una política de identidad puede cambiar el departamento de un usuario al asignar una función al usuario. El nuevo departamento inicia otra política de identidad. Sin embargo, si el nivel de repetición se establece en 1, el cambio posterior no se realiza hasta que el usuario se vuelve a sincronizar.

  Al establecer el nivel de recursión se limita el número de veces que CA Identity Manager debe evaluar las políticas de identidad.

- **Limitar las dependencias entre las reglas de la política de identidad**

  Se puede crear una política de identidad donde la acción de cambio (Acción al Aplicar política o Acción al Eliminar política) de una política se utiliza en la condición de la política de identidad de otra política, como se muestra en la siguiente tabla.

Condición de la política de identidad	Acción al Aplicar política	Acción al Eliminar política
donde (Job Code [Código de Trabajo] = "100")	Hacer miembro de (rol de aprovisionamiento "Gestor de cuentas")	Eliminar miembro de (rol de aprovisionamiento "Gestor de cuentas")
Miembros de (rol de aprovisionamiento "Gestor de cuentas")	Hacer miembro de (grupo "Gestores de cuentas")	Eliminar miembro de (grupo "Gestores de cuentas")

Cuando CA Identity Manager evalúa este tipo de política, debe evaluar y aplicar los cambios al menos dos veces para garantizar que se cumplen ambas condiciones. El nivel de recursión, que se establece para un entorno de CA Identity Manager completo, debe ser mayor que 1 y provoca evaluaciones adicionales para cada conjunto de políticas de identidad.

Limitación de las tareas que activan sincronización de usuarios

Las políticas de identidad se evalúan y se aplican durante el proceso de sincronización de usuarios. Se puede configurar la sincronización automática especificando una de las siguientes opciones de sincronización de usuarios para una tarea:

Al completar la tarea

CA Identity Manager comienza el proceso de sincronización de los usuarios después de que hayan finalizado todos los eventos de una tarea.

En cada evento

CA Identity Manager inicia el proceso de sincronización de usuarios cuando se completa cada evento de la tarea.

Para obtener un mejor rendimiento, se limita el número de tareas que activan la sincronización de usuarios automática.

Se debe considerar la posibilidad de realizar lo siguiente al configurar sincronización de usuarios:

- **Desactivar la sincronización de usuarios para tareas de contraseña**

  En la mayoría de los casos, las contraseñas no se utilizan en las condiciones de la política de identidad.

- **Desactivar la sincronización de usuarios para la tarea Sincronizar usuario**

  Dado que la tarea Sincronizar usuario activa las evaluaciones de política de identidad, CA Identity Manager vuelve a realizar las evaluaciones si la opción de sincronización de usuarios está activada para esta tarea.

- **Crear tareas especializadas**

  Cuando sea posible, se pueden crear tareas que ejecuten modificaciones que activan las condiciones de la política de identidad y activan las sincronizaciones de usuarios para esas tareas solamente.

Optimización de la evaluación de la regla de la política de identidad

Para reducir el tiempo de evaluación de las condiciones de la política de identidad 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 condiciones de la política. Esto limita el número de llamadas que CA Identity Manager hace directamente al almacén de usuarios.

Nota: Para obtener más información sobre la opción de evaluación en memoria, consulte la *Guía de configuración*.

Ajuste de almacén de usuarios

El ajuste de almacén de usuarios implica varios pasos, entre los que se incluyen los siguientes:

- Optimización de la estructura del almacén de usuarios
- Ajuste de almacenes subyacentes
- Implementación del equilibrio de carga y replicación

Estos pasos dependen del tipo de almacén de usuarios que se esté utilizando. Para obtener información de ajustes en estas áreas, consulte la documentación de la base de datos o el directorio que contenga el almacén de usuarios.

Además de las consideraciones de ajuste generales, las siguientes consideraciones de ajuste son específicas de CA Identity Manager:

- **Medición del rendimiento de búsqueda en el almacén de usuarios**

  Para obtener un rendimiento óptimo, las búsquedas de evaluación de la política de CA Identity Manager se deben completar en un intervalo de 10 a 20 milisegundos.

  Para garantizar que CA Identity Manager puede completar de forma constante estas búsquedas en el tiempo recomendado, se debe considerar la posibilidad de realizar pruebas del rendimiento de las búsquedas en distintas condiciones de carga.

  También se puede utilizar esta medida para determinar cuándo un almacén de usuarios alcanza sus límites físicos y se requieren servidores adicionales para el equilibrio de la carga.

- **Indexación de atributos**

  Se indexa cada atributo que se utiliza en una política de rol o política de identidad. Los atributos de indexación pueden proporcionar mejoras de rendimiento significativas.

