Informatica

Informatica® Multidomain MDM
10.4

Guía de implementación del director de datos

Informatica Multidomain MDM Guía de implementación del director de datos
10.4
Marzo 2020

Fecha de publicación: 2020-06-05

Tabla de contenido

Prefacio

Utilice la *Guía de implementación de Multidomain MDM Data Director* de Informatica® para saber cómo configurar una aplicación para Informatica Data Director que utilice el modelo de áreas de asunto. Obtenga más información sobre las áreas de asunto, los procesos de implementación de las aplicaciones y las configuraciones manuales de Data Director. Para ver información sobre cómo configurar una aplicación para Data Director con entidades de negocio, consulte la *Guía de la herramienta de aprovisionamiento de Multidomain MDM*.

Recursos de Informatica

Informatica proporciona una variedad de recursos de productos a través de Informatica Network y otros portales en línea. Use los recursos para sacar el mayor provecho de los productos y las soluciones de Informatica y aprender de otros expertos en la materia y usuarios de Informatica.

Informatica Network

Informatica Network es la puerta de entrada a muchos recursos, entre ellos, la base de conocimientos de Informatica y el servicio internacional de atención al cliente de Informatica. Para entrar en Informatica Network, visite https://network.informatica.com.

Como miembro de Informatica Network, tiene las siguientes opciones:

- Buscar recursos de productos en la base de conocimientos
- Ver la información de disponibilidad del producto
- Crear y revisar casos de soporte
- Buscar su red de grupos de usuarios de Informatica locales y colaborar con sus pares

Base de conocimiento de Informatica

Use la base de conocimientos de Informatica para encontrar recursos de productos como artículos prácticos, procedimientos recomendados, tutoriales de video y respuestas a preguntas frecuentes.

Para buscar en la base de conocimiento, visite https://search.informatica.com. Si tiene preguntas, comentarios o ideas relacionadas con la base de conocimiento de Informatica, póngase en contacto con el equipo de la base de conocimiento de Informatica en KB_Feedback@informatica.com.

Documentación de Informatica

Use el portal de documentación de Informatica para recorrer una extensa biblioteca de documentación para las versiones de productos actuales y recientes. Para recorrer el portal de documentación, visite https://docs.informatica.com.

Si tiene preguntas, comentarios o ideas acerca de la documentación de los productos, póngase en contacto con el equipo de la documentación de Informatica en infa_documentation@informatica.com.

Matrices de disponibilidad de producto de Informatica

Las matrices de disponibilidad de producto (PAM, Product Availability Matrixes) indican las versiones de sistemas operativos, bases de datos y otros tipos de orígenes y destinos de datos admitidos por la versión de un producto. Puede recorrer las PAM de Informatica en https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity es una colección de consejos y procedimientos recomendados desarrollados por los servicios profesionales de Informatica que se basan en experiencias reales de cientos de proyectos de administración de datos. Informatica Velocity represente el conocimiento colectivo de los consultores de Informatica que trabajan con organizaciones de todo el mundo para planificar, desarrollar, implementar y dar mantenimiento a soluciones de administración de datos exitosas.

Puede encontrar recursos de Informatica Velocity en http://velocity.informatica.com. Si tiene alguna pregunta, comentario o idea acerca de Informatica Velocity, póngase en contacto con los servicios profesionales de Informatica en ips@informatica.com.

Catálogo de soluciones de Informatica

El catálogo de soluciones de Informatica es un foro donde puede buscar soluciones que aumenten, amplíen o mejoren sus implementaciones de Informatica. Aproveche cualquiera de los cientos de soluciones de socios y desarrolladores de Informatica que se encuentran en el catálogo para mejorar su productividad y acelerar la implementación de los proyectos. Puede encontrar el catálogo de soluciones de Informatica en https://marketplace.informatica.com.

Servicio internacional de atención al cliente de Informatica

Puede ponerse en contacto con un centro de atención global por teléfono o a través del Informatica Network.

Para encontrar el número de teléfono local del servicio internacional de atención al cliente de Informatica, visite el sitio web de Informatica en el siguiente vínculo: https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

Para encontrar recursos de soporte en línea en Informatica Network, visite https://network.informatica.com y seleccione la opción eSupport.

CAPÍTULO 1

Introducción

Este capítulo incluye los siguientes temas:

Resumen

Atención: Data Director con áreas de asunto ya no se admite. Informatica recomienda migrar a Data Director con entidades de negocio.

Esta guía describe cómo crear una aplicación para Data Director con áreas de asunto. Para ver instrucciones sobre cómo crear una aplicación para Data Director con entidades de negocio, consulte la *Guía de la herramienta de aprovisionamiento de Multidomain MDM* en su lugar.

Data Director es una aplicación de control de datos que proporciona soluciones de datos principales que son eficaces para todas las partes implicadas en la ecuación de control de datos, como:

- Usuarios profesionales
- Gestores de datos
- Administradores de TI

Data Director permite a los usuarios profesionales realizar con eficacia las funciones descritas en la siguiente tabla:

Funcionalidad	Descripción
Crear	Cree datos principales de alta calidad personalmente o en equipo en toda su empresa.
Administrar	Administre duplicados, resuelva coincidencias, apruebe y administre actualizaciones de sus datos principales, y cree y asigne tareas a usuarios de datos.
Consumir	Busque todos los datos principales desde una ubicación central y vea los detalles de los datos principales.
Supervisar	Realice un seguimiento del linaje y el historial, realice auditorías para verificar la conformidad de los datos principales y personalice su panel.

Requisitos previos

Este documento requiere conocer adecuadamente la arquitectura de Multidomain MDM y tener un buen conocimiento de todos los componentes del entorno que utilizan las aplicaciones de Data Director.

Para obtener más información, consulte la documentación del producto Multidomain MDM.

CAPÍTULO 2

Conceptos de IDD

Este capítulo incluye los siguientes temas:

Aplicación IDD

La aplicación IDD es la unidad principal de configuración e implementación para las implementaciones de IDD. Una aplicación IDD es lo que ven los usuarios profesionales al iniciar IDD e iniciar sesión.

Administrador de configuración de IDD

El Administrador de configuración de IDD es una utilidad basada en web que se utiliza para añadir, modificar y administrar aplicaciones IDD.

Temas relacionados

- "Administrador de configuración de IDD" en la página 40

Archivos de configuración de IDD

Una aplicación IDD se compone de un conjunto de archivos de configuración: un archivo de configuración de IDD (XML), paquetes de recursos, paquetes de mensajes de internacionalización, ayuda en línea y otros archivos auxiliares. Puede cargar o modificar aplicaciones IDD en el Administrador de configuración de IDD o exportarlas y editarlas manualmente.

Temas relacionados

- "Componentes de aplicación" en la página 116

Herramienta de aprovisionamiento

Puede utilizar la herramienta de aprovisionamiento para definir modelos de entidad de negocio, tareas y transformaciones, y para diseñar la interfaz de usuario de Data Director

Informatica Data Director requiere una configuración de entidad de negocio basada en el marco de Entity 360, como pueda ser el administrador de tareas y las vistas de registros. Informatica Data Director también requiere una configuración de área de asunto para características como la vista Jerarquía, la vista Referencia cruzada y la página Comparación de fusión de coincidencia.

En esta guía se describe la configuración de área de asunto para Informatica Data Director. Para obtener información sobre la configuración del marco de Entity 360 y la configuración de le entidad de negocio, consulte la *Guía de la herramienta de aprovisionamiento de Multidomain MDM*.

Áreas de asunto y grupos de área de asunto

En una aplicación IDD, los datos se organizan en áreas de asunto y se agregan a grupos de área de asunto.

Áreas de asunto

El *área de asunto* es un concepto de organización básico para una aplicación de Informatica Data Director.

Otros términos o conceptos que están relacionados o son similares al área de asunto son: objeto de negocio y entidad jerárquica. Informatica Data Director usa la definición de área de asunto para determinar cómo tratar cada relación de clave externa en un almacén de referencias operativas (ORS).

El almacén del concentrador mantiene metadatos detallados sobre las tablas y las relaciones definidas en un ORS. Estos metadatos incluyen relaciones entre las tablas de objetos base que pueden representar:

- Referencias a tablas de búsqueda
- Enlaces entre datos principales y datos secundarios relacionados
- Enlaces asociativos entre tablas, que no representan una relación de propiedad.

El almacén del concentrador proporciona algunos de los metadatos que permiten a Informatica Data Director comprender cómo deben tratarse las relaciones. Por ejemplo, el indicador de búsqueda de objetos base informa a Informatica Data Director cuándo debe tratar una tabla relacionada como una búsqueda con una lista desplegable rellenada previamente que los usuarios ven en una aplicación de Informatica Data Director.

Para otras relaciones, una aplicación de Informatica Data Director podría requerir información adicional para comprender correctamente las relaciones (si se deben interpretar como relaciones entre tablas en un área de asunto o como relaciones entre áreas de asunto). El administrador de configuración de Informatica Data Director se utiliza para especificar esta información de relación adicional para las aplicaciones de Informatica Data Director. No puede usar alias para un área de asunto que se base en una relación del administrador de jerarquía.

Un área de asunto representa un conjunto de datos que se debe tratar como una unidad desde una perspectiva empresarial. Un área de asunto tiene:

- Un único registro raíz de un objeto base
- Varios registros secundarios y registros secundarios de segundo nivel (mediante relaciones de uno a muchos y muchos a muchos).

Grupos de área de asunto

Un *grupo de área de asunto* es un conjunto de una o más áreas de asunto que tienen el mismo objeto base en su raíz (también llamado *objeto principal*).

Por ejemplo, un ORS que use un modelo de entidad (un único objeto base que representa a distintos tipos de entidades) tendrá un grupo de área de asunto con varias áreas de asunto.

Nota: Un objeto base solo puede estar asociado a un grupo de área de asunto.

Relaciones en áreas de asunto

En una aplicación IDD, las relaciones en áreas de asunto se basan en las relaciones que se han configurado entre objetos base en el Almacén del concentrador (mediante el Administrador de esquema de la consola del concentrador).

El Administrador de configuración de IDD hace referencia a los *componentes de ruta de coincidencia*, que se basan en relaciones de clave externa.

Relaciones secundarias uno a muchos

Para las relaciones uno a muchos, el registro secundario tiene una clave externa directa del objeto principal. IDD admite dos tipos de relaciones uno a muchos.

La siguiente tabla describe los tipos de relaciones secundarias de uno a muchos:

Relación	Descripción
Uno a muchos	La lista de registros secundarios se mostrará en una ficha debajo de los datos principales.
Uno a uno lógica	Se espera que solo haya un registro secundario por cada objeto principal. Los datos se muestran en el formulario con el objeto principal. Si hay más de un elemento secundario (debido, por ejemplo, a la fusión de dos registros de objetos principales), la aplicación IDD proporciona un método para solucionar este caso.

Relaciones secundarias muchos a muchos

Para las relaciones muchos a muchos, el registro secundario está relacionado con el objeto principal a través de una tabla de relaciones.

La tabla de relaciones en un elemento secundario de muchos a muchos debe contener dos claves externas.

IDD admite dos tipos de relaciones de muchos a muchos. La siguiente tabla describe los tipos de relaciones secundarias de muchos a muchos:

Relación	Descripción
Parte de	El registro secundario pertenece al objeto principal. Ninguna otra área de asunto debe hacer referencia a este elemento secundario. Cuando se añade un elemento secundario, se añaden tanto la relación como los registros secundarios. Al editar un elemento secundario, si otra área de asunto hace referencia a ese elemento, se crea una copia del elemento secundario. Los datos a los que haga referencia el otro elemento secundario no se modificarán.
Referencia	El elemento secundario es otra área de asunto. Cuando se añade un elemento secundario, solo se añada un registro de relación. El usuario de la aplicación IDD debe buscar el elemento secundario del área de asunto que relacionar. Para editar los datos del elemento secundario, el área de asunto de ese elemento secundario debe estar abierta. Este elemento secundario se puede vincular a un objeto base de relación estándar o un objeto base de relación de HM.

Relaciones secundarias de segundo nivel de uno a muchos

Para relaciones de uno a muchos, el registro secundario de segundo nivel tiene una clave externa directa a un objeto secundario. IDD admite dos tipos de relaciones de uno a muchos. Si el elemento secundario es de muchos a muchos, la clave externa puede hacer referencia a (consulte los ejemplos de modelo de datos a continuación):

- La relación secundaria
- El registro de relaciones

Relación	Descripción
Uno a muchos	La lista de registros secundarios de segundo nivel se muestra en una ficha bajo los datos de elemento secundario.

Relaciones secundarias de segundo nivel de muchos a muchos

Para relaciones de muchos a muchos, el registro secundario de segundo nivel está relacionado con un objeto secundario a través de una tabla de relación.

IDD admite dos tipos de relaciones muchos a muchos. Si el elemento secundario es de muchos a muchos, la clave externa puede hacer referencia a (consulte los ejemplos de modelo de datos a continuación):

- Un registro secundario
- El registro de relaciones

La siguiente tabla describe los tipos de relaciones secundarias de segundo nivel de muchos a muchos:

Relación	Descripción
Parte de	El registro secundario de segundo nivel pertenece al objeto principal (ninguna otra área de asunto debe hacer referencia a este elemento secundario de segundo nivel). Al añadir un elemento secundario de segundo nivel, también se añaden tanto la relación como los registros secundarios de segundo nivel. Al editar un elemento secundario de segundo nivel, si otra área de asunto hace referencia a ese elemento, se crea una copia del elemento secundario de segundo nivel. Los datos a los que haga referencia el otro elemento secundario no se modificarán.
Referencia	El elemento secundario de segundo nivel es otra área de asunto. Al añadir un elemento secundario de segundo nivel, solo se añade un registro de relación. El usuario de la aplicación IDD debe buscar el elemento secundario de segundo nivel del área de asunto al que hacer referencia. Para editar los datos del elemento secundario de segundo nivel, el área de asunto de ese elemento secundario de segundo nivel debe estar abierta. Este elemento secundario de segundo nivel puede estar vinculado mediante un objeto base de relación estándar o un objeto base de relación de HM.

Nota: Al configurar la ruta de coincidencia para elementos secundarios de segundo nivel en el Administrador de esquema de la Consola del concentrador, asegúrese de que **Comprobar si falta un elemento secundario** está deshabilitado. La aplicación IDD no funciona correctamente si **Comprobar si falta un elemento secundario** está habilitado.

Referencias de elemento del mismo nivel

Una referencia de elemento del mismo nivel es una relación de un registro de un área de asunto con un registro secundario de esa área de asunto.

Para un modelo de datos, un cliente podría incluir registros secundarios de dirección y número de teléfono, y que el número de teléfono incluya una clave externa para asociarlo con una dirección específica. IDD puede configurarse para admitir este tipo de relación.

Al añadir o editar la clave de dirección en el número de teléfono, se proporciona al usuario de la aplicación IDD una lista de direcciones que solo contiene elementos secundarios de este grupo.

Temas relacionados

- "Configuración manual de IDD" en la página 62

Registros principales

En el área de asunto se puede incluir un registro que sea un elemento principal del objeto principal.

Se muestra en una ficha secundaria. Dado que nunca hay más de un registro en esta ficha, se muestra siempre en una vista de formulario. Estos datos son de solo lectura. IDD no permite editar estos datos ni la relación con estos datos.

Uso de características de Informatica MDM Hub

Marco de servicios de integración

Toda la interacción entre una aplicación de Data Director y un ORS se realiza mediante llamadas de API del Marco de servicios de integración (SIF).