  Nota: Para obtener información acerca de los atributos de indexación, consulte la documentación del directorio LDAP o la base de datos relacional que contiene el almacén de usuarios.

- **Vínculo LDAP de la memoria caché**

  En CA Identity Manager, todos los vínculos LDAP de los directorios los ejecuta el proxy definido por el usuario en el objeto del directorio de CA Identity Manager. Para cada conexión, se da el mismo vínculo LDAP para el mismo usuario repetidamente.

  Si se está utilizando un directorio LDAP como almacén de usuarios, se debe configurar el directorio para que almacene en la memoria caché los vínculos LDAP (o las sesiones), si el directorio lo admite.

- **Activado de las memorias caché del almacén de usuarios**

  Cuando CA Identity Manager evalúa las decisiones de la política para un usuario, esa información se almacena en una memoria caché de autorización. Cuando la información de la memoria caché caduca, CA Identity Manager vuelve a evaluar todas las políticas para ese usuario.

  Para mejorar el rendimiento de las búsquedas en el almacén de usuarios en las subsiguientes evaluaciones de la regla de la política, se activa el almacén de usuarios para que almacene en la memoria caché los datos que se hayan buscado, si el almacén de usuarios lo admite.

  CA Directory incluye una memoria caché, llamada dxCache, que es una implementación de la base de datos en memoria que puede realizar búsquedas en los datos de la memoria caché.

  Nota: Para obtener más información sobre CA Directory, consulte *CA Directory Administrator Guide*.

Ajuste para componentes de aprovisionamiento

Cuando una implementación de CA Identity Manager incluye aprovisionamiento, se utilizan las siguientes optimizaciones para garantizar el mejor rendimiento:

- Optimizar la conexión entre el servidor de CA Identity Manager y el servidor de aprovisionamiento.

  CA Identity Manager se comunica con el servidor de aprovisionamiento mediante el uso de la API de Java IAM (JIAM). Para mejorar rendimiento de la comunicación, se configura lo siguiente:

  - Agrupación de sesiones de JIAM para varias conexiones al servidor de aprovisionamiento

    Nota: CA recomienda establecer el valor inicial de las sesiones en 8 y el valor máximo de sesiones en 128.

  - Almacenamiento en memoria caché de JIAM para objetos recuperados del servidor de aprovisionamiento

  Nota: Si desea obtener más información sobre los valores de configuración de JIAM, consulte la *Guía de administración*.

- Establecer la sincronización de cuentas para que se produzca al final de una tarea (en la página 82), en lugar de al final de cada evento
- Ajustar el servidor de aprovisionamiento

  Nota: Consulte la *Guía de administración* y la *Guía de instalación* para obtener más información.

Ajuste de los componentes del tiempo de ejecución

Los cambios de negocio en CA Identity Manager se llevan a cabo mediante tareas. Una tarea incluye uno o varios eventos, que representan actividades que CA Identity Manager realiza para completar la tarea. Por ejemplo, una tarea Crear usuario puede incluir CreateUserEvent y AddToGroupEvent.

CA Identity Manager incluye los siguientes componentes, que procesan tareas y eventos en el tiempo de ejecución:

- Bases de datos de CA Identity Manager, que admiten la funcionalidad de CA Identity Manager
- Mensajes del servicio de mensajes Java, que son los responsables de los eventos de procesamiento

Ajuste de las bases de datos de CA Identity Manager

Al ejecutar tareas, CA Identity Manager utiliza las siguientes bases de datos:

- Persistencia de la tarea

  Mantiene información acerca de eventos y tareas de CA Identity Manager de forma gradual. Esto permite que CA Identity Manager restaure el último estado conocido de eventos y tareas en caso de que se produzca un error del sistema.

  Nota: Esta base de datos tiene el impacto más significativo en el rendimiento de CA Identity Manager porque la tarea y sus eventos se guardan y se recuperan de la base de datos durante las transiciones de estado.

- Auditoría

  Proporciona un registro del historial de las operaciones que se producen en un entorno de CA Identity Manager.

- Flujo de trabajo

  Almacena las definiciones del flujo de trabajo, trabajos, scripts y otros datos que necesita el motor del flujo de trabajo.

- Generación de informes

  Almacena los datos de la instantánea, que reflejan el estado actual de los objetos de CA Identity Manager en el momento en que se hace la instantánea.