No hay acceso directo a la base de datos de ORS (con una excepción: se pueden configurar gráficos para que utilicen un origen de datos de servidor de aplicaciones para obtener datos de informes). El Administrador de configuración de IDD utiliza SIF para acceder a metadatos sobre un ORS, pero usa un origen de datos para acceder directamente a la tabla CMX_SYSTEM.C_REPOS_DS_CONFIG.

Algunas de las llamadas de la API de SIF son asíncronas. Para habilitar la compatibilidad con llamadas de SIF asíncronas, el bloqueo a nivel de filas debe habilitarse para el ORS que utilice la aplicación de Data Director. Para obtener más información, consulte la sección sobre el bloqueo a nivel de filas en la *Guía de configuración de Multidomain MDM*.

Uso de un servidor web

Antes de implementar un servidor web que actúe como proxy inverso, configure el formato de la URL del servicio que IDD genera para las llamadas de SIF. Configure la propiedad "referer.url" del archivo `cmxserver.properties` para especificar el formato de la URL del servicio.

Añada el siguiente texto al archivo `cmxserver.properties` para configurar el formato de la URL del servicio:

```
referer.url=http://<host local>:<número de puerto>
```

Autenticación de usuario (SSO)

De forma predeterminada, Data Director autentica a los usuarios con una llamada de SIF al servidor del concentrador. Para el proceso de autenticación, la implementación de MDM Hub requiere que configure usuarios en la base de datos principal. Para obtener más información sobre la configuración de los usuarios de MDM Hub, consulte la *Guía de seguridad de Multidomain MDM*.

También puede implementar el inicio único de sesión (SSO) y autenticar los usuarios con proveedores de identidad externos. El proveedor de inicio de sesión de Data Director se comunica con el proveedor de seguridad de Hub (Módulo de inicio de sesión). Para obtener más información sobre los archivos de proveedores, consulte la *Guía de seguridad de Multidomain MDM*.

Objetos base

La seguridad a nivel de columna se configura en el Administrador de acceso de seguridad (SAM) al definir el acceso basado en funciones a objetos base y sus columnas, lo que proporciona un control avanzado sobre el acceso de los usuarios a los datos.

IDD hace referencia a objetos base directamente para todas las operaciones `GET` y `PUT`. IDD utiliza paquetes solo para mostrar resultados de búsqueda.

Memorias caché y la opción Borrar memoria caché

Informatica Data Director mantiene una memoria caché de los metadatos de MDM Hub que describe los objetos base, las columnas las relaciones, etc. Si cambia los metadatos de MDM Hub, haga clic en **Borrar memoria caché** en el Administrador de configuración de IDD antes de exportar una aplicación de IDD.

La opción Borrar memoria caché del Administrador de configuración de IDD borra la memoria caché de la aplicación IDD seleccionada. En un entorno de Microsoft SQL Server, Informatica recomienda borrar la memoria caché al realizar cambios en los metadatos de ORS mediante la consola del concentrador. Por ejemplo, si añade una relación a un objeto base en la consola del concentrador y, a continuación, guarda el

cambio y lo valida, puede volver a implementar la aplicación IDD para que el cambio surta efecto. Sin embargo, debe borrar la memoria caché antes de exportar la aplicación IDD para ver la nueva relación en el archivo Metadatabundle.properties.

También puede reiniciar el servidor de aplicaciones para borrar la memoria caché.

IDD también mantiene memorias caché de definiciones de funciones de SAM, así como asignaciones y valores de búsqueda. IDD actualiza las memorias caché con la frecuencia que se configura mediante las propiedades globales de IDD.

Rutas de coincidencia

Defina las relaciones secundarias en IDD con rutas de coincidencia. Las rutas de coincidencia se pueden configurar en el Administrador de esquema de la consola del concentrador.

Antes de la introducción de IDD, las rutas de coincidencia se utilizaban estrictamente para definir columnas de coincidencia y reglas de coincidencia. La definición de rutas de coincidencia funciona igualmente bien para definir relaciones secundarias en IDD.

Para añadir un elemento secundario a un área de asunto, debe crear una nueva ruta de coincidencia para ese elemento secundario si no existe. Al crear una ruta de coincidencia, se debe basar en ROWID_OBJECT.

Las rutas de coincidencia también pueden utilizarse para habilitar la búsqueda en tablas relacionadas que no forman parte de un área de asunto. Por ejemplo, supongamos que tiene un grupo relacionado con un producto. El producto no formará parte del área de asunto del grupo. Sin embargo, se puede definir una ruta de coincidencia del grupo al producto. Mediante esta ruta de coincidencia, un usuario de la aplicación IDD podría buscar un grupo basado en los atributos de un producto relacionado.

Buscar

La búsqueda de datos en un área de asunto se puede basar en cualquiera de las siguientes API de búsqueda de SIF: searchQuery y searchMatch.

En ambos casos, se utiliza un paquete de visualización para mostrar los resultados de búsqueda.

Básica: búsqueda basada en SQL

La búsqueda básica utiliza la API searchQuery.

Una búsqueda puede basarse en los datos de:

- El registro de objetos principal
- Cualquiera de sus registros secundario (PO)
- Cualquier registro relacionado mediante un componente de ruta de coincidencia

Puede realizar una búsqueda básica que no distinga entre mayúsculas y minúsculas al ejecutar una consulta de datos. La búsqueda básica encuentra resultados mediante comparaciones de cadenas y patrones de cadenas.

Extendida: búsqueda basada en coincidencias

La búsqueda extendida no distingue entre mayúsculas y minúsculas y utiliza la API **searchMatch** API con matchType=NONE.

Está pensada para buscar y, por lo tanto, no utiliza un conjunto de reglas de coincidencia predefinido. Se puede usar como criterio de búsqueda cualquiera de los datos del área de asunto que contribuya a una

columna de coincidencia. Una aplicación IDD requiere que los usuarios especifiquen criterios en la clave de coincidencia parcial antes de poder ejecutar la búsqueda.

Búsqueda avanzada

La búsqueda avanzada permite a los usuarios de la aplicación IDD crear consultas complejas al definir expresiones SQL de tipo WHERE y texto de consulta de forma libre.

Puede realizar una búsqueda avanzada que no distinga entre mayúsculas y minúsculas al ejecutar una consulta de datos. La búsqueda avanzada permite a los usuarios de la aplicación IDD especificar condiciones de búsqueda más avanzadas que las funciones disponibles en la búsqueda básica o extendida.

Funciones de limpieza

IDD usa la API **PUT**, en lugar de **cleansePut**.

Sin embargo, IDD puede llamar a la API **cleanse** para cada registro de objeto base antes de que se guarde. En ocasiones esto se conoce como *función de limpieza en línea*. La función de limpieza puede realizar la limpieza y estandarización periódicas de datos, así como personalizar validaciones en los datos. Se llama a cada función de limpieza configurada antes de guardar los datos.

- En la vista de datos, se llama a la función de limpieza al hacer clic en **Aplicar** en un formulario de edición.
- En la vista de jerarquía, se llama a la función de limpieza al hacer clic en **Aceptar** en un cuadro de diálogo de adición/edición de relación.

Limpieza y estandarización

El Administrador de configuración de IDD proporciona un método directo para conectar registros de objeto base a las entradas y salidas de una función de limpieza.

Los datos del registro de objeto base se actualizan con las salidas de la función de limpieza.

Nota: Solo las columnas de objetos base seleccionadas en el diseño para la configuración del área de asunto pueden actuar como entradas o salidas de la función de limpieza.

Validación

La función de limpieza se puede utilizar para realizar la validación de datos personalizados.

Los resultados de la validación se procesan si la función de limpieza tiene un parámetro de salida validationStatus.

- Si el parámetro validationStatus está en blanco, no hay errores de validación y el proceso puede continuar.
- Si hay errores de validación, el parámetro validationStatus incluirá una serie de mensajes de validación que describen el nombre de inputParameter y un mensaje. En la IU de la aplicación IDD, cada error de validación se asocia con un valor de entrada en una columna de entrada determinada.

Nota: El kit de recurso contiene la muestra ValidationCleanseLib, que ofrece un ejemplo de una biblioteca de limpieza con funciones que realizan la validación en una aplicación IDD.

Funciones de limpieza que devuelven un valor NULL

Cuando la salida de una función de limpieza es un valor nulo, la API de **limpieza** no devuelve información sobre ese campo.

Se supone que la función no modifica ese campo. Si el objetivo de la función de limpieza es reemplazar un valor por NULL, las opciones dependen del tipo de datos y se requiere lo siguiente:

- Cadena: la función se puede cambiar para devolver una cadena vacía.
- Fecha o valor numérico: se debe implementar una salida de usuario para modificar los datos. Se pueden usar los métodos beforeEverything() o beforeSave() del controlador Save.

Temas relacionados

- "Salidas de usuario" en la página 86

Confianza

Una aplicación de Data Director se configura para que utilice un único sistema de origen para todas sus operaciones.

Los datos introducidos y actualizados mediante una aplicación de Data Director siguen todas las reglas de confianza estándar, tal como se describe en la ayuda en línea de la consola de administración o en la *Guía de configuración de Multidomain MDM*. Los datos introducidos en una aplicación de Data Director se aplican al registro de objeto base basado en las reglas de confianza y validación configuradas en Informatica MDM Hub para ese sistema de origen. Al visualizar datos de referencia cruzada, puede promover el valor de un atributo de un registro de referencia cruzada para columnas que tengan la confianza habilitada. Esto produce un reemplazo de confianza para ese atributo.

Flujos de trabajo y tareas

Una aplicación IDD puede utilizar flujos de trabajo y tareas para ser compatible con un proceso de aprobación de cambios para registros habilitados para el estado en el Almacén del concentrador.

Por ejemplo, considere un caso en el que un Administrador financiero desee revisar todos los cambios de la información bancaria del cliente antes de que se pueda aceptar el cambio como un dato principal. Puede configurar una aplicación IDD para que, cuando cualquier persona del Departamento financiero utilice la aplicación para actualizar información, se asigna una tarea automáticamente al Administrador financiero para que revise o rechace el cambio pendiente. Un proceso de aprobación de cambios garantiza que únicamente los registros aprobados puedan contribuir a los registros de la mejor versión de confianza (BVT).

Una aplicación IDD coordina las actividades de la tarea entre la Bandeja de entrada de tareas de IDD, una herramienta de administración de proceso empresarial (BPM) y tablas habilitadas para el estado en almacén del concentrador. Para incluir la compatibilidad del flujo de trabajo en su aplicación, consulte "Paso 7. Configurar los flujos de trabajo de MDM" en la página 36.

Tareas y acciones

Una *tarea* es un paso de un proceso de flujo de trabajo.

Para cualquier tarea, habrá una o varias *acciones* que se puedan realizar. Las tareas y sus acciones asociadas se pueden configurar como parte de una aplicación IDD.

Datos en vuelo

Los *datos en vuelo* son datos empresariales que pueden pasar por distintos estados (ACTIVO, PENDIENTE o ELIMINADO) mientras progresan por un flujo de trabajo.

IDD admite datos en vuelo con la funcionalidad de administración de estado de Informatica MDM Hub y las características de administración de tareas.

Los datos se pueden añadir o actualizar y "enviarse para su aprobación", en lugar de guardarse. Los cambios en los datos se almacenan como cambios PENDIENTES (los datos no se aplican al objeto base). Se crea una tarea para que otro usuario apruebe este cambio. Una vez aprobado, los datos pendientes se promueven a activos y estos se aplican entonces al objeto base.

Administrador de jerarquía

Si el Administrador de jerarquía (HM) está configurado para un ORS, puede configurar una aplicación IDD para que funcione con esta configuración.

Configure la aplicación IDD según las reglas siguientes:

- Cualquier entidad de HM que una aplicación IDD utilice debe configurarse como área de asunto en el Administrador de configuración de IDD. HM se utiliza para modelar las relaciones entre áreas de asunto.
- Una aplicación IDD opera con una única configuración de HM (combinación de perfil/espacio aislado). IDD utiliza la configuración de control de acceso de SAM para administrar el control de acceso de usuario, en lugar de distintas configuraciones de HM. La configuración de HM que utiliza una aplicación IDD debe incluir todos los tipos de relación y entidad de HM que se van a usar en la aplicación IDD.

Administrador de acceso de seguridad

Use el Administrador de acceso de seguridad para conceder a las funciones de usuario un acceso granular a los objetos base y a otros recursos. Data Director hereda las funciones de usuario e implementa el mismo acceso granular a los registros.

Para obtener más información, consulte la *Guía de seguridad de Multidomain MDM*.

Temas relacionados

- "Configuración de seguridad de IDD" en la página 117

Seguridad de objetos y columnas

SAM proporciona privilegios de seguridad basados en funciones en columnas y objetos de diseño definidos en un ORS.

Una aplicación IDD utiliza esta configuración de seguridad para que los datos que se muestran y las operaciones disponibles para un usuario individual dependan de las funciones asignadas a esa cuenta de usuario. Los usuarios de la aplicación IDD solo ven los datos y funciones para los que se les ha concedido acceso. Por ejemplo, si un usuario no tiene acceso de lectura para la tabla HISTORY de un objeto base, el comando Historial de esa área de asunto no está disponible para el usuario en la aplicación IDD.

Nota: Un usuario del concentrador con acceso de administrador (configurado en la herramienta Usuarios de la Consola del concentrador) es un superusuario para IDD y tiene todos los privilegios en todos los objetos.

Seguridad de datos

SAM no proporciona seguridad de datos a nivel de fila (restringe los registros que pueden ver los usuarios en función del contenido de esos registros).

IDD, no obstante, proporciona un mecanismo de seguridad de datos simple. Para cada área de asunto, se pueden definir *filtros de seguridad* en el archivo de configuración de IDD. Un filtro de seguridad especifica una condición de filtro que IDD aplica a todos los datos a los que acceden los usuarios asignados a una función específica. Por ejemplo, un filtro de seguridad puede especificar `COUNTRY_CODE = 'US'`, que puede aplicarse a los usuarios con la función de gestor de datos en EE. UU. Cada filtro puede aplicarse a varias funciones. Para un área de asunto se pueden crear todos los filtros que se deseen para cualquier número de funciones.

Enmascaramiento de datos

IDD proporciona un mecanismo para ocultar (enmascarar) información basándose en funciones de seguridad.

Puede definir una máscara para cada campo en un diseño de columna. La máscara se puede especificar para una función única, para un conjunto de funciones o para todos los usuarios que no sean administradores. Cuando se especifica una máscara, todo el valor o parte del valor se reemplazará con un asterisco (*).

TEMAS RELACIONADOS

- "Enmascaramiento de datos" en la página 144

Historial

IDD proporciona una vista de área de asunto del historial de cambios de cada registro.

Esta función requiere que el historial se habilite en el objeto base. Si el historial no está habilitado para un objeto base, la vista del historial no está disponible para el área de asunto asociada en la aplicación IDD. IDD muestra una vista de línea temporal de eventos para el registro y sus registros secundarios. También se puede mostrar una vista de punto en el tiempo de los datos.

Tablas de búsqueda

La tabla de búsqueda, que también se conoce como búsqueda u objeto base de búsqueda, es una tabla que almacena una lista de valores predefinidos. Data Director (IDD) consulta la tabla de búsqueda para recuperar un valor basado en el valor de origen de entrada y la condición de búsqueda. Data Director rellena después una lista desplegable de valores en la aplicación. Por ejemplo, si introduce un valor en un campo País, la aplicación enumera los países almacenados en la tabla de objetos base de búsqueda LU_COUNTRY.