CA Identity Manager se comunica con cada base de datos mediante una agrupación de conexiones JDBC. Se debe crear y configurar una agrupación de conexiones JDBC en el servidor de aplicaciones que hospeda CA Identity Manager. Cuando se configura la agrupación de conexiones JDBC, se debe tener en cuenta lo siguiente:

- Tener en cuenta el número de tareas simultáneas que se ejecutarán en cualquier momento.
- Tener en cuenta el resto de componentes del tiempo de ejecución cuando se configura el tamaño de la agrupación de conexiones JDBC. Cada componente de tiempo de ejecución funciona conjuntamente con el resto de componentes del tiempo de ejecución.

  Nota: CA recomienda establecer el valor de la agrupación de conexiones inicial en 128.
- Para la base de datos de persistencia de la tarea, el número de conexiones de la base de datos del grupo debe permitir que cada tarea en ejecución recupere y actualice los datos de tarea y evento a lo largo de la vida de la tarea.
- La base de datos de persistencia de la tarea utiliza instrucciones preparadas. Es necesario asegurarse de configurar la memoria caché de la instrucción preparada para la base de datos que se esté utilizando para que almacene los datos de persistencia de la tarea.

  Nota: Consulte la documentación de la base de datos que esté utilizando para la persistencia de la tarea para obtener información sobre la configuración de la memoria caché de la instrucción preparada.

Configuración de JMS

Una tarea de CA Identity Manager incluye eventos, acciones que CA Identity Manager realiza para completar una tarea.

Durante el ciclo de vida de un evento, pasa por los siguientes estados:

- BEGIN
- APPROVED
- EXECUTING
- COMPLETED
- INVALID

Los eventos de flujo de trabajo controlados también pueden tener los estados siguientes:

- PENDING
- REJECTED

CA Identity Manager utiliza el servicio de mensajes Java para controlar estas transiciones de estado.

Cómo controla el servicio de mensajes Java las transiciones de los eventos

CA Identity Manager utiliza el servicio de mensajes Java para controlar las transiciones de estado de un evento. El siguiente procedimiento describe los pasos implicados:

1. Un usuario envía una tarea.
2. La tarea genera uno o varios eventos.
3. Cuando un evento está preparado para el procesamiento, CA Identity Manager establece el estado del evento en BEGIN y el evento persiste en la base de datos de persistencia de la tarea.
4. CA Identity Manager crea un servicio de mensajes Java que contiene el ID del evento y publica ese mensaje en la cola de mensajes de eventos.
5. Al recibir el mensaje, el servicio de mensajes Java invoca una instancia del bean controlado por mensaje de eventos, que es una implementación del controlador de eventos.
6. El controlador de eventos usa el ID del evento del mensaje para recuperar el evento de la base de datos de persistencia de la tarea y ejecuta las acciones del estado actual del evento.
7. Al terminar ese estado, el evento se establecerá en el estado siguiente, persistirá en la base de datos de persistencia de la tarea y se publicará un mensaje del servicio de mensajes Java nuevo para procesar el estado siguiente.

   Este ciclo continúa hasta que el evento haya completado su equipo de estado.

Rendimiento y mensajes del servicio de mensajes Java

Para cualquier evento, hay entre tres y cinco estados que requieren mensajes del servicio de mensajes Java para la transición de estado:

- BEGIN
- PENDING (solamente bajo control de flujo de trabajo)
- APPROVED o REJECTED
- EXECUTING
- COMPLETED o INVALID

Para procesar un evento único, tienen lugar las siguientes acciones:

- De tres a cinco publicaciones en la cola de mensajes de eventos
- De tres a cinco invocaciones del bean controlado por mensaje
- De seis a diez conexiones a la base de datos de persistencia de la tarea (una acción de lectura y una acción de escritura por estado)

Estas acciones pueden afectar a la cantidad de tiempo que tarda CA Identity Manager en procesar una tarea.

Para garantizar el mejor rendimiento durante las transiciones de estado, se ajustan los recursos del servicio de mensajes Java en el servidor de aplicaciones que hospeda CA Identity Manager para que los recursos del servicio de mensajes Java adecuados estén disponibles.

Ajuste de la configuración del servicio de mensajes Java

Los siguientes parámetros de ajuste del servicio de mensajes Java del servidor de aplicaciones definen las agrupaciones de instancias de bean controlado por mensaje y conexiones de cola.

- **Ajuste del servicio de mensajes Java de WebSphere**

  WebSphere proporciona a las fábricas de conexiones de cola dos parámetros que se pueden configurar para mejorar el rendimiento. Para establecer las siguientes propiedades se utiliza la Consola de administración de WebSphere:

  - En Recursos, se buscan las siguientes fábricas de conexiones de cola: iam-im-neteQCF e iam-im-wpConnectionFactory.
  - Para cada uno, se editan las propiedades de la agrupación de conexiones para establecer el número máximo de conexiones en 128.