Puede definir valores de búsqueda de las siguientes maneras:

- En una tabla de objetos base de búsqueda física con una clave externa entre el objeto base y el objeto base de búsqueda. Data Director utiliza metadatos sobre esta clave externa para rellenar los valores de búsqueda.
- En una tabla de objetos base de búsqueda física sin clave externa entre el objeto base y el objeto base de búsqueda. La configuración de IDD describe la relación de clave externa, que rellena los valores de búsqueda.
- En una lista estática de valores en la configuración de IDD.

Para búsquedas definidas en una tabla física, la columna LOOKUP_IND de C_REPOS_TABLE indica si la tabla contiene valores de búsqueda o datos regulares. Puede habilitar el indicador de búsqueda mediante la

Herramienta de esquema de la consola del concentrador. De forma predeterminada, el indicador de búsqueda se deshabilita al crear un objeto base. Al habilitar el indicador de búsqueda, MDM Hub considera el objeto base como una búsqueda. Para obtener más información acerca de la herramienta Esquema, consulte la *Guía de configuración de Multidomain MDM*.

Nota: Cuando cree una búsqueda, utilice un nombre para mostrar único. Data Director no puede distinguir diferentes tablas de búsqueda que comparten el mismo nombre para mostrar.

Cuando Data Director reconoce que una columna tiene una clave externa a otra tabla, Data Director determina si la tabla relacionada es una tabla de búsqueda. Si la tabla relacionada es una tabla de búsqueda, Data Director crea una lista desplegable en la aplicación para esa columna, que se rellena con valores de la tabla de búsqueda. La columna de la tabla de búsqueda que se utiliza depende del campo **Nombre para mostrar de búsqueda** configurado para la relación en la Herramienta de esquema.

TEMAS RELACIONADOS

- "Columna de búsqueda" en la página 65

Búsquedas de dependientes

Una búsqueda dependiente es una tabla de búsqueda que depende de otra tabla de búsqueda.

Un ejemplo típico de tabla de búsqueda dependiente es una tabla de búsqueda de tipo y una tabla de búsqueda de subtipo. La lista de valores que aparece en el campo de subtipo depende del valor seleccionado en el campo de tipo en IDD. Por ejemplo, si ha seleccionado Estados Unidos en un campo País, al introducir un valor en el campo estado, IDD muestra los estados de EE. UU. almacenados en la tabla de búsqueda dependiente LU_STATE.

Línea temporal

La línea temporal le permite ver y administrar los eventos de cambio de datos de entidades empresariales y sus relaciones. Puede definir las versiones o los eventos de cambios de datos de entidades empresariales y sus relaciones en función de sus períodos efectivos.

Los cambios de datos se producen con el tiempo y no dependen de las relaciones con otros datos. Los cambios de datos dan como resultado un nuevo período efectivo o un período efectivo actualizado para el pasado, presente o futuro. La función de línea temporal permite realizar un seguimiento de estos cambios en los datos durante un período de tiempo.

Por ejemplo, John Smith ha vivido en Los Ángeles desde el 31 de enero de 2008 hasta el 20 de octubre de 2010. Ahora vive en San Francisco desde el 21 de octubre de 2010. Vivirá en Las Vegas desde el 25 de noviembre de 2014. Utilice líneas temporales para realizar un seguimiento de los cambios pasados, presentes y futuros en los datos, como la dirección de John Smith.

Nota: Puede especificar el período efectivo con el formato de fecha. El sistema utiliza la configuración regional de hora de la base de datos para las fechas.

Las funciones de la línea temporal proporcionan un punto de vista bidimensional de los datos basado en el período efectivo y el historial. El período efectivo de un registro está definido por la fecha de inicio efectiva y la fecha de finalización efectiva de un registro de objeto base. El historial es una fecha del historial de un registro para el que necesita ver el valor. Puede administrar eventos de datos de entidades empresariales, como la dirección del cliente, su número de teléfono y sus relaciones, para lo que debe habilitar la línea temporal para los objetos base pertinentes. Para habilitar la línea temporal para un objeto base secundario, primero deberá habilitar la línea temporal para el objeto base principal. El MDM Hub utiliza las tablas de referencias cruzadas (XREF) asociadas a los objetos base habilitados para la línea temporal para mantener los períodos efectivos para los registros de objeto base.

Nota: Debe habilitar la línea temporal para cada objeto base en la Consola del concentrador, salvo para el objeto base de relación secundaria habilitado para la jerarquía.

Para obtener más información, consulte la *Guía de configuración de Multidomain MDM*.

Reglas de línea temporal

Al definir y mantener la información de línea temporal, Informatica MDM Hub aplica las reglas de línea temporal.

Se requiere conocer las reglas que Informatica MDM Hub aplica para administrar líneas de tiempo de entidades empresariales y relaciones. En cualquier momento, Informatica MDM Hub solo considerará una versión de un registro como efectiva en función de las fechas de inicio y finalización efectivas. Cuando se utilizan procesos por lotes, el Marco de servicios de integración o Data Director para modificar datos, Informatica MDM Hub mantiene los datos efectivos actuales. Asimismo, cuando muchos sistemas contribuyen a un registro de objeto base, Informatica MDM Hub aplica reglas para actualizar la versión del registro, según los registros efectivos que contribuyen.

También puede utilizar salidas de usuario para definir y aplicar reglas personalizadas para administrar líneas de tiempo y fechas efectivas.

Para obtener más información, consulte la *Guía de configuración de Multidomain MDM*.

Marcadores

Los marcadores son direcciones URL que abren una aplicación IDD y muestran una vista, tarea o búsqueda.

Nota: Hay marcadores disponibles para aplicaciones IDD que utilizan el modelo de áreas de asunto.

La URL especifica qué aplicación IDD invocar, qué parte de la aplicación abrir y qué entidad mostrar. Los marcadores se pueden utilizar para invocar IDD desde una aplicación externa (por ejemplo, Informatica MDM Data Control o IDC) o desde un navegador. Los usuarios pueden compartir una URL de marcador con otro usuario. Cuando el usuario abre la URL en un explorador, debe iniciar sesión correctamente en la aplicación IDD para ver la vista.

En una aplicación IDD, puede vincular a los comandos Mostrar marcador en las páginas. Estos comandos proporcionan el enlace de URL de la entidad actual. Los marcadores están disponibles para las siguientes funciones: Vista de datos, vista de jerarquía, tareas y búsquedas.

El formato de la URL es el siguiente:

```
http://<host>[:<port>]/bdd/?deeplink=<operation>;<iddAppName>/
<subjectAreaID>;<param1>[;<param2>]
```

Donde:

Variable	Descripción
host	Nombre del equipo que aloja Informatica MDM Hub.
puerto	Opcional. Número de puerto.

Variable	Descripción
operation	Uno de los siguientes valores: - openrecord;dv: abre una entidad en la vista de datos. - openrecord;hm: abre una entidad en la vista de jerarquía. - opentask: abre una ventana de tarea. - search: abre una ventana de búsqueda.
iddAppName	Nombre de la aplicación IDD.
subjectAreaID	Identifica el área de asunto. Utiliza el formato siguiente: `subjectAreaGroupName/SubjectAreaName`
param1	Define qué datos mostrar y depende de la operación.
param2	Opcional. Depende de la operación.

Nota: Cualquier carácter que no esté permitido en una URL debe codificarse por duplicado. La codificación dual (el proceso de codificación se ejecuta dos veces) es necesaria para permitir que los servidores web acepten solicitudes que contengan barras ("/" y "\") en sus parámetros. Los servidores web rechazan aquellas solicitudes que contienen barras de parámetros codificadas una sola vez. Solo se deben codificar por duplicado los valores de parámetros.

Vista de datos

La operación *openrecord;dv* se usa para abrir una vista de datos.

subjectAreaID identifica el área de asunto, mientras que *param1* identifica el registro. Al igual que las API de SIF, un registro puede identificarse por rowid o por el nombre del sistema y la clave de origen. Al utilizar la clave de origen, asegúrese de incluir todos los espacios iniciales o finales del valor.

Además, *param2* puede utilizarse para especificar *xref*, *history*, *duplicates* para abrir la vista de datos con las pantallas **Referencias cruzadas**, **Historial** o **Buscar duplicados**.

Ejemplos:

```
http://<host>[:<port>]/bdd/?deeplink=openrecord;dv;test/Customer;rowid:268
http://<host>[:<port>]/bdd/?deeplink=openrecord;dv;test/Customer;
systemName:SFA,sourceKey:CST1160
http://<host>[:<port>]/bdd/?deeplink=openrecord;dv;test/Customer;rowid:268;xref
```

Los registros fusionados son un caso especial. Si fusiona un registro con otro, el registro fusionado tiene el rowid del registro que se conserva. No obstante, podrá seguir utilizando una URL de marcador que haga referencia al rowid que no se conserva. En tal caso, la URL se redirecciona al rowid del registro fusionado. Por ejemplo, supongamos que fusiona dos registros con los rowid 1 y 2, y que el registro fusionado tiene el rowid 1. Si utiliza una URL de marcador y especifica el rowid 2, el vínculo se redirecciona y recupera el registro fusionado con el rowid 1.

Vista de jerarquía

La operación *openrecord;hm* se usa para abrir una vista de jerarquía.

subjectAreaID identifica el área de asunto, mientras que *param1* identifica el registro. Estos parámetros se usan igual que los parámetros de la vista de datos.

Ejemplos:

```
http://<host>[:<port>]/bdd/?deeplink=openrecord;hm;test/Customer;rowid:268
http://<host>[:<port>]/bdd/?deeplink=openrecord;hm;test/Customer;
systemName:SFA,sourceKey:CST1160
```

Tarea

La operación *opentaskv* se usa para abrir una tarea.

subjectAreaID identifica el área de asunto, mientras que *param1* identifica la tarea (este es simplemente el valor de ROWID_TASK para la tarea).

Ejemplo:

```
http://<host>[:<port>]/bdd/?deeplink=opentask;test/Customer;3162
```

Buscar

La operación *search* se usa para abrir una ficha de búsqueda y ejecutar una búsqueda.

subjectAreaID identifica el área de asunto, mientras que *param1* define los campos y valores del formulario de búsqueda. Utilice el comando Mostrar marcador para ver ejemplos de *param1*.

CAPÍTULO 3

Proceso de implementación

Este capítulo incluye los siguientes temas:

Resumen del proceso de implementación

Esta sección describe el proceso de alto nivel recomendado para configurar aplicaciones IDD.

Este proceso debe utilizarse como plantilla para la creación de planes de implementación de IDD. El principal objetivo es describir los pasos del ciclo de creación/prueba que facilitarán un modelo eficiente para un rápido desarrollo de IDD. Este enfoque permite usar las etapas intermedias del proceso de configuración para obtener información adicional y validar los requisitos con el cliente.

Antes de empezar

Esta sección asume que se cumplen los siguientes requisitos previos:

- Informatica MDM Hub, los adaptadores de limpieza y Servidores de procesos ya están configurados y operativos en su entorno. Para obtener más información, consulte la *Guía de instalación de Multidomain MDM*.
- Los esquemas de ORS están configurados y contienen algunos datos de prueba. Para configurar la aplicación IDD es necesario usar tanto el Administrador de configuración de IDD como la Consola del concentrador. La Consola del concentrador se utiliza para crear los elementos de configuración necesarios en el ORS de destino (como objetos base, paquetes, búsquedas, componentes de ruta de coincidencia, etc.).
- Todos los objetos base (y los metadatos asociados) requeridos para una aplicación IDD se deben configurar como SECURE en la herramienta Recursos seguros de la Consola del concentrador.
- La configuración y la prueba inicial se deben realizar con una cuenta de usuario de MDM Hub con privilegios sin restringir para los esquemas de ORS de destino. Puede usar la cuenta de administrador o cualquier otra cuenta configurada con todos los privilegios para el grupo ALL_GLOBAL_RESOURCES.

  Nota: ALL_GLOBAL_RESOURCES no incluye los recursos personalizados añadidos como parte de la aplicación IDD. Esos recursos deben configurarse individualmente.

- El análisis y el modelado de datos para definir las áreas de asunto y las reglas empresariales se han completado.
- Si desea compatibilidad con flujos de trabajo, en el MDM Hub debe habilitar la administración de estado en las tablas de objeto base de destino y decidir qué herramienta de BPM desea utilizar para su motor de flujo de trabajo. Es posible que necesite completar algunos pasos de integración para herramientas independientes de BPM. Para obtener más información, véase *Guía de configuración de Multidomain MDM*.
- Otras áreas del Almacén del concentrador que deben configurarse:
  - Seguridad
  - Funciones de limpieza (si se usan para comprobar los datos introducidos por usuarios de IDD en una aplicación IDD);
  - Administrador de jerarquía (si se utiliza en una aplicación IDD).

    Nota: si habilita la administración de estado en cualquier tabla de entidad o relación de Administrador de jerarquía, debe habilitar la función en todas ellas.

Para obtener más información sobre las herramientas de la consola del concentrador, consulte la ayuda en línea de la Consola de administración o la *Guía de configuración de Multidomain MDM*.

Proceso de configuración

Siga el proceso de configuración para realizar cambios en la configuración de Informatica Data Director.

El proceso de configuración es un proceso iterativo, es decir, que no es un procedimiento lineal ni puntual. Puede administrar la mayor parte de la configuración de la aplicación IDD directamente en el administrador de configuración de Informatica Data Director. Para algunos pasos del proceso de configuración es necesario editar manualmente los componentes de la aplicación IDD.

Si ha cambiado los metadatos del almacén de referencias operativas, haga clic en **Borrar memoria caché** para obtener los metadatos más recientes de MDM Hub.

Nota: No implemente IDD mientras se ejecuta un trabajo por lotes de carga de MDM Hub o mientras otro usuario realiza cambios en la consola de MDM Hub. Si implementa IDD durante estas actividades de MDM Hub, se producirán errores de validación del almacén de referencias operativas en IDD.

Temas relacionados

- "Administrador de configuración de IDD" en la página 40

Paso 1. Crear la aplicación IDD

Cree la aplicación IDD en el Administrador de configuración de IDD.

1. Para instancias de IDD que abarcan varias bases de datos de ORS puede crear áreas de asunto de distintos ORS, pero el elemento secundario del área de asunto de un área de asunto debe ser del mismo ORS; cree áreas de asunto individuales para cada ORS por separado (en distintas aplicaciones IDD).
2. Exporte la configuración.
3. Integre los archivos de configuración XML individuales fusionándolos para crear una instancia de IDD de varios ORS.

Tenga en cuenta las siguientes consideraciones relativas a la configuración:

Consideraciones	Descripción
Sistema de origen de la aplicación	La propiedad más importante definida a nivel de aplicación IDD es el sistema de origen que una aplicación IDD utiliza para realizar un seguimiento de las actualizaciones realizadas en la propia aplicación IDD (como las ediciones realizadas por los usuarios de la aplicación IDD en una vista de datos). De forma predeterminada, se utiliza el sistema de administración. Mediante la herramienta Sistemas y confianza de la Consola del concentrador, puede crear un sistema de origen de aplicación. Para configurar la confianza en columnas de objetos base para otro sistema, debe crear una tabla de ensayo ficticia y asignarla al sistema de origen de IDD. Independientemente de qué sistema de origen de aplicación IDD utilice, deberá configurarlo para tener el más alto nivel de confianza que garantice que los cambios aplicados por los usuarios de la aplicación IDD reemplazan a cualquier otro valor contributivo y acaban en la mejor versión de confianza (BVT) (registro principal). Si este no es el caso, los resultados de una actualización serán muy confusos para los usuarios de la aplicación IDD.
Configuración de HM	Si planea utilizar las funciones de HM de IDD, debe definir el perfil de HM (mediante la herramienta Jerarquías en la Consola del concentrador) que se usará para configurar las funciones del Administrador de jerarquía de IDD. La configuración de HM debe especificarse por adelantado para garantizar que las definiciones de áreas de asunto sean coherentes con las definiciones de entidades de HM.