- **Ajuste de WebLogic**

  En los servidores de aplicaciones de WebLogic, las fábricas de conexiones de cola obtienen subprocesos de gestión de las conexiones del grupo de subprocesos del servicio de mensajes Java del servidor o el grupo de ejecución predeterminado, en función del tamaño del grupo de subprocesos del servicio de mensajes Java. Si el tamaño de la agrupación de subprocesos del servicio de mensajes Java es 0, WebLogic utilizará los subprocesos en el grupo de ejecución.

  Se recomienda que se establezca el número de subprocesos del grupo de subprocesos del servicio de mensajes Java igual al tamaño máximo del grupo de bean para el bean controlado por mensaje de evento de CA Identity Manager, que está establecido en 128 de forma predeterminada.

  Se utiliza la consola del servidor de WebLogic para establecer el tamaño del grupo de subprocesos del servicio de mensajes Java en las propiedades de los servicios del servicio de mensajes Java para el dominio y el servidor donde CA Identity Manager esté instalado.

El tamaño del grupo de bean controlado por mensaje de evento de CA Identity Manager se establece modificando la opción de configuración max-beans-in-free-pool que se encuentra en el archivo descriptor en la siguiente ubicación:

WebLogic_home\domain\applications\iam_im.ear\identityminder_ejb.jar\META-INF\weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>
                <initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>
            <destination-jndi-name>com.netegrity.ims.msg.queue</destination-
jndi-name>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **Ajuste de JBoss**

  En los servidores de aplicaciones de JBoss, las fábricas de conexiones de cola obtienen subprocesos de gestión de las conexiones de la fábrica de sesión del grupo del servicio de mensajes Java estándar del servidor. De forma predeterminada, el número máximo de subprocesos está establecido en 15.

  Se recomienda que se establezca este valor de modo que coincida con el valor de tamaño máximo del contenedor de bean de mensaje estándar.

  La fábrica de sección de la agrupación de sesiones del servicio de mensajes Java está establecida en el elemento MaximumSize de JMSContainerInvoker en el siguiente archivo:

  jboss_home\server\default\conf\standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         ….
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            ….
         </proxy-factory-config>
     </invoker-proxy-binding>
```

El tamaño de la agrupación de bean controlado por mensaje de evento de CA Identity Manager se establece modificando el valor de tamaño máximo en el siguiente archivo descriptor:

jboss_home\server\default\conf\standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>
         <invoker-proxy-binding-name>message-driven-bean</invoker-proxy-
binding-name>
        ……
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

Ajuste del rendimiento de JBoss 5

En una instalación predeterminada de JBoss 5, el explorador de la implementación en caliente de JBoss se ejecuta cada 5 segundos, lo que afecta al rendimiento de JBoss. Se puede desactivar esta función, si no es necesaria, o se puede cambiar su frecuencia de ejecución.

Para desactivar o modificar la implementación en caliente

1. Se edita el archivo hdscanner-jboss-beans.xml en esta ubicación:

   Nodo único: *jboss_home*/server/default/deploy

   Clúster: *jboss_home*/server/all/deploy

2. Para desactivar esta función, se agrega la siguiente línea dentro del bean de HDScanner:
   `<attribute name="ScanEnabled">False</attribute>`

3. Para modificar la frecuencia de exploración, se aumenta el valor del atributo scanPeriod por encima de 5000 (milisegundos).

Nota: Para obtener más información, consulte este vínculo: http://community.jboss.org/wiki/JBossASTuningSlimming.

Para abordar errores de memoria insuficiente

Pueden encontrarse excepciones de memoria insuficiente si el tamaño de la memoria dinámica de Java es demasiado pequeño. Se recomienda un tamaño inicial de 1024.

Capítulo 7: Creación de un plan de recuperación de desastres

Esta sección contiene los siguientes temas:

Pérdida de servicio de un desastre

En caso de desastre, los usuarios pueden perder el acceso a los servicios que son esenciales para sus trabajos. Como resultado, estos usuarios no podrían proporcionar servicios a otros usuarios.

La urgencia en restaurar el acceso a los servicios depende del uso real de CA Identity Manager. En algunas organizaciones, los usuarios requieren un acceso ininterrumpido a los servicios que proporciona CA Identity Manager, mientras que otros usuarios requieren la restauración del sistema en un día. En cualquiera de los dos casos, se recomienda estar preparado para proteger la implementación de CA Identity Manager de un evento que cause una pérdida completa o parcial de los sistemas.

Al configurar una arquitectura redundante para CA Identity Manager, se puede garantizar que los usuarios disfrutarán de una alta disponibilidad de los servicios. Cuando se produce un error con un componente principal, el componente alternativo continúa ofreciendo el mismo servicio. Además, se puede realizar una copia de seguridad rutinaria de sistemas y software críticos, para que se pueda restaurar cualquier sistema o datos que se pierdan completamente.

Este documento proporciona directrices de planificación generales para estos escenarios. Se recomienda utilizar estas directrices para desarrollar procedimientos de recuperación de desastres específicos que aborden los requisitos de la organización.

Cómo planificar la recuperación de desastres

Para desarrollar un plan de recuperación de desastres eficaz, se llevan a cabo a las fases siguientes, que se detallan en este capítulo.

✓	Fase
	1. Definición de requisitos de recuperación de desastres (en la página 101) En función de las necesidades de la organización, se identifican qué tipos de desastre se deben prever y la rapidez con la que sería necesario restaurar los servicios.
	2. Diseño de una arquitectura redundante (en la página 102) Según los requisitos, se diseña una arquitectura con componentes redundantes en una ubicación remota.
	3. Desarrollo de planificaciones de copia de seguridad (en la página 104) Para proteger la instalación, se desarrollan planes para realizar copias de seguridad de componentes.
	4. Desarrollo de procedimientos de restauración (en la página 105) Se desarrollan procedimientos para restaurar componentes perdidos.
	5. Documentación del plan de recuperación (en la página 109) Se documentan los planes para recuperar CA Identity Manager de un desastre.
	6. Prueba del plan de recuperación (en la página 109) En función de los procedimientos de recuperación de desastres, se verifica que se puede reinstaurar la implementación de CA Identity Manager tal como existía antes del evento.
	7. Formación de recuperación de desastres (en la página 111) Se completa el esfuerzo al asegurarse de que las personas responsables de recuperar los sistemas de un desastre están preparados para ello.

Definición de requisitos de recuperación de desastres

Las siguientes son algunas directrices generales que se deben tener en cuenta para definir requisitos para un plan de recuperación de desastres:

1. Reúna a un equipo con el conocimiento siguiente:
   - Conocimiento de la arquitectura y los sistemas que son compatibles con CA Identity Manager.
   - Conocimiento de cómo realizar la copia de seguridad de las bases de datos relacionales y los almacenes de usuario LDAP que utiliza CA Identity Manager.
2. Identifique escenarios de desastre potenciales que se deban abarcar, incluida la pérdida parcial o total de los sistemas de uno o varios sitios.
3. Enumere los sistemas críticos para que estén disponibles para ser compatibles con la instalación.
4. Defina el tiempo de inactividad máximo aceptable para cada uno de estos sistemas.

   Por ejemplo, la restauración de los sistemas que son compatibles con un servidor alternativo puede tener menor prioridad.

Diseño de una arquitectura redundante

Para protegerse frente a errores de un componente crítico, se deben tener en cuenta las siguientes acciones de protección que utilizan componentes alternativos (servidores y directorios) y bases de datos redundantes en ubicaciones remotas.

Se debe configurar la redundancia para CA Identity Manager mediante la *Guía de instalación* .Se incluyen los siguientes componentes:

- Nodos de servidor de aplicaciones de CA Identity Manager redundantes como parte de un clúster.
- Un clúster de servidor de políticas proporciona conmutación por error (si se está utilizando CA SiteMinder para proteger CA Identity Manager).
- Servidores de aprovisionamiento alternativos, directorios de aprovisionamiento y servidores de conectores. Si un componente principal se pierde, el sistema cambia al componente alternativo.

Se debe configurar la redundancia para bases de datos incluidas las siguientes:

- Cualquiera de las bases de datos de tiempo de ejecución que formen parte de CA Identity Manager, como el flujo de trabajo o la base de datos de auditoría.

  Consulte la documentación facilitada con ORACLE o Microsoft SQL Server.
- La base de datos de Business Objects si se está usando el servidor de informes.

  Consulte la documentación de Business Objects Enterprise (versión 2 y versión 2 SP4) en el sitio web de documentación de SAP.

Servidores de CA Identity Manager alternativos

Al proporcionar nodos de servidor de aplicaciones redundantes para el servidor de CA Identity Manager se otorgan beneficios de escalabilidad y rendimiento, y recuperación de desastres si se produce un error en los servidores individuales. El método más común de proporcionar conmutación por error para un servidor de aplicaciones es la creación de un clúster. Los procedimientos para crear el clúster se abarcan en la sección sobre clústers de la *Guía de instalación*.

Nota: Para CA Identity Manager r12.0 y versiones posteriores, un clúster de servidor de aplicaciones es el único método válido para aplicar una implementación de varios nodos. Los entornos de CA Identity Manager requieren la arquitectura de clústers J2EE estándar del sector, que utiliza colas de JMS para la red troncal. Como resultado, el único método válido de utilizar varios nodos en una configuración de CA Identity Manager es un clúster de servidor de aplicaciones.

Para obtener más detalles sobre este cambio, consulte TechDoc 545594.

Componentes de aprovisionamiento alternativos

Varios componentes de aprovisionamiento tienen la opción de disponer de un componente alternativo para proporcionar una disponibilidad alta. El componente alternativo debería estar en un sitio remoto para que la protección sea superior.

Consulte el capítulo High Availability Provisioning de la *Guía de instalación* para obtener detalles específicos de la configuración de directorios y servidores alternativos.

Directorios de aprovisionamiento de varios sitios

Se pueden crear directorios de aprovisionamiento principales y alternativos con los directorios alternativos en una ubicación remota. CA Directory recomienda que se instalen tres directorios de aprovisionamiento: uno principal y dos alternativos.

Servidores de aprovisionamiento de varios sitios

Para protegerse contra errores del servidor de aprovisionamiento principal, se puede configurar un servidor de aprovisionamiento alternativo. La diferencia entre los servidores de aprovisionamiento principales y alternativos es que la instalación del servidor primario rellena las entradas de contenedor del directorio de aprovisionamiento. Además, la desinstalación de un servidor primario elimina esas entradas. Aparte de instalación y desinstalación, el servidor principal y los alternativos funcionan de la misma manera.

Servidores de conectores de varios sitios

Para el servidor de conector de C++ o Java, se pueden configurar varios servidores de conectores para servir al mismo punto final o tipo de punto final.

Por cada servidor de conectores que se configure, se debe configurar un servidor de conectores alternativo en una ubicación remota para gestionar los mismos puntos finales. Si se produce un error con el servidor de conectores, el servidor alternativo gestiona inmediatamente la comunicación con los puntos finales.

Bases de datos redundantes

Los tipos de software de base de datos compatibles, Microsoft SQL Server y Oracle, otorgan la capacidad de proporcionar bases de datos redundantes. Si se produce un error con la base de datos principal, la base de datos redundante estará disponible inmediatamente. La base de datos redundante debería estar en un sitio remoto en caso de que el sitio entero se vea afectado.

Desarrollo de planificaciones de copia de seguridad

Para protegerse contra la pérdida de alguno o todos los sistemas, se debe utilizar almacenamiento fuera del sitio para todos los datos de los que se realice copia de seguridad y una programación de la copia de seguridad que cumpla los requisitos de tiempo de inactividad máximo. Los procedimientos de copia de seguridad y restauración utilizan aplicaciones diferentes, así que se deben coordinar para la recuperación del sistema de CA Identity Manager en conjunto.

Se deben incluir los componentes siguientes en sus planificaciones de copia de seguridad:

Componente	Descripción	Método de copia de seguridad
Almacén de usuarios de CA Identity Manager	Un directorio de usuarios LDAP o una base de datos relacional que contenga los registros de usuarios de CA Identity Manager.	Consulte la documentación proporcionada con su base de datos o software de LDAP.