Paso 2. Configurar grupos de área de asunto

Configure grupos de área de asunto.

- Utilice el Administrador de configuración de IDD para crear cualquier grupo de área de asunto que necesite.

  Por ejemplo, puede crear un grupo de área de asunto de cliente que contenga dos áreas de asunto: Persona y Organización.

Paso 3. Configurar áreas de asunto

Configure áreas de asunto.

- Si el grupo de área de asunto contiene varias áreas de asunto, identifique el atributo de datos del objeto raíz del área de asunto que se usará para diferenciar las áreas de asunto.

  Por ejemplo, un atributo party_type distingue entidades de un grupo por tipo.

Paso 3.1. Configurar áreas de asunto en la Consola del concentrador

Configure áreas de asunto en la Consola del concentrador.

1. En el Administrador de esquema, revise los componentes de la ruta de coincidencia configurados para el objeto raíz del área de asunto y compruebe que hay rutas de coincidencia para cada uno de los objetos secundarios que deben incluirse en el área de asunto y para los objetos relacionados que deben usarse en las búsquedas.

2. En la herramienta Paquetes, cree el paquete de visualización de búsqueda que se va a utilizar para mostrar los resultados de búsqueda para el área de asunto. Este es un paquete con el objeto raíz del área de asunto como tabla principal.
3. En el Administrador de esquema, compruebe las dependencias de búsqueda de área de asunto.

Mecanismo de búsqueda	Descripción
Tablas de búsqueda de código	Las tablas de búsqueda de código deben tener el Indicador de búsqueda establecido en TRUE (seleccionado) en las propiedades del objeto base en el Administrador de esquema.
Búsquedas de entidad	Las búsquedas de entidad solo se pueden especificar para entidades configuradas como áreas de asunto. Esto puede introducir dependencias complejas entre las áreas de asunto. Como parte del desarrollo iterativo de una aplicación IDD, puede excluir búsquedas de entidad de la configuración de IDD inicial si hay dependencias en el resto de áreas de asunto que no se han configurado. Los campos de búsqueda se pueden añadir cuando se cumplan todas las dependencias de áreas de asunto.

Paso 3.2. Configurar áreas de asunto en el Administrador de configuración de IDD

Configure áreas de asunto en el Administrador de configuración de IDD.

1. Cree la configuración básica de área de asunto y pruébela validando e implementando la aplicación.

   Esta configuración incluye la configuración del diseño (se deben especificar como mínimo las columnas que mostrar con el tamaño y el tipo de campo de cada una), la configuración de coincidencia utilizada para realizar comprobaciones de duplicados, la configuración de todas las funciones de limpieza que se utilizarán para comprobar los datos introducidos por usuarios de la aplicación IDD (se utiliza para la validación y/o limpieza de datos), la configuración de la etiqueta para el área de asunto y las asignaciones de tareas de área de asunto.
2. Añada los elementos secundarios y los elementos secundarios de segundo nivel al área de asunto.

   Todos los elementos secundarios y los elementos secundarios de segundo nivel deben tener una ruta de coincidencia debidamente configurada al objeto raíz del área de asunto (configurada en el panel Detalles de la configuración de coincidencia/fusión del Administrador de esquema). Al crear un nuevo elemento secundario, el Administrador de configuración de IDD muestra los nombres de los componentes de la ruta de coincidencia en lugar de los nombres de los objetos secundarios.

   Solo se mostrarán los componentes de la ruta de coincidencia que sean relevantes para el tipo de elemento secundario. Esta configuración incluye la configuración del diseño (columnas que mostrar con el tamaño y el tipo de campo de cada una) y la configuración de una función de limpieza (opcional) que aplicar al registro (se utiliza para limpieza y/o validación).

Sugerencia sobre cómo añadir elementos secundarios y elementos secundarios de segundo nivel

Para simplificar la solución de problemas con la configuración de elementos secundarios y elementos secundarios de segundo nivel, puede añadirlos de uno en uno e implementar/probar la configuración cada vez que añada uno (antes de agregar el siguiente) para aislar cualquier problema de configuración que pueda surgir de forma incremental.

Configuración de diseño

La configuración del diseño se utiliza para:

- Especificar qué campos mostrar del objeto base.

- Especificar el número de columnas para diseños de formulario.
- Especificar el formato de fecha y hora.
- Especificar el tamaño del campo de IU para todos los campos (pequeño, mediano o grande).
- Especificar los campos obligatorios, es decir, los que no pueden tener un valor NULL (esto se configura en el archivo de configuración de IDD).
- Especificar qué campos se muestran como hipervínculo.

  Nota: En el Administrador de configuración de IDD, solo se puede marcar con **Mostrar como hipervínculo** el tipo de datos de columna de Cadena definido en la Consola del concentrador. Solo se analizarán como hipervínculo los campos con una URL o dirección de correo electrónico válida.

Paso 3.3. Validar, implementar y probar los cambios

En la aplicación IDD, valide, implemente y pruebe los cambios.

1. Cree una consulta para una nueva búsqueda.
2. Compruebe que están disponibles todos los atributos necesarios (atributos definidos en los diseños de los objetos raíz y secundarios).
3. Añada una nueva entidad (registro) a un área de asunto.
   a. Confirme que se pueden crear todos los elementos secundarios y que todos los campos se muestran en el orden esperado.
   b. Confirme que todos los campos de búsqueda se muestran correctamente y tienen las listas de valores adecuadas. Si los campos no muestran los controles de búsqueda, debe ajustar la configuración del campo Búsqueda (establezca el Indicador de búsqueda en TRUE en el Administrador de esquema).

Paso 3.4. Configurar otras fichas secundarias

Para configurar fichas secundarias del área de asunto adicionales, actualice el archivo de configuración de Informatica Data Director.

Puede configurar las fichas secundarias del área de asunto **Parte del objeto principal** y **XREF**.

Paso 4. Configurar la limpieza y la validación

La validación y la limpieza son elementos opciones para primaryObject, one2ManyChild y many2ManyChild.

El Administrador de configuración de IDD no crea el elemento cleanseFunction; simplemente enlaza la función de limpieza a columnas del objeto base.

Los datos que el usuario de la aplicación IDD ha introducido en atributos de área de asunto se transmiten a la función de limpieza como entradas. El registro del objeto base se actualizan con las salidas de la función de limpieza.

La función de limpieza puede indicar errores de validación si se configura con una salida validationStatus. Si se detectan errores de validación, la aplicación IDD muestra los errores junto a los campos con problemas.

1. Cree la biblioteca de funciones de validación con la muestra ValidationCleanseLib del kit de recurso de Informatica MDM Hub como plantilla.
2. Mediante la herramienta Funciones de limpieza de la Consola del concentrador, implemente la biblioteca de limpieza creada en el ORS.
3. Mediante las herramientas Funciones de limpieza y Asignaciones de la Consola del concentrador, cree funciones de limpieza y asignaciones para utilizarlas en aplicaciones IDD.

4. Mediante el Administrador de configuración, configure estas funciones para usarlas en una aplicación IDD (en el cuadro de diálogo Editar del área de asunto).
5. Implemente y pruebe las funciones de limpieza y validación. Compruebe que todos los campos se han limpiado y validado correctamente.

Paso 5. Configurar la búsqueda

La configuración de búsqueda comprende la búsqueda básica y la búsqueda ampliada, así como consultas públicas.

La búsqueda avanzada está preconfigurada con opciones de configuración que no se pueden editar.

Paso 5.1. Configurar la búsqueda básica

La búsqueda básica permite a los usuarios de la aplicación IDD buscar instancias de áreas de asunto mediante la creación de consultas en el área de asunto.

Los resultados se muestran mediante un paquete de MDM Hub que se crea en la herramienta Paquetes de la consola del concentrador. IDD emplea un nuevo modo de la API de **searchQuery** para mostrar los resultados.

El paquete de búsqueda debe cumplir con los criterios siguientes:

- Se basa en el objeto base raíz del área de asunto.
- Devuelve una única fila de resultados por cada entidad de área de asunto.
- Contiene el ROWID_OBJECT del objeto base raíz del área de asunto.

El paquete utilizado para buscar debe contener las columnas necesarias para presentar los resultados de búsqueda al usuario. Una aplicación IDD busca directamente en un objeto base raíz y los elementos secundarios asociados. No realiza consultas en los atributos del paquete de visualización.

IDD no elimina los duplicados de los resultados de búsqueda. Para devolver una única fila por cada entidad encontrada, es necesario crear un paquete.

1. Para garantizar que un paquete de búsqueda devuelva una única fila por cada entidad, pruebe el paquete de búsqueda directamente con SQL. Un método de prueba consiste en ejecutar revisiones aleatorias en entidades que contengan un número conocido de elementos secundarios de tipos diferentes.
2. Identifique los atributos de búsqueda principales. En el Administrador de esquema, cree los índices personalizados correspondientes para respaldar estas búsquedas.
3. Para probar las búsquedas, cree tipos de consultas diferentes y ejecútelas en una aplicación IDD. Utilice distintas combinaciones de criterios de búsqueda para garantizar un rendimiento satisfactorio de estas búsquedas.
4. Asimismo, la búsqueda se puede configurar para objetos que no forman parte del área de asunto mediante la ficha Buscar en el elemento secundario de la configuración de búsqueda. De esta forma, puede buscar en cualquier objeto para el que exista una ruta de coincidencia desde el objeto principal. Estos objetos estarán disponibles en el Constructor de consulta.

   La ficha Buscar en el elemento secundario le permite buscar los siguientes tipos de datos:

   - Datos relacionados que no forman parte del área de asunto.
   - Referencias cruzadas de datos del área de asunto.
   - En general, todos los datos que se pueden relacionar con el objeto principal mediante una ruta de coincidencia.

Paso 5.2. Configurar la búsqueda ampliada

La búsqueda ampliada utiliza la API searchMatch para solicitar búsquedas parciales en los datos.

1. Debe asegurarse de que se hayan creado todas las columnas de coincidencia necesarias. Para habilitar la búsqueda parcial, no es necesario configurar nada más en una aplicación IDD. IDD asignará automáticamente los criterios de búsqueda proporcionados por el usuario de la aplicación IDD a las columnas habilitadas para coincidencias disponibles y ejecutará la búsqueda.
2. Antes de probar la configuración de la búsqueda ampliada, compruebe que los datos se han agrupado correctamente en tokens y, a continuación, pruebe las funciones de búsqueda parcial creando las consultas de búsqueda para incluir los atributos de área de asunto que tienen columnas habilitadas de coincidencias subyacentes.

   Para obtener más información, consulte "Configurar el proceso de coincidencia" en la *Guía de configuración de Multidomain MDM* o la Ayuda en línea de la Consola del concentrador, así como la descripción de la API searchMatch en la *Guía del marco de servicios de integración de Multidomain MDM* o Javadoc.
3. La búsqueda ampliada utiliza la API **searchMatch** con matchType=NONE. En la configuración predeterminada, se generan todas las posibles columnas de coincidencia en cada solicitud de searchMatch. IDD se puede configurar para generar únicamente columnas de coincidencia específicas. En la ficha Búsqueda del cuadro de diálogo del área de asunto, puede especificar el conjunto determinado de columnas de coincidencia que se va a generar.

   Nota: De forma predeterminada, en este modo de searchMatch, el nivel de búsqueda se establece en Estrecha. Este es el nivel más restrictivo, pero se puede reemplazar si se configura el siguiente valor en cmxcleanse.properties:

   ```
   cmx.server.match.searcher_search_level=<level>
   ```

   donde *<level>* es uno de los siguientes valores: Estrecha, Típica, Exhaustiva o Extrema. Para obtener más información sobre los niveles de búsqueda en las propiedades del conjunto de reglas de coincidencia, consulte "Configurar el proceso de coincidencia" en la *Guía de configuración de Multidomain MDM*.

Paso 5.3. Configurar consultas públicas

IDD permite a los administradores y usuarios expertos compartir las consultas que crean con el resto de usuarios.

- Se recomienda que configure al menos una búsqueda frecuente como pública para cada una de las áreas de asunto definidas en una aplicación IDD.

  Esto permite a los usuarios navegar rápidamente por todas las áreas de asunto sin necesidad de crear sus propias versiones de consultas frecuentes.

Búsqueda sin distinción entre mayúsculas y minúsculas

Dado que la búsqueda ampliada se basa en la capacidad de coincidencia de Informatica MDM Hub, no distingue entre mayúsculas y minúsculas.

En general, la búsqueda que no distingue entre mayúsculas y minúsculas no está disponible para la búsqueda básica. La única excepción es que todos los datos del área de asunto ya estén en mayúsculas o minúsculas. En este caso, la API searchQuery puede configurarse para convertir los términos de búsqueda entrantes en mayúsculas o minúsculas antes de ejecutar la consulta. Para obtener más información, consulte la descripción de SearchQuery en la *Guía del marco de servicios de integración de Multidomain MDM* o el Javadoc.

Paso 6. Configurar el proceso de coincidencia

Configure la manera en la que el proceso de coincidencia identifica los registros duplicados.

El proceso de coincidencia se configura en la ficha **Configuración de coincidencia** del cuadro de diálogo **Área de asunto**. Se puede especificar un conjunto de reglas de coincidencia predeterminado y el tipo de coincidencia. Además, puede seleccionar columnas de coincidencia.
Para obtener más información sobre la configuración de coincidencia, consulte la *Ayuda en línea de Multidomain MDM Data Director Configuration Manager*. Para obtener más información sobre las reglas de coincidencia y los conjuntos de reglas de coincidencia, consulte la *Guía de configuración de Multidomain MDM*.

Paso 7. Configurar los flujos de trabajo de MDM

Puede configurar su aplicación de Data Director (IDD) para utilizar los flujos de trabajo de MDM predefinidos que se implementan al instalar el Servidor ActiveVOS incrustado.

Su paso siguiente depende de si su entorno MDM incluye el Servidor ActiveVOS:

- Si su entorno incluye el Servidor ActiveVOS, seleccione el flujo de trabajo de MDM que desee utilizar como su flujo de trabajo de aprobación.
- Si su entorno no incluye el Servidor ActiveVOS, necesita instalarlo mediante el instalador del servidor del concentrador. Para obtener más información, véase *Guía de instalación de Multidomain MDM*.

Temas relacionados

- "Flujos de trabajo y tareas" en la página 147
- "Configuración manual de IDD" en la página 62

Establecer un flujo de trabajo de aprobación predeterminado para la vista Datos de área de asunto

Cuando los gestores de datos modifican datos principales, pueden enviar la actualización para aprobación haciendo clic en el botón **Enviar para aprobar**. Esta acción abre el cuadro de diálogo Crear tarea. El flujo de trabajo de aprobación predeterminado se muestra en el campo Tipo de tarea.

Antes de modificar el tipo de tarea para establecer un flujo de trabajo de aprobación predeterminado, asegúrese de que no hay tareas en el panel de tareas de IDD.