Bases de datos de CA Identity Manager	Bases de datos de persistencia de la tarea, flujo de trabajo, auditoría, almacén de objetos, generación de informes y archivado de persistencia de la tarea. El flujo de trabajo, persistencia de la tarea y auditoría tienen la frecuencia más alta de cambio y se deberían programar copias de seguridad en consecuencia.	Consulte la documentación proporcionada con el software de su base de datos.
Almacén de políticas de SiteMinder	Un directorio de usuarios LDAP o una base de datos relacional con objetos para el servidor de políticas SiteMinder, si se está utilizando SiteMinder.	Consulte la documentación proporcionada con su base de datos o software de LDAP.
Directorio de aprovisionamiento	Un directorio de usuarios LDAP que contiene los registros para usuarios de aprovisionamiento y objetos de aprovisionamiento.	Consulte la documentación de CA Directory.
Almacenes persistentes del servicio de mensajes Java del servidor de aplicaciones	Los almacenes que se utilizan para contener el procesamiento de mensajes de eventos de la tarea de CA Identity Manager.	Consulte la documentación de Servidor de aplicación.

Componente	Descripción	Método de copia de seguridad
Bases de datos de informes	Base de datos de instantáneas Base de datos de Business Objects	Consulte la documentación proporcionada con el software de su base de datos.
Informes personalizados	Informes personalizados y archivos XML relacionados	Consulte la documentación de Business Objects Enterprise (versión 2 y versión 2 SP4) en el sitio web de documentación de SAP.

Los componentes siguientes se incluyen en sus planificaciones de copia de seguridad utilizando un programa de copia de seguridad del sistema de archivos:

Componente	Descripción
Componentes del servidor Web	Configuración de los componentes del servidor Web implementados, como complementos del servidor de aplicaciones y agentes Web de SiteMinder. Se requiere un cliente de servidor Web si se está utilizando equilibrio de carga o si se está utilizando SiteMinder para proteger el acceso a la Consola de usuario.
Archivos de datos XML	Todos los archivos del entorno y el directorio de CA Identity Manager que se utilicen para crear, mantener y archivar objetos del almacén de objetos de CA Identity Manager.
Componentes de personalización de CA Identity Manager	Los archivos encontrados en las siguientes carpetas de iam_im.ear implementadas: ■ Config ■ User_console.war WEB-INF\web.xml
Scripts y programas	Scripts de TEWS, programas, salidas de programa.
Componentes de Connector Xpress	Conectores personalizados Archivos de proyecto de Connector Xpress
Documentación sobre recuperación de desastres	Después de crear una documentación personalizada para la recuperación de desastres, se debe realizar una copia de seguridad con regularidad por si las instrucciones cambian.

Desarrollo de procedimientos de restauración

Los procedimientos de restauración dependen del método de copia de seguridad. El proceso de recuperación para un sistema en el que se ha producido un error depende de las circunstancias. Sin embargo, en muchos casos, el método de restauración es reinstalar el software. Consulte el capítulo High Availability Provisioning de la *Guía de instalación* para obtener más detalles.

Restauración del almacén de usuarios de CA Identity Manager

Para restaurar el almacén de usuarios de CA Identity Manager, consulte la documentación facilitada con la base de datos o el software de LDAP. Verifique que el almacén de datos de la copia de seguridad está intacto incluido el acceso a todos los almacenes de usuarios.

Restauración de las bases de datos de CA Identity Manager

Para restaurar las bases de datos de CA Identity Manager, consulte la documentación facilitada con la base de datos. Verifique que el almacén de datos de la copia de seguridad está intacto incluido el acceso a todas las bases de datos.

Restauración del almacén de políticas de SiteMinder

Para restaurar el almacén de políticas de SiteMinder, consulte la documentación facilitada con la base de datos o el software de LDAP. Verifique que el almacén de datos de la copia de seguridad está intacto incluido el acceso a todos los almacenes de usuarios.

Restauración del servidor de CA Identity Manager

Si se pierde un nodo de clúster de un servidor de CA Identity Manager, se deben realizar los siguientes pasos:

1. Utilice el procedimiento documentado estándar para agregar un nodo.

   Consulte el capítulo de la *Guía de instalación* sobre la instalación del clúster.

2. Actualice la conexión al servidor de aprovisionamiento.

   Consulte la sección sobre conmutación por error de aprovisionamiento en el capítulo High Availability de la *Guía de instalación* para obtener más detalles.

Restauración de un directorio y un servidor de aprovisionamiento

Se puede restaurar un servidor de aprovisionamiento perdido instalando un servidor alternativo. Si se ha producido un error en todos los sistemas, se deben restaurar los datos perdidos durante el desastre.

Siga estos pasos:

1. Copie algunos archivos de esquema personalizados en directorio config\schema de CA Directory.
2. Instale el directorio de aprovisionamiento nuevo.

   Los almacenes de datos estarán vacíos.
3. Restaure los datos de la ubicación de la copia de seguridad.
4. Utilice el instalador de servidor de aprovisionamiento, proporcionando los detalles para el directorio de aprovisionamiento recién restaurado.

   La información del dominio ya debe encontrarse ahí.
5. Restaure cualquier conector personalizado y archivos de configuración de copia de seguridad.

Nota: Para obtener más información, consulte la documentación de CA Directory.

Restauración de los servidores de conectores

Si se pierde un servidor de conectores, realice los siguientes pasos:

1. Utilice el instalador del servidor de conectores para instalar un servidor de conectores nuevo.

   Regístrelo con el servidor de aprovisionamiento durante la instalación.