1. En el Administrador de configuración de IDD, seleccione la aplicación y haga clic en **Editar**.
2. Haga clic en la ficha **Tareas**.
3. En los tipos de tareas, haga clic en el tipo de tarea con el nombre del flujo de trabajo de aprobación que desee utilizar como valor predeterminado y haga clic en **Editar**.
4. Seleccione la casilla **Crear tipo de tarea predeterminado al aprobar** y haga clic en **Aceptar**.

   Nota: Si la casilla está deshabilitada, significa que esta opción está establecida para otro tipo de tarea. Edite los otros tipos de tarea para encontrar el tipo de tarea con esta opción establecida y desmarque la casilla. A continuación, puede establecer la opción en el tipo de tarea de flujo de trabajo preferida.

Actualizar flujos de trabajo para admitir varias acciones de tareas

Los flujos de trabajo ActiveVOS se pueden configurar para que los revisores realicen varias acciones en una tarea sin cerrar la ficha Tarea. Para cada acción de tarea en la que desee admitir varias acciones sin cerrar la ficha Tarea, establezca la propiedad `closeTaskView` en `false`.

1. Abra el diseñador de ActiveVOS.
2. Abra el archivo `.bpel` del flujo de trabajo.
3. Para cada acción de tarea que desee cambiar, edite la definición de acción y establezca el parámetro siguiente:

   ```
   <mdmavxsd:closeTaskView>false</mdmavxsd:closeTaskView>
   ```
4. Implemente el archivo `.bpel` en ActiveVOS.

Paso 8. Configurar la seguridad

Las políticas del administrador de acceso de seguridad (SAM) de MDM Hub configuradas en la Consola del concentrador controlan toda la seguridad de las aplicaciones en Data Director.

Data DirectorEl comportamiento de la aplicación puede ser muy sensible a la configuración de seguridad.

1. Para configurar y probar la aplicación para Data Director, use el usuario administrador o un usuario con todos los privilegios a todos los recursos seguros.

   Para obtener más información, consulte la *Guía de seguridad de Multidomain MDM*.
2. Por cada área de asunto, puede configurar los filtros de seguridad a nivel de filas. De forma predeterminada, no hay filtros de seguridad definidos.

   En la ficha Búsqueda del cuadro de diálogo del área de asunto, puede configurar reglas de seguridad de datos.
3. Para cada usuario determinado, las funciones de usuario asignadas podrían incluir varios filtros de datos.

   Por ejemplo, un usuario podría tener derechos para los registros con una dirección en California mediante una función y derechos para los registros con una dirección en Nueva York mediante otra función.

Temas relacionados

- "Seguridad de datos" en la página 125
- "Configuración de seguridad de IDD" en la página 117

Paso 9. Configurar extensiones de interfaz de usuario

Configure extensiones de interfaz de usuario.

1. Una aplicación IDD se puede personalizar al incrustar contenido externo en la página web e invocar acciones de ubicaciones de la aplicación IDD.

El contenido se puede incrustar mediante:

Elemento	Descripción
Ficha de nivel superior	Se pueden añadir fichas junto a las fichas del Espacio de trabajo Inicio, el espacio de trabajo de datos y el espacio de trabajo de tareas.
Espacio de trabajo Inicio	Se puede añadir un componente o widget al Espacio de trabajo Inicio.
Ficha secundaria en la vista de datos	Se pueden añadir fichas como elementos secundarios de un área de asunto.

2. Se pueden configurar acciones personalizadas para que se invoquen desde elementos de menú en varias ubicaciones de una aplicación IDD.

   Se puede transmitir información contextual al invocar la acción externa.
   La siguiente tabla muestra áreas de una aplicación IDD donde se pueden configurar estas acciones, junto con los datos contextuales disponibles.

Áreas	Datos contextuales disponibles
Área de asunto	rowid_object y datos del objeto principal
Elemento secundario de uno a muchos	rowid_object y datos del elemento secundario
Elemento secundario de muchos a muchos	rowid_object y datos del elemento secundario
Resultados de la búsqueda	rowid_object de los datos seleccionados en la lista de resultados de búsqueda

TEMAS RELACIONADOS

- "Extensiones de interfaz de usuario" en la página 77

Paso 10. Localizar la aplicación

Cuatro conjuntos de paquetes de recursos contienen las cadenas que se muestran en una aplicación IDD.

Cada conjunto incluye los siguientes componentes:

- El archivo predeterminado.
- Un archivo en inglés de marcador de posición. Este archivo puede estar vacío.
- Las versiones localizadas del archivo, si es necesario.

Por ejemplo, para el conjunto MessageBundle, incluye el archivo predeterminado MessageBundle.properties y el archivo en inglés de marcador de posición MessageBundle_en.properties.

Cada archivo de paquete de recursos es un archivo de propiedades con codificación UTF-8. Cada entrada del archivo es un par de nombre y valor, `<nombre>=<valor>`. Ejemplos:

```
title=Business Data Director
locale=Locale
search=Search
```

Para cada entrada:

- <nombre> es un valor fijo al que hace referencia la aplicación IDD y que no se puede modificar.

- <valor> es la parte que se puede localizar.

Para localizar la aplicación:

▶ Utilice el administrador de configuración de IDD para añadir archivos de paquete de recursos a una aplicación IDD, ya sea al incluirlos en el archivo .zip de la aplicación que se importa o al importarlos individualmente en una aplicación IDD existente.

TEMAS RELACIONADOS

- "Componentes de aplicación" en la página 116

CAPÍTULO 4

Administrador de configuración de IDD

Este capítulo incluye los siguientes temas:

Introducción al Administrador de configuración de IDD

El Administrador de configuración de IDD se utiliza para añadir, modificar y administrar aplicaciones IDD.

Una aplicación IDD consta de un archivo de configuración XML, paquetes de recurso, archivos de ayuda y otros componentes. Es posible exportar o importar una aplicación IDD completa como un archivo .zip que contiene todos estos componentes.

El Administrador de configuración de IDD está diseñado para crear y mantener la configuración de una aplicación IDD. Sin embargo, no muestra todas las opciones de configuración disponibles; algunas funciones se deben configurar manualmente, para lo que es necesario exportar y editar directamente el archivo de configuración XML y, a continuación, volver a importarlo al Administrador de configuración de IDD.

Temas relacionados

- "Componentes de aplicación" en la página 116
- "Configuración manual de IDD" en la página 62

Iniciar el administrador de configuración de Informatica Data Director

Para iniciar el administrador de configuración de Informatica Data Director, utilice un navegador web compatible.

1. Abra un navegador web compatible.

   Para obtener información sobre los navegadores web compatibles, consulte la tabla de disponibilidad de productos en el portal My Support de Informatica en https://mysupport.informatica.com/community/my-support/product-availability-matrices.

2. En la barra de direcciones, introduzca la siguiente dirección URL para acceder a la página de inicio de sesión del administrador de configuración de IDD:

   ```
   http://<host de MDM Hub>:<número de puerto>/bdd/config/
   ```

3. Introduzca el nombre de inicio de sesión y la contraseña y, a continuación, haga clic en **Iniciar sesión**.

   Debe iniciar sesión como un usuario que tenga todos los privilegios para todos los objetos base. Para obtener más información acerca de la configuración de los privilegios de usuario, consulte la *Guía de seguridad de Multidomain MDM*.

Se inicia el administrador de configuración de Informatica Data Director y aparece la página de aplicaciones.

Página de inicio

La página de inicio de IDD tiene los siguientes elementos:

Elemento	Descripción
Lista de aplicaciones	Lista de aplicaciones IDD existentes
Barra de comandos	Comandos disponibles (descritos a continuación)
Resumen de la aplicación	Resumen de las aplicaciones IDD existentes que incluye las siguientes propiedades: - Nombre lógico y nombre de visualización - Estado de validación - Estado de implementación - URL para iniciar la aplicación IDD
Tipos de componente	Disponible solo si la característica Componentes de datos de Informatica (IDC) tiene licencia para su implementación de Informatica MDM Hub. Para obtener más información, consulte la *Ayuda en línea de Multidomain MDM Data Director Configuration Manager* y la *Guía de implementación de componentes de datos de Multidomain MDM*.
Configuración del proveedor de inicio de sesión	Acceso directo a la pantalla para configurar el módulo del proveedor de inicio de sesión personalizado (compatibilidad con SSO).

La barra de comandos de IDD contiene los siguientes comandos:

Comando	Descripción
Añadir	Añadir una nueva aplicación IDD.
Editar	Editar la configuración de la aplicación IDD seleccionada.
Eliminar	Eliminar la aplicación IDD seleccionada.
Exportar	Exportar una configuración de aplicación IDD (archivo ZIP).
Validate	Validar la aplicación IDD seleccionada.
Estado de la aplicación	Cambie el estado de implementación de la aplicación IDD: completa, limitada o no implementada.
Importar	Importe la configuración de una aplicación IDD (consulte los formatos a continuación).
Volver a implementar	Quita y vuelve a implementar una aplicación IDD.
Borrar memoria caché	Borra la memoria caché de IDD local de la aplicación IDD seleccionada. Esta memoria caché almacena los metadatos del concentrador y debe borrarse si se han producido cambios en estos metadatos.

La ayuda en línea también está disponible desde cualquier página del Administrador de configuración.

Enlace de ORS

Una configuración de aplicación IDD declara una o más bases de datos de ORS lógico.

Una *base de datos de ORS lógico* es un puntero de configuración de IDD a una base de datos de ORS físico del almacén del concentrador que se configura en la Consola del concentrador. Todos los objetos de Informatica MDM Hub a los que se hace referencia en una configuración se encuentran siempre en el contexto de un ORS lógico determinado. Para que una configuración de IDD sea válida, los objetos a los que hace referencia deben existir en el ORS físico asociado.

Cuando una aplicación IDD se añade o importa, las bases de datos de ORS lógico que declara deben estar enlazadas a un ORS físico registrado con Informatica MDM Hub.

El enlace de ORS se utiliza para conectar una aplicación IDD a un ORS y para validar la configuración. Además, el Administrador de configuración de IDD usa el enlace de ORS para obtener metadatos sobre el ORS.

Añadir una aplicación IDD

El comando Añadir se utiliza para crear una nueva aplicación IDD.

Una nueva aplicación IDD se define por su nombre, nombre de visualización, descripción y lista de bases de datos de ORS lógico. Después de añadir la aplicación, elija el comando Editar para realizar cambios más detallados en la configuración de la aplicación (como añadir áreas de asunto).

Importar una configuración de aplicación IDD

El comando Importar se utiliza para crear o actualizar una aplicación IDD.

Ofrece las siguientes tres opciones de importación; dos para importar una aplicación completa y una para la importación de un componente en una aplicación existente:

Opción de importación	Descripción
Importar solo la configuración de IDD (XML)	Cree una nueva aplicación IDD mediante la importación del archivo XML de configuración de IDD. Esto puede utilizarse para reemplazar una aplicación IDD existente que tenga el mismo nombre. En este caso, la aplicación existente se reemplaza por completo (como si se realizara una eliminación seguida por una importación). Si ya existe una aplicación con el mismo nombre de la nueva aplicación, puede utilizar la opción para importar la aplicación con un nombre diferente. **Nota:** Si reemplaza una aplicación IDD, debe volver a configurar los **Privilegios de recurso** asignados para todas las funciones de la Consola del concentrador.
Importación aplicación IDD completa (ZIP)	Cree una nueva aplicación IDD al importar un archivo .zip que contenga varios archivos de componentes como XML, paquetes de recurso y archivos de ayuda. El tamaño máximo del archivo .zip que puede importar es de 20 megabytes. En entornos de IBM Db2, para importar un archivo de más de 1 megabyte, ejecute el siguiente comando para establecer el tamaño de archivo máximo permitido: `ALTER TABLE CMX_SYSTEM.C_REPOS_DS_CONFIG ALTER COLUMN BLOB_DATA SET DATA TYPE BLOB(`*`tamaño máximo de archivo, bytes`*`);` **Nota:** Si reemplaza una aplicación IDD, debe volver a configurar los **Privilegios de recurso** asignados para todas las funciones de la Consola del concentrador.
Importar a la aplicación IDD existente	Actualice una aplicación IDD existente mediante la importación de un archivo individual. Esto se utiliza para añadir o reemplazar cualesquiera de los archivos de componente de la aplicación IDD. **Nota:** También puede usar esta opción al promover cambios de un entorno a otro.

Temas relacionados

- "Componentes de aplicación" en la página 116

Validación, estado de la aplicación e implementación

Los siguientes parámetros persistentes determinan si se implementa una aplicación IDD y cómo se implementa.

Parámetro	Descripción
valid_ind	Contiene el último estado de validación de la aplicación. El estado de validación es un valor único que representa el error mayor (más grave) que se ha encontrado.
active_ind	Parámetro administrado directamente por el usuario para reflejar la intención de implementar la aplicación.

Validación

La configuración de aplicación IDD está acoplada ligeramente a los metadatos en un ORS.

La configuración contiene referencias a objetos de un ORS. Los cambios en un ORS (la suma, modificación o eliminación de objetos base, columnas, funciones de limpieza, etc.) no se reflejan automáticamente en la configuración de IDD. Por este motivo, el proceso de validación de IDD es necesario y debe repetirse periódicamente.

La validación se ejecuta en las siguientes circunstancias:

- cuando el usuario lo solicita en el Administrador de configuración de IDD
- Al importar una configuración de IDD.
- antes de implementar una aplicación cuando se ha iniciado el servidor de aplicaciones

Los niveles de validación disponibles son los siguientes.

valid_ind	Nivel de validación	Descripción
-1	No validado	La aplicación IDD no se ha validado.
0	No hay errores	No se han encontrado errores ni advertencias durante la validación.
1	Información	Proporciona información al usuario. No se requieren cambios en la configuración.
2	Advertencia	Es posible que deba cambiarse una configuración, pero no provocaría problemas de tiempo de ejecución.
3	Error	Debe corregirse un error de configuración. Se podrían esperar problemas de tiempo de ejecución.
4	Error crítico	Igual que Error, pero indica un problema que requiere una atención más urgente.
5	Error fatal	Un error que impide que la aplicación IDD se ejecute de ningún modo. La aplicación no se implementará en ninguna circunstancia.

Estado de la aplicación

El usuario controla el estado de la aplicación en el Administrador de configuración de IDD.

Almacena la implementación prevista para la aplicación IDD.

Nota: Las aplicaciones IDD se pueden implementar incluso si la configuración contiene errores. Solo los errores fatales (descritos en la sección anterior) impedirán que se implemente una aplicación IDD. Puede ser

útil implementar una aplicación IDD que contenga errores al compilar una aplicación, ya que así el implementador podrá probar partes de la configuración mientras otras partes están incompletas.

active_ind	Nombre	Descripción
-1	No se ha implementado	La aplicación IDD no está implementada. Útil cuando la aplicación está en desarrollo. Los cambios se pueden realizar y guardar sin la sobrecarga adicional de implementar la aplicación.
0	Implementación limitada	La aplicación IDD está implementada, pero solo los usuarios que son administradores pueden iniciar sesión. La aplicación no se mostrará en la lista de aplicaciones disponibles. Debe poder acceder a la aplicación a través de su URL completa: `http://<hostname>[:<port>]/bdd?bdd_name=name`
1	Implementación completa	La aplicación IDD está implementada para su uso completo. La aplicación se muestra en la lista de aplicaciones y todos los usuarios autorizados pueden ejecutar la aplicación.

Implementación

La implementación es el proceso mediante el que una configuración de IDD pasa a estar disponible como aplicación.

Una aplicación no se implementará si active_ind es -1 para esa aplicación.