2. Elimine el registro del servidor de conectores perdido mediante csfconfig o Connector Xpress.

Restauración de un servidor de informes

Si se pierde el servidor de informes, consulte la documentación de Business Objects para los procedimientos que se aplican. En el sitio web de documentación de SAP, busque la documentación de Business Objects Enterprise (versión 2 y versión 2 SP4).

Restauración de las tareas de administración

Si había una tarea de administración en proceso en el momento del desastre, se puede recuperar en las condiciones siguientes.

- Cualquier tarea de administración que estuviera en estado Pendiente esperando en las aprobaciones continuará estando disponible si se conservan los almacenes que se utilizan para mantener la información del estado. Los almacenes incluyen la base de datos de persistencia de la tarea, el almacén del servicio de mensajes Java que conserva los mensajes del servicio de mensajes Java de tarea y evento, y la base de datos de flujo de trabajo.
- Las tareas en estado En proceso (cualquier estado distinto de Pendiente) están sujetas a condiciones adicionales.

  Una tarea en este estado requiere la publicación de un nuevo mensaje del servicio de mensajes Java en la cola de mensajes de eventos de CA Identity Manager para continuar siendo procesada. Las interrupciones que se produzcan antes de que ese evento se publique en la cola evitarán que la tarea continúe hacia la recuperación.

  En esta situación, existen dos opciones para recuperar la tarea:

  - Si la tarea está presente en la tarea Ver tareas enviadas en el estado en que se ha producido un error, vaya a la página de detalles de la tarea y utilizar la opción correspondiente para reenviar la tarea.
  - Envíe una tarea nueva con los mismos cambios.

Documentación del plan de recuperación

Según las directrices de este capítulo, se recomienda el desarrollo de una documentación sobre recuperación de desastres específica que se aplique a su organización.

Puede utilizar el siguiente enfoque:

1. Identifique los nombres y las ubicaciones de los sistemas de su arquitectura y los componentes alternativos de cada sistema.

   Para cada uno, haga una lista del software instalado, como el JDK específico instalado, la versión de corrección de un servidor de aplicaciones y la cantidad de memoria instalada. Estos detalles se necesitan para cualquier sistema que se decida que es necesario reconstruir completamente.

2. Escriba procedimientos para recuperar cada componente o para reconstruir un sistema completo, si es necesario.
3. Identifique un método para encontrar o restablecer los nombres del usuario y las contraseñas de sistemas e interfaces de usuario de CA Identity Manager si solamente las conocen una o dos personas.
4. Para evitar que se pierda la documentación sobre recuperación de desastres, cree una copia de seguridad se que almacena en una ubicación conocida fuera del sitio.

Prueba del plan de recuperación

Para ayudar garantizar una recuperación correcta de un desastre, se puede programar un desastre simulado, donde ciertos sistemas se vuelvan no disponibles. Tenga en cuenta estas pruebas, que se describen en las secciones siguientes.

1. Prueba del proceso de conmutación por error.
2. Prueba de la restauración de los sistemas.

Prueba del proceso de conmutación por error

Todos los servidores o los directorios deben tener un servidor o directorio alternativo en un sitio remoto, incluidos estos componentes:

- Servidor de CA Identity Manager
- Servidor de aprovisionamiento
- Directorios de aprovisionamiento
- Servidores de conectores Java y C++
- Servidor de informes
- Servidor de políticas

Se debe detener manualmente cada componente y verificar que todas las operaciones continúan funcionando, usando el componente alternativo. Por ejemplo, se podría realizar la prueba siguiente del servidor de aprovisionamiento:

1. En un sistema con el servidor de aprovisionamiento principal, detenga los servicios del servicio de aprovisionamiento del cuadro de diálogo de servicios de Windows.

   El servidor de aprovisionamiento principal se detiene.

2. En la Consola de usuario, realice las siguientes acciones:

   a. Asigne un rol de aprovisionamiento a un usuario.

   b. Verifique que las cuentas de puntos finales se crean para ese usuario.

      Las cuentas que se crean dependen del servidor de aprovisionamiento alternativo que gestiona la comunicación con el servidor de CA Identity Manager.

Este procedimiento es un ejemplo de una prueba. Para cada componente que se detenga, desarrolle pruebas similares para verificar que el componente alternativo está en uso.

Prueba de los procedimientos de restauración

Según la documentación sobre recuperación de desastres pertinente, realice una prueba de cada componente crítico para confirmar que se puede restaurar el sistema perdido.

Formación de recuperación de desastres

Cuando los procedimientos de recuperación se consideren fiables, se debe ayuda garantizar que las personas que deben implementarla son capaces de ello. Su organización puede requerir otros pasos, sin embargo, las siguientes son algunas directrices generales:

1. Anuncie la ubicación de la documentación de recuperación.
2. Realice un ensayo de la formación.
3. Incorpore comentarios de la formación para ayudar a garantizar que los procedimientos de recuperación de desastres finales son suficientes.

Nota: También puede elegir utilizar la formación como una oportunidad de asignar coordinadores de recuperación, incluida una persona como el coordinador de recuperación y una segunda persona como el coordinador alternativo. A estas personas se les debería encargar encontrarse en una ubicación documentada para empezar el plan de recuperación de desastres.