La implementación se produce como respuesta a los siguientes eventos:

Eventos	Descripción
Inicio del servidor de aplicaciones	Todas las aplicaciones IDD en las que active_ind no sea -1 se validarán primero. Si el nivel de validación no es Error fatal, la aplicación IDD se implementa. En este momento solo se ejecuta una validación parcial para comprobar si hay errores fatales.
Importar/guardar	Cada vez que se importa o guarda una aplicación IDD, también se implementa, a menos que su active_ind sea -1.
Nueva implementación	El usuario vuelve a implementar una aplicación IDD.

Editar aplicación

En la pantalla Editar aplicación, puede ver y editar los detalles de la configuración para una aplicación IDD seleccionada. IDD utiliza metadatos de ORS lógico para presentar las opciones de configuración disponibles.

En la parte inferior de la pantalla, están disponibles las siguientes fichas:

Ficha	Descripción
Áreas de asunto	Defina grupos de área de asunto, áreas de asunto, elementos secundarios de áreas de asunto y elementos secundarios de segundo nivel para la aplicación IDD seleccionada.
Tareas	Defina tareas para la aplicación IDD seleccionada. Para obtener más información, consulte la ayuda en línea del Administrador de configuración.
Controles	Disponible solo si su implementación de MDM Hub dispone de licencia para la característica Componentes de datos de Informatica (IDC). Para obtener más información, consulte *Ayuda en línea de Multidomain MDM Data Director Configuration Manager* y *Guía de implementación de componentes de datos de Multidomain MDM*.

Los siguientes botones de comandos también están disponibles:

Botón	Descripción
Guardar	Guarda los últimos cambios de la base de datos. Si el estado de la aplicación no es No se ha implementado (-1), la aplicación IDD se volverá a implementar después de guardar los cambios.
Validar	Ejecuta la validación en la configuración de la aplicación IDD y muestra el informe de validación.
Enlace	Se utiliza para cambiar el enlace de ORS lógico.
Generar esquema de entidades de negocio	Genera archivos de configuración para todas las entidades de negocio de la aplicación IDD.

Temas relacionados

- "Áreas de asunto" en la página 47

Bases de datos de ORS lógico

Al editar una configuración, la primera tarea que se debe realizar es configurar las bases de datos de ORS lógico.

Para cada una de estas bases de datos de ORS, debe seleccionar un sistema de origen.

Si la aplicación IDD va a usar el Administrador de jerarquía, también se deberá seleccionar la configuración de HM. El icono a la derecha del menú desplegable de configuración de HM incluye valores de parámetros de HM adicionales (como valores de saltos y de relación).

Nota: En el Administrador de configuración de IDD, en la ventana **Configuración de HM**, el valor de **Número total de relaciones** no debe ser superior a 2000.

Tiempo de espera de la sesión

En la pantalla Editar aplicación, puede establecer un tiempo de espera de sesión para una aplicación de IDD seleccionada.

Para establecer el tiempo de espera de la sesión, introduzca un valor en minutos en el campo **Tiempo de espera de la sesión**. A continuación, guarde la aplicación de IDD. De forma predeterminada, una sesión supera el tiempo de espera al cabo de 30 minutos.

Si cambia el valor del tiempo de espera de la sesión, todas las sesiones activas en IDD no serán válidas y los usuarios tendrán que volver a iniciar la sesión.

Áreas de asunto

La ficha Áreas de asunto de la parte inferior de la pantalla proporciona un árbol que muestra cómo se configura la aplicación IDD.

A medida que se seleccionan elementos en el árbol, se actualizan los botones Agregar, Editar y Eliminar para reflejar las opciones disponibles. Los niveles del árbol son los siguientes:

Nivel de árbol	Descripción
Aplicación IDD	Se pueden añadir grupos de área de asunto.
Grupo de área de asunto	El grupo de área de asunto se puede editar o eliminar. Se pueden añadir áreas de asunto. El grupo de área de asunto identifica a qué ORS lógico pertenecen las áreas de asunto secundarias y qué objeto base es la tabla principal para esas áreas de asunto. Un grupo de área de asunto puede tener una o más áreas de asunto secundarias que comparten la misma tabla principal. Estas áreas de asunto se agrupan en la aplicación IDD.
Área de asunto	El área de asunto se puede editar o eliminar. Se pueden añadir elementos secundarios de área de asunto. Si el grupo de área de asunto contiene más de un área de asunto, cada área de asunto define el calificador de tipo o de subtipo de entidad de HM que identifica el área de asunto. También puede especificar: - El paquete utilizado para mostrar los resultados de búsqueda - El conjunto de reglas de coincidencia y el tipo de coincidencia para utilizar en las comprobaciones de duplicados - Las columnas de la tabla principal que forman parte de este área de asunto
Elemento secundario del área de asunto	El elemento secundario de área de asunto se puede editar o eliminar. Para cada elemento secundario de área de asunto, debe especificar lo siguiente: - el tipo de relaciones (uno a muchos, muchos a muchos, etc.); - la ruta de coincidencia que dirige a la tabla secundaria (la lista de rutas de coincidencia se completa según el tipo de relación seleccionado); - las columnas de la tabla secundaria que se van a mostrar.
Elemento secundario de segundo nivel del área de asunto	El elemento secundario de segundo nivel de área de asunto se puede editar o eliminar. Para cada elemento secundario de segundo nivel de área de asunto, debe especificar lo siguiente: - el tipo de relación (uno a muchos, muchos a muchos, etc.); - la ruta de coincidencia que dirige a la tabla secundaria (la lista de rutas de coincidencia se completa según el tipo de relación seleccionado); - las columnas de la tabla secundaria que se van a mostrar.

Propiedades de grupos de área de asunto

El cuadro de diálogo utilizado para añadir y editar un grupo de área de asunto se usa para configurar lo siguiente:

- Nombre y nombre de visualización. El nombre es el identificador interno para esta área de asunto y solo debe contener caracteres alfanuméricos. No se permiten caracteres especiales.
- El ORS lógico al que está enlazado el grupo de área de asunto.
- Tabla principal para las áreas de asunto del grupo:

Característica	Descripción
Nombre y nombre de visualización.	Se utiliza para identificar el grupo de área de asunto. El nombre es el identificador interno para este grupo de área de asunto y solo debe contener caracteres alfanuméricos. No se permiten caracteres especiales.
ORS lógico	Configura el ORS lógico del que proceden los objetos de este grupo de área de asunto.
Tabla principal	Configura qué objeto base es la tabla principal o raíz para las áreas de asunto del grupo de área de asunto.
Buscar solo	Esta opción se selecciona para un grupo de área de asunto que contiene datos creados y mantenidos fuera de una aplicación IDD. Las áreas de asunto definidas en este grupo solo se pueden ver en una aplicación IDD al crear una clave externa desde otra área de asunto (la búsqueda se utiliza para encontrar el registro que relacionar).

Propiedades de áreas de asunto

El cuadro de diálogo utilizado para añadir y editar un área de asunto se usa para configurar las siguientes propiedades:

- Nombre y nombre de visualización: El nombre es el identificador interno para esta área de asunto y solo debe contener caracteres alfanuméricos. No se permiten caracteres especiales. Un nombre de área de asunto no puede empezar por un número.
- Tipo de entidad de HM: Esta propiedad define los tipos de objetos que se pueden relacionar, si los hubiera.
- Paquete de visualización de resultados de búsqueda: Esta propiedad se utiliza para mostrar los resultados de búsqueda para esta área de asunto. El paquete debe tener la tabla principal del grupo de área de asunto como su tabla principal.
- Columnas de vínculos de coincidencias potenciales: Esta propiedad define qué columna de un diseño debe mostrarse como un hipervínculo que abre una entidad de coincidencia potencial en una nueva ficha de vista de datos.
- Columna de subtipo: Esta propiedad especifica la columna utilizada para el filtro de subtipos: Código de tipo (categoría) de este área de asunto. Se establece automáticamente si se selecciona un tipo de entidad de HM.
- Valor de subtipo: Esta propiedad especifica el valor utilizado para el filtro de subtipos. Se establece automáticamente si se selecciona un tipo de entidad de HM.
- Número de columnas inmovilizadas: Esta propiedad muestra el número de columnas inmovilizadas en los resultados de búsqueda para el área de asunto.
- Mostrar XREF: Si se selecciona, la aplicación IDD muestra una ficha secundaria para el área de asunto que muestra las referencias cruzadas para el objeto principal.

- Fichas para configurar los siguientes valores:

Característica	Descripción
Diseño	Configura las columnas del objeto base que están disponibles en la aplicación IDD para su visualización y edición, el tipo de componente de interfaz de usuario que se va a utilizar y, si es una búsqueda, si los datos de búsqueda están localizados.
Configuración de coincidencia	Configura el conjunto de reglas de coincidencia y el tipo de coincidencia para utilizar en las comprobaciones de duplicados.
Buscar	Configura las propiedades de búsqueda.
Seguridad de datos	Configura la seguridad basada en funciones a nivel de fila para el área de asunto.
Enmascaramiento de datos	Configura el enmascaramiento de datos basado en funciones para las columnas seleccionadas en la ficha Diseño.
Limpieza	Configura la función de limpieza que se va a utilizar para la limpieza y la validación.
Etiqueta	Configura la forma en que se genera una etiqueta para el área de asunto. Esta etiqueta se utiliza, por ejemplo, como el título de una ficha de vista de datos.
Asignación de tareas	Configura cómo se asignan las tareas. Especifica la lista de funciones y el usuario para cada tipo de tarea.
Orden de elementos secundarios	Configura el orden de las fichas secundarias para el área de asunto.

Propiedades de elementos secundarios y elementos secundarios de segundo nivel del área de asunto

El cuadro de diálogo utilizado para añadir y editar un área de asunto se usa para configurar las siguientes propiedades:

- Nombre y nombre de visualización. El nombre es el identificador interno para un elemento secundario o elemento secundario de segundo nivel de área de asunto y solo debe contener caracteres alfanuméricos. No se permiten caracteres especiales.
- Tipo de elemento secundario: el tipo de relación con el elemento principal.
- Ruta de coincidencia al elemento secundario: el componente de la ruta de coincidencia que dirige a este objeto secundario.

- Fichas para configurar los siguientes valores:

Característica	Descripción
Diseño	Configura las columnas del objeto base que están disponibles en la aplicación IDD para su visualización y edición, el tipo de componente de interfaz de usuario que se va a utilizar y, si es una búsqueda, si los datos de búsqueda están localizados. **Nota:** Esta configuración no se aplica a los filtros de registros secundarios. Todas las columnas están disponibles para los filtros.
Enmascaramiento de datos	Configura el enmascaramiento de datos basado en funciones para las columnas seleccionadas en la ficha Diseño.
Limpieza	Configura las funciones de limpieza que se van a utilizar para la limpieza y la validación.

TEMAS RELACIONADOS

- "Localización de búsqueda" en la página 50
- "Paso 4. Configurar la limpieza y la validación" en la página 33

Localización de búsqueda

Una aplicación de Informatica Data Director rellena una lista desplegable de valores aceptables para columnas que debe configurar como búsquedas en el administrador de esquema. Para crear búsquedas localizadas, se necesita una tabla de localización. Cuando crea una búsqueda, utilice un nombre para mostrar único. Informatica Data Director no puede distinguir las búsquedas con distintos códigos que comparten el mismo nombre para mostrar.

Informatica Data Director también admite la localización de los valores de búsqueda de visualización de búsqueda. Puede configurar valores de visualización de búsqueda en la ficha Diseño del Administrador de configuración de Informatica Data Director para áreas de asunto y elementos secundarios de áreas de asunto.

Por ejemplo, un Almacén de referencias operativas tiene las siguientes tablas:

- C_PARTY
- C_LU_SALUTATION
- C_LCL_SALUTATION

La tabla C_PARTY tiene un código de búsqueda de tratamiento configurado en la tabla C_LU_SALUTATION. Para cada código de tratamiento, el nombre para mostrar puede tener un valor localizado configurado en la tabla C_LCL_SALUTATION.

Para generar la lista de valores para la configuración regional de un usuario determinado, Informatica Data Director primero busca un nombre de búsqueda en C_LCL_SALUTATION basado en la configuración regional. Si Informatica Data Director no encuentra un nombre de búsqueda en C_LCL_SALUTATION, utilizará el nombre de búsqueda de la tabla de búsquedas de SALUTATION_DISP.

Nota: La configuración regional está determinada por el código de idioma y país. Los valores de código de idioma y país son códigos ISO de dos letras.

La configuración para el escenario anterior especifica que la columna tiene valores de búsqueda localizados, así como la tabla y las columnas que se utilizan. El siguiente XML de ejemplo muestra la configuración del ejemplo anterior:

```
<column columnUid="C_PARTY|SALUTATION_CODE"
        editStyle="FIELD"
```

```
        horizontalStyle="SMALL">
    <columnI18NLookup languageCdUid="C_LCL_SALUTATION|LANGUAGE_CODE"
                      countryCdUid="C_LCL_SALUTATION|COUNTRY_CODE"
                      lookupFKUid="C_LCL_SALUTATION|SALUTATION_CODE"
                      localizedNameUid="C_LCL_SALUTATION|LOCALIZED_STRING"/>
</column>
```

TEMAS RELACIONADOS

- "Tablas de búsqueda" en la página 24
- "Códigos de configuración regional" en la página 165
- "Configuración manual de IDD" en la página 62

Importar una plantilla de importación de datos

Un desarrollador de la aplicación Informatica Data Director (IDD) puede configurar una aplicación IDD de manera que permita a los usuarios autorizados importar datos de un archivo de origen. El gestor de datos crea una plantilla de importación de datos, que se importa a la configuración de la aplicación IDD.

Nota: La importación de datos está disponible para aplicaciones IDD que implementan el modelo de datos de área de asunto y las vistas de IDD heredadas.

Para obtener más información sobre la importación de datos, consulte la *Guía del usuario de Multidomain MDM Data Director*.

Importar la plantilla de importación de datos

En IDD Configuration Manager, un administrador de MDM importa la plantilla de importación de datos en la aplicación Data Director (IDD). El proceso de importación valida la plantilla.

1. Inicie sesión en el administrador de configuración de IDD.
2. Seleccione la aplicación.
3. Haga clic en **Importar** > **Importar a la aplicación IDD existente**.

   Se abrirá la ventana **Importar a la aplicación IDD existente**.
4. En la lista **Tipo de configuración**, seleccione **Plantilla de importación de datos**.
5. Haga clic en **Examinar** y seleccione el archivo XML que contiene la plantilla de importación de datos.
6. Haga clic en **Importar**.

   El proceso de importación valida la plantilla. Se abrirá la ventana **Resultado de la validación** que muestra los errores que se hayan producido.
7. Si existen errores de validación, corríjalos en la plantilla y vuelva a importarla.
8. En la ventana **Resultado de la validación**, haga clic en **Aceptar**.

Paquete del proveedor de inicio de sesión personalizado

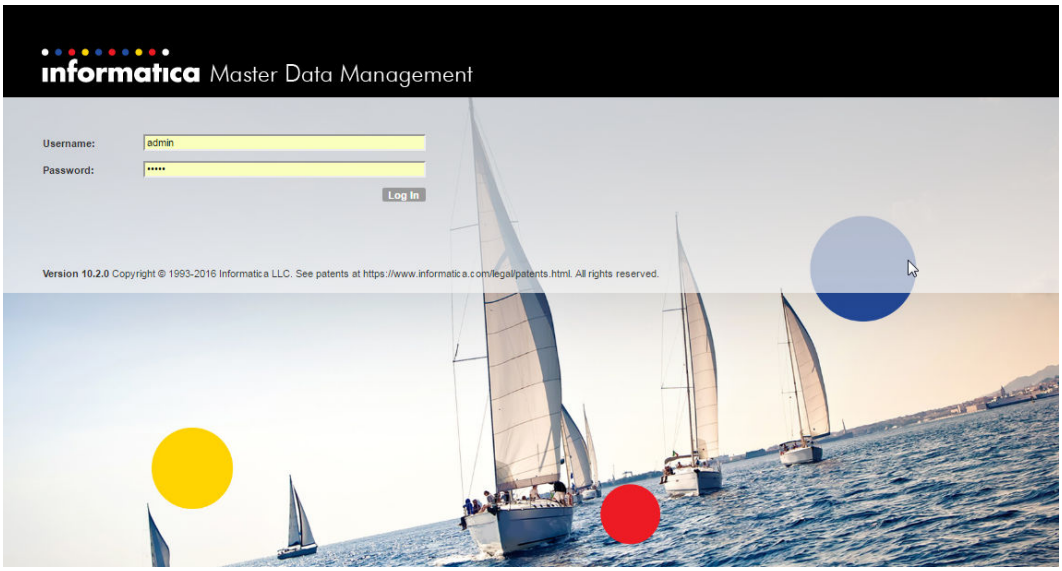
El paquete del proveedor de inicio de sesión personalizado es un archivo de almacenamiento que contiene clases Java. Puede utilizar Informatica Data Director Configuration Manager para cargar el archivo de almacenamiento. El paquete del proveedor de inicio de sesión personalizado debe estar en un archivo ZIP.

En el marco de Entidad 360, el paquete del proveedor de inicio de sesión personalizado debe estar en un archivo ZIP que contenga lo siguiente:

- Carpeta META-INF. Esta carpeta contiene el archivo MANIFEST.MF, que tiene una entrada Login-Provider-Class-Name que contiene el nombre de una clase que implementa la interfaz de LoginProvider.
- Archivo JAR con implementación de proveedor de inicio de sesión personalizado.
- Otros archivos JAR que contienen dependencias para la implementación del proveedor de inicio de sesión personalizado, como clases de utilidades, registros y bibliotecas de terceros.

Puede configurar el paquete del proveedor de inicio de sesión personalizado para que utilice el formulario de inicio de sesión de Informatica Data Director o el formulario de inicio de sesión de un proveedor de identidad externo, como Google o Salesforce.

La imagen siguiente muestra el formulario de inicio de sesión de Informatica Data Director:



Si no carga un paquete del proveedor de inicio de sesión personalizado, la implementación predeterminada de Informatica Data Director autentica a los usuarios con las credenciales almacenadas en la base de datos principal de MDM Hub.

Paquetes del proveedor de inicio de sesión personalizado en el kit de recurso

El kit de recurso contiene ejemplos de paquetes del proveedor de inicio de sesión que puede utilizar con la aplicación Informatica Data Director. Estos paquetes de inicio de sesión de inicio de sesión único se almacenan como archivos JAR y ZIP. Los administradores de bases de datos y otros miembros técnicos de un equipo de implementación de MDM pueden utilizar estos archivos para crear sus propios paquetes del proveedor de inicio de sesión personalizados.

Los archivos del paquete de inicio de sesión único de ejemplo se encuentran en el siguiente directorio:

`<directorio de instalación de infamdm>/hub/resourcekit/samples/sso`

Cargar el paquete del proveedor de inicio de sesión personalizado

Para cargar el paquete del proveedor de inicio de sesión personalizado, utilice el Informatica Data Director Configuration Manager.

1. Desde el panel de navegación en el Informatica Data Director Configuration Manager, haga clic en **Configuración del proveedor de inicio de sesión**.
2. Desde el panel **Configuración del proveedor de inicio de sesión**, haga clic en **Editar**.
3. Desde el cuadro de diálogo **Editar la configuración del proveedor de inicio de sesión**, haga clic en **Examinar**.
4. Seleccione el archivo de almacenamiento del proveedor de inicio de sesión personalizado y, a continuación, haga clic en **Aceptar**.
5. Escriba el nombre del archivo ZIP con la implementación de la clase del proveedor de inicio de sesión en el campo Archivo de implementación del proveedor de inicio de sesión.

   Debe esperar hasta que el archivo ZIP termine de cargarse en el servidor.
6. Introduzca el nombre de la clase que implementa `com.siperian.bdd.security.LoginProvider` en el campo Nombre de clase del proveedor de inicio de sesión.

   Este es el nombre completo de la clase que implementa LoginProvider.
7. Haga clic en **Aceptar**.

   IDD valida el archivo ZIP que se ha cargado y crea una instancia de la clase del proveedor de inicio de sesión especificada.

Bibliotecas de otros fabricantes

En IDD, podría usar un proveedor de inicio de sesión personalizado con bibliotecas de terceros. Sin embargo, en el marco de Entidad 360, todas las bibliotecas de terceros deben empaquetarse en el mismo archivo ZIP que el paquete del proveedor de inicio de sesión personalizado.

Implementar proveedor de inicio de sesión personalizado

El proveedor de inicio de sesión personalizado es una clase Java que implementa la interfaz de LoginProvider (`com.siperian.bdd.security.LoginProvider`) que se define en IDD. Admite el mecanismo de autenticación de inicio de sesión único (SSO).

El proveedor de inicio de sesión trabaja con el módulo de inicio de sesión del concentrador. Todos los datos que requiere el módulo de inicio de sesión del concentrador para la verificación del usuario autenticado deben transferirse desde el proveedor de inicio de sesión como un campo de matriz de byte `securityPayload` de clase `com.siperian.bdd.security.LoginCredentials`. Este campo se transfiere tal cual del proveedor de inicio de sesión al módulo de inicio de sesión del concentrador y contiene información codificada específica de la implementación acerca de los usuarios.

Proveedor de inicio de sesión personalizado con formulario de inicio de sesión externo

Si un mecanismo de autenticación determinado requiere una página de inicio de sesión que no sea de IDD, la implementación del proveedor de inicio de sesión personalizado debe utilizar los métodos de interfaz indicados y descritos en la tabla siguiente:

Nombre de método de interfaz	Descripción
initialize	IDD llama a este método antes que a cualquier otro método de la implementación del proveedor de inicio de sesión y transfiere un conjunto de propiedades que describen el contexto de ejecución. En IDD, estas propiedades contienen una entrada, que puede referenciarse como LoginProvider. La propiedad SSO_POST_REDIRECT_PAGE_PROPERTY contiene la URL de la página jsf que puede publicar los datos mediante el método POST en el proveedor de inicio de sesión externo. La implementación de un proveedor de inicio de sesión puede utilizar esta página para redirigir IDD a la página de inicio de sesión externo usando el método POST.
isUseIDDLoginForm	Este método debe devolver FALSE.
redirectToProviderLoginPage	Este método debe crear la URL al formulario de inicio de sesión externo y redirigir a esa página. También puede redirigir a una página de inicio de sesión externo mediante el método POST.
extractLoginCredentials	IDD invoca este método cuando se recibe una nueva solicitud de autenticación de usuario. Si la solicitud contiene información del proveedor de identidad externo, como los parámetros de la solicitud y las cookies, este método debe extraerla y devolver la instancia de LoginCredentials (com.siperian.bdd.security.LoginCredentials) con los campos debidamente completados. Si la solicitud no contiene información de autenticación, el método debe devolver NULL.
encodeComponentUrl	Este método no se implementa debido a que un formulario de inicio de sesión externo que IDD no reconoce solicita el nombre de usuario y la contraseña.
onLogout	Cuando un usuario cierra la sesión, se llama a este método. Puede ejecutar un cierre de sesión en un proveedor de identidad externo, así como parámetros de limpieza definidos por el método requestLoginCredentials.
getLogoImageBody	Este método debe devolver NULL.

Tras iniciar sesión correctamente, se le dirige a la página principal de IDD o a la página de componentes de Informatica Data Controls (IDC), según su solicitud inicial.

Asimismo, puede omitir la autenticación externa mediante el parámetro `internal_login_form=true` de la URL de IDD que muestra el inicio de sesión de IDD.

Por ejemplo:

```
http://localhost:8080/bdd?internal_login_form=true
```

En este caso, el nombre de usuario y la contraseña se comprueban con la lista de usuarios de MDM Hub.

Pasar credenciales a vínculo externo

Si necesita integrar vínculos externos en IDD y los vínculos utilizan el mismo proveedor de SSO (por ejemplo, SalesForce.com) que el proveedor de inicio de sesión personalizado instalado, utilice este método para

añadir información de autenticación a la URL del vínculo. Si no se añade información, el método debe devolver la misma cadena de URL que se le ha pasado como parámetro o valor nulo.

Ejemplo:

Suponga que implementa LoginProvider para trabajar con SalesForce.com.

También define el vínculo externo con la URL `https://na7.salesforce.com/home/home.jsp` para ver la página de inicio de la cuenta de SalesForce.com integrada en la pantalla de IDD.

El método encodeComponentUrl recibe esta URL y la convierte en lo siguiente:

```
https://na7.salesforce.com/secur/frontdoor.jsp?sid=<SFDC_API_SESSIONID>&retUrl=https://
na7.salesforce.com/home/home.jsp
```

Después de esta transformación, un IFrame de la página de IDD muestra la página de inicio solicitada sin redireccionar al formulario de inicio de sesión de SalesForce.

Usar una página POST

IDD emplea la página POST para redirigir a los usuarios a una página de inicio de sesión externa. Esta página se envía después de que se cargue en el cliente.

El origen de la página utiliza la variable predefinida JSF requestScope para acceder a los parámetros descritos en la tabla siguiente:

Nombre del parámetro	Uso
providerGateURL	Debe ser un valor de cadena. Define la URL a la que se enviará el formulario (acción de formulario).
authParameters	Es una asignación de pares de clave-valor. Cada par de valores se utiliza para crear una entrada oculta. La clave de entrada de asignación se utiliza como nombre de entrada y el valor como valor del campo de entrada.

En el siguiente ejemplo, la variable postRedirectPageUrl se configura durante una llamada a un método initialize:

```
public void redirectToProviderLoginPage(HttpServletRequest httpRequest,
                                        HttpServletResponse httpResponse,
                                        String returnUrl) throws LoginProviderException {
RequestDispatcher dispatcher =
                  httpRequest.getRequestDispatcher(postRedirectPageUrl);
httpRequest.setAttribute( PROVIDER_GATE_URL_ATTR, authReq.getOPEndpoint() );
httpRequest.setAttribute( AUTH_PARAMETERS_ATTR, authReq.getParameterMap() );
dispatcher.forward( httpRequest, httpResponse );
}
```

Para enviar una redirección a la nueva página durante el cierre de la sesión, puede añadir el siguiente código al método redirectToProviderLoginPage():

```
if("gotoLogoutPage".equalsIgnoreCase(httpRequest.getParameter("logoutParam"))){
    try
        { httpResponse.sendRedirect("http://www.google.com/"); }
        catch (Exception e)
        { // TODO Auto-generated catch block e.printStackTrace(); }
}
```

El método onLogout() escribe código en la respuesta, como se muestra en el siguiente ejemplo:

```
{\"logoutURL\":\"/mdm/entity360view/?logoutParam=gotoLogoutPage\",\"kerberos\":\"true\"}
```

Configurar E360 para enviar solicitudes POST a un servicio web

En ocasiones, un proveedor de inicio de sesión personalizado utiliza servicios web que esperan una solicitud POST. Entidad 360 incluye un servlet que envía solicitudes POST. Para configurar el servlet para que envíe una solicitud POST a un servicio web de terceros, introduzca la URL a la que enviar la solicitud POST en el método `redirectToProviderLoginPage`.

1. Utilice un editor de texto para modificar la implementación del proveedor de inicio de sesión personalizado.
2. En las propiedades transferidas al método `initialize` del proveedor de inicio de sesión personalizado, copie la URL del servlet.
3. En el método `redirectToProviderLoginPage`, cree una solicitud.
   a. En el atributo `AuthParameters`, defina los parámetros con pares de nombre–valor.

      Los pares de nombre–valor conforman el cuerpo de la solicitud POST.

   b. En el atributo `ProviderGateURL`, introduzca la URL a la que se envía la solicitud POST.

      Nota: Asegúrese de que la URL termina con una barra diagonal (“/”). De lo contrario, la aplicación E360 genera una excepción de puntero nulo.

El código siguiente muestra una solicitud de ejemplo en una implementación de proveedor de inicio de sesión personalizado:

```
    @Override
    public void redirectToProviderLoginPage(javax.servlet.http.HttpServletRequest
request,
            javax.servlet.http.HttpServletResponse response, String originalRequest)
throws
    LoginProviderException {
        RequestDispatcher dispatcher = request.getRequestDispatcher(forwardUrl);

        Map<String, String> params = new HashMap<>();

        params.put("param1", “value1”);
        params.put("param2", “value2”);

        request.setAttribute(“AuthParameters”, params);
        request.setAttribute(“ProviderGateURL”, “http://external.server.com/”);

        dispatcher.forward(request, response);
}
```

Proveedor de inicio de sesión personalizado con formulario de inicio de sesión de IDD

Si el mecanismo de autenticación utiliza el formulario de inicio de sesión de IDD para solicitar el nombre de usuario y la contraseña, la implementación del proveedor de inicio de sesión personalizado debe utilizar los métodos de interfaz que se describen en la tabla siguiente:

Nombre de método de interfaz	Descripción
initialize	IDD llama a este método antes que a cualquier otro método de la implementación del proveedor de inicio de sesión y transfiere un conjunto de propiedades que describen el contexto de ejecución. En IDD, las propiedades contienen la única entrada. Se puede hacer referencia a esta entrada como LoginProvider. SSO_POST_REDIRECT_PAGE_PROPERTY contiene la URL de la página JSF que puede publicar los datos mediante el método POST en el proveedor de inicio de sesión externo.
isUseIDDLoginForm	Este método debe devolver TRUE.
redirectToProviderLoginPage	Este método no se utiliza.
extractLoginCredentials	Este método extrae las credenciales de usuario de una solicitud HTTP. Si la solicitud contiene información de autenticación, este método debe devolver la instancia de LoginCredentials (`com.siperian.bdd.security.LoginCredentials`) con los campos debidamente completados. Si la solicitud no contiene información de autenticación, el método debe devolver NULL.
requestLoginCredentials	Después de que un usuario envíe el formulario de inicio de sesión completado, se llama a este método. Este método se utiliza para enviar solicitudes a un proveedor de identidad externo para la autenticación de usuarios. Si la autenticación se realiza correctamente, se devuelven instancias de LoginCredentials debidamente completadas. Si se produce un error durante la autenticación, se lanza la excepción `com.siperian.bdd.security.LoginProviderException`.
encodeComponentUrl	Este método recibe la URL ExternalLink y puede añadir parámetros de autenticación.
onLogout	Cuando un usuario cierra la sesión, se llama a este método. Puede ejecutar un cierre de sesión en un proveedor de identidad externo, así como en parámetros de limpieza definidos por el método `requestLoginCredentials`.
getLogoImageBody	Este método devuelve InputStream con el cuerpo del archivo de imagen. Puede utilizar este método para mostrar el logotipo de un proveedor de identidad externo en el formulario de inicio de sesión de IDD. El formato de imagen debe ser PNG, JPEG o GIF. La imagen no debe superar un ancho de 155 píxeles y una altura de 29 píxeles. Si este método devuelve NULL, IDD utiliza la imagen predefinida para indicar que el proveedor de inicio de sesión personalizado administra el formulario de inicio de sesión.

Compilar biblioteca del proveedor de inicio de sesión

La clase LoginProvider y todas las clases de IDD que se necesitan para compilar la implementación del proveedor de inicio de sesión personalizado están empaquetadas en el archivo `siperian-bdd.jar`. Este archivo está incluido en el kit de recurso de MDM, que también contiene ejemplos de implementación de LoginProvider. Para obtener más información, consulte *Guía del kit de recursos de Multidomain MDM*.

Configurar la autenticación de SSO de SalesForce (WebLogic)

Si necesita configurar la autenticación de SSO de SalesForce para IDD, se debe deshabilitar la verificación del nombre de host en WebLogic. Puede deshabilitar la verificación del nombre de host con el siguiente procedimiento:

1. Abra la Consola de administración del servidor WebLogic e inicie sesión.
2. Expanda **Entorno** y seleccione **Servidores**.
3. Haga clic en el nombre del servidor que ejecuta el concentrador (AdminServer es el servidor predeterminado).
4. En la página Configuración, haga clic en la ficha **SSL**.
5. Haga clic en **Avanzadas** en la parte inferior de la página.
6. Establezca el campo Verificación de nombre de host en **Ninguna**.
7. Haga clic en **Guardar**.
8. Reinicie el servidor WebLogic.

Configurar la autenticación de SSO de SalesForce (WebSphere)

Si necesita configurar la autenticación de SSO de SalesForce para IDD, se debe configurar WebSphere para que confíe en el servidor de SalesForce. Debe recuperar los certificados del firmante del host de SalesForce al que intenta conectarse y añadirlos al almacén de confianza de WebSphere con el siguiente procedimiento:

1. Abra la Consola de administración de WebSphere e inicie sesión.
2. Expanda **Seguridad** y haga clic en **Certificado SSL y administración de claves** > **Administrar configuraciones de seguridad de punto final**.
3. Expanda **Saliente** y haga clic en **HTTP**.
4. Seleccione **Almacenes de claves SSL** de la lista desplegable.
5. Haga clic en **NodeDefaultTrustStore** > **Certificados del firmante**.
6. Haga clic en **Recuperar del puerto**.
7. Introduzca los siguientes valores en los campos **Host**, **Puerto** y **Alias**:
   - Host: `www.salesforce.com`
   - Puerto: `443`
   - Alias: `www.salesforce.com`
8. Haga clic en **Recuperar información del firmante**.

   Se mostrarán los datos del certificado.
9. Haga clic en **Aplicar**.
10. Repita los pasos 6 a 9 para los siguientes hosts:
    - na10-api.salesforce.com
    - c.na10.visual.force.com
11. Haga clic en **Guardar**.
12. Reinicie el servidor WebSphere.

Ejemplo de implementación de proveedor de inicio de sesión del inicio de sesión único de Google

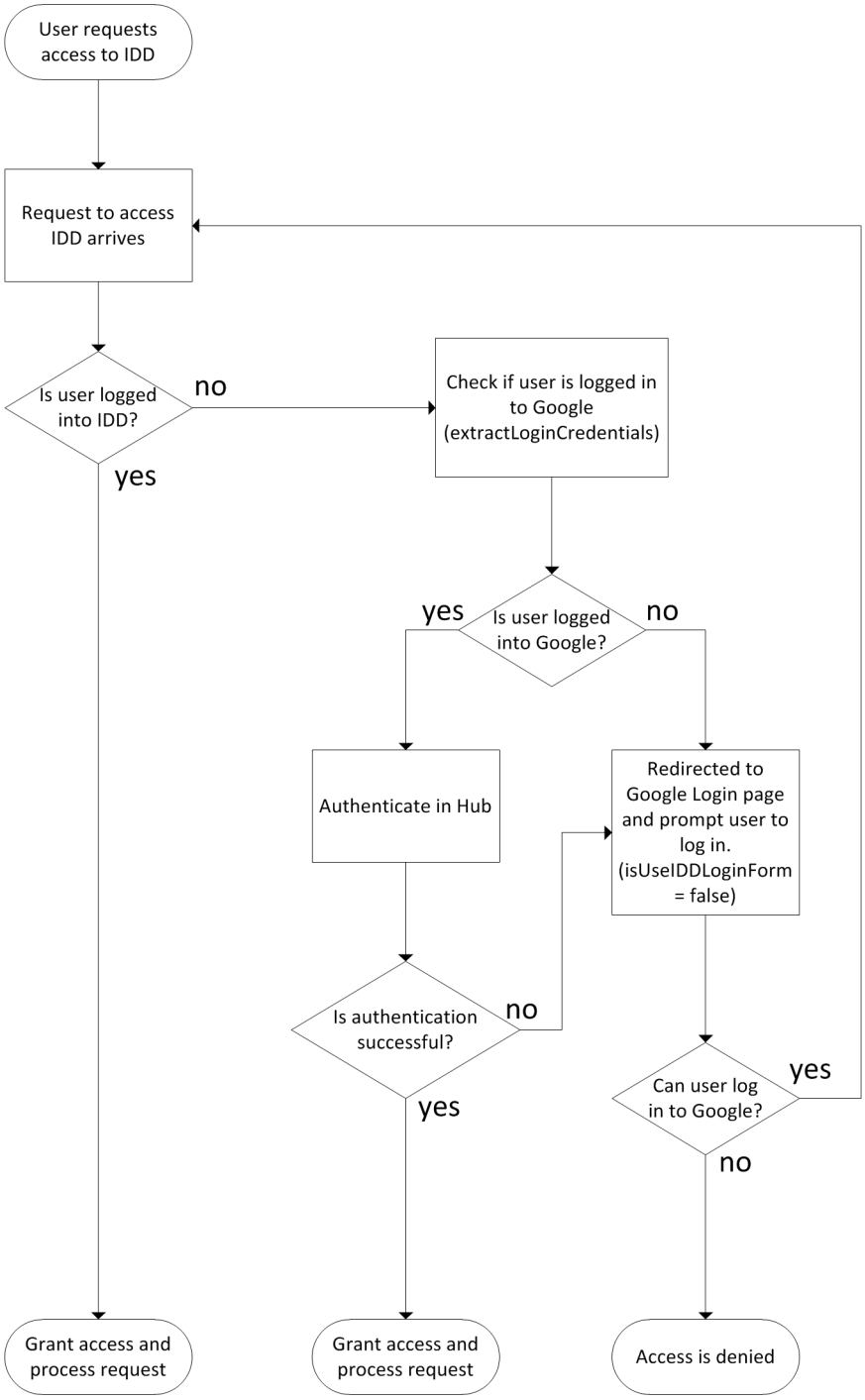
El kit de recurso contiene una implementación de proveedor de inicio de sesión de muestra para el inicio de sesión único de Google (SSO). La implementación del proveedor de inicio de sesión de muestra demuestra una forma de implementar SSO.

Puede encontrar la implementación del proveedor de inicio de sesión de muestra para Google SSO en el archivo siguiente:

```
<directorio de instalación de MDM Hub>\hub\resourcekit\samples\sso\GoogleSSO\source\java
\com\siperian\dsapp\sso\google\GoogleLoginProvider.java
```

Cuando un usuario solicita acceso a Informatica Data Director, el proveedor de inicio de sesión autentica al usuario a través de una secuencia de eventos.

La imagen siguiente muestra la secuencia de eventos que se producen cuando implementa Google SSO con la implementación del proveedor de inicio de sesión de muestra:



Las siguientes secuencias se pueden producir en función de si el usuario está registrado en Informatica Data Director, en Google o si no está registrado en ninguno de los dos:

Secuencia para usuarios que están registrados en Informatica Data Director.

Cuando un usuario solicita acceso a Informatica Data Director, el proveedor de inicio de sesión comprueba si el usuario está registrado. Si el usuario está registrado en Informatica Data Director, el proveedor de inicio de sesión concede acceso a Informatica Data Director.

Secuencia para usuarios que no están registrados en Informatica Data Director pero sí lo están en Google.

Cuando el proveedor de inicio de sesión determina que el usuario no está registrado en Informatica Data Director, comprueba si el usuario está registrado en Google. Si el usuario está registrado en Google, el proveedor de inicio de sesión pasa las credenciales Google del usuario al MDM Hub. La herramienta Proveedores de seguridad de MDM Hub autentica las credenciales de Google. Si la herramienta Proveedores de seguridad de MDM Hub autentica al usuario, el usuario puede acceder a Informatica Data Director. Si la herramienta Proveedores de seguridad no autentica al usuario, el proveedor de inicio de sesión redirige al usuario a la página de inicio de sesión de Google para que introduzca otras credenciales.

Secuencia para usuarios que no están registrados en Informatica Data Director ni en Google.

Cuando el proveedor de inicio de sesión determina que el usuario no está registrado en Informatica Data Director ni en Google, el proveedor de inicio de sesión redirige al usuario al formulario de inicio de sesión de Google. En la implementación de muestra, el proveedor de inicio de sesión redirige al formulario de inicio de sesión de Google en lugar de al formulario de inicio de sesión de Informatica Data Director porque `isUseIDDLoginForm` es `false`. Si establece `isUseIDDLoginForm` en `true`, el proveedor de inicio de sesión redirige al formulario de inicio de sesión de Informatica Data Director.

Después de que el usuario inicie sesión en Google, el proceso comienza de nuevo pero el usuario ahora ha iniciado sesión en Google. La herramienta Proveedores de seguridad de MDM Hub autentica las credenciales de Google para el usuario.

Configurar la autenticación de SSO de Google

Si utiliza la autenticación SSO de Google para Informatica Data Director, configure Informatica Data Director para volver a la pantalla de inicio de sesión después de que el usuario cierre la sesión.

1. Abra `cmxserver.properties` en el siguiente directorio:
   - En UNIX. `<directorio de instalación de infamdm>/hub/server/resources`
   - En Windows. `<directorio de instalación de infamdm>\hub\server\resources`
2. Añada la siguiente propiedad a `cmxserver.properties`:

   ```
   cmx.bdd.redirect_to_login_after_logout=false
   ```
3. Reinicie la aplicación Servidor del concentrador para volver a cargar la configuración en el archivo `cmxserver.properties`.

CAPÍTULO 5

Configuración manual de IDD

Este capítulo incluye los siguientes temas:

Resumen de configuración manual de IDD

El archivo de configuración de IDD (IDDConfig.xml) es un documento XML que se puede modificar en el Administrador de configuración de IDD o exportarse y editarse manualmente.

Para editar la configuración de una aplicación existente:

1. Exporte la aplicación IDD a un archivo .zip.
2. Extraiga el archivo .zip de la aplicación.
3. Edite el archivo de configuración de IDD (IDDConfig.xml).
4. Importe el archivo de configuración editado directamente para reemplazar el de la base de datos (Importar solo la configuración de IDD). La aplicación IDD también puede volver a comprimirse mientras que se importa la aplicación completa para reemplazar todos los archivos para la aplicación (Importación aplicación IDD completa).

Herramientas XML

El kit de recurso de Informatica MDM Hub incluye un esquema XML (archivo XSD) para el archivo de configuración de IDD.

Esto es muy útil al trabajar con editores XML. Este esquema puede guiarle al editar el archivo y, lo que es más importante, sirve para que el editor compruebe si el XML de un archivo de configuración de IDD es correcto. El archivo de configuración de IDD debe pasar esta prueba antes de importarse en el Administrador de configuración de IDD.

Aunque se puede usar un editor de texto simple para modificar la configuración de IDD, existen muchas herramientas de edición de XML que facilitan el trabajo con XML, como las siguientes:

Editor	URL
XML Copy Editor	http://xml-copy-editor.sourceforge.net/
XML Spy	http://www.altova.com/products/xmlspy/xmlspy.html
oXygen	http://www.oxygenxml.com/

El ejemplo de IDD del kit de recurso contiene los siguientes componentes que pueden ser útiles para la configuración manual.

Elemento del kit de recurso	Descripción
`siperian-bdd-config-6.xsd`	Esquema XML para el archivo de configuración de IDD. El archivo se encuentra en `<Carpeta de instalación>\hub\resourcekit\sdk\bddXsdDoc\siperian-bdd-config-6.xsd`
Documentación HTML para el esquema XML	Documentación de estilo Javadoc. Proporciona la misma información encontrada en el esquema XML, pero con un formato que permite una navegación más sencilla. **Nota:** Consulte esta documentación para obtener información detallada sobre los elementos y atributos XML del archivo de configuración de IDD.
Ejemplo de configuración de IDD	Se utiliza con el esquema de ejemplo.
Ejemplo de salidas de usuario de IDD	Un ejemplo de cómo compilar código Java personalizado para integrarlo con IDD.
Javadocs de biblioteca de IDD	Javadocs para las interfaces en Siperian-bdd.jar. Se utiliza para la implementación de salidas de usuario de IDD en Java.

Trabajar con el archivo XML de configuración de IDD

Un archivo XML de configuración de IDD puede ejecutar fácilmente cientos de líneas.

Aquí no se muestra un archivo completo, solamente el fragmento relevante. Puede encontrar un archivo de configuración completo en el kit de recurso o al exportarlo desde el Administrador de configuración de IDD.

El siguiente fragmento de código es un ejemplo de un grupo de área de asunto con una única área de asunto:

```
<subjectAreaGroup name="Customer" primaryObjectUid="C_PARTY">
        <subjectArea name="Person">
            <primaryObject hmEntityTypeUid="Person">
                <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE"  filterValue="Person"/>
                <cleanseFunction
                                cleanseFunctionUid="BDD Cleanse and Validation Library|
CVPerson">
                    <cleanseInput>
                        <cleanseColumn columnUid="C_PARTY|FIRST_NAME"
parameterName="firstName"/>
                        <cleanseColumn columnUid="C_PARTY|MIDDLE_NAME"
                                       parameterName="middleName"/>
                        <cleanseColumn columnUid="C_PARTY|LAST_NAME"
parameterName="lastName"/>
                    </cleanseInput>
                    <cleanseOutput>
                        <cleanseColumn columnUid="C_PARTY|FIRST_NAME"
parameterName="firstName"/>
                        <cleanseColumn columnUid="C_PARTY|MIDDLE_NAME"
                                       parameterName="middleName"/>
                        <cleanseColumn columnUid="C_PARTY|LAST_NAME"
parameterName="lastName"/>
                        <cleanseColumn columnUid="C_PARTY|DISPLAY_NAME"
                                       parameterName="displayName"/>
                    </cleanseOutput>
                </cleanseFunction>
                <layout columnsNum="3">
                    <column columnUid="C_PARTY|NAME_PREFIX_CD" editStyle="FIELD"
                            horizontalStyle="SMALL"/>
                    <column columnUid="C_PARTY|FIRST_NAME" editStyle="FIELD"
                            horizontalStyle="MEDIUM" required="true"/>
                    <column columnUid="C_PARTY|MIDDLE_NAME" editStyle="FIELD"
                            horizontalStyle="MEDIUM"/>
                    <column columnUid="C_PARTY|LAST_NAME" editStyle="FIELD"
                            horizontalStyle="MEDIUM" required="true"/>
                    <column columnUid="C_PARTY|GENERATION_SUFFIX_CD" editStyle="FIELD"
                            horizontalStyle="SMALL"/>
                    <column columnUid="C_PARTY|BIRTHDATE" editStyle="CALENDAR"
                            horizontalStyle="MEDIUM"/>
                    <column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD"
                            horizontalStyle="SMALL">
                        <columnI18NLookup languageCdUid="C_LU_GENDER_LCL|LANGUAGE_CODE"
                                          countryCdUid="C_LU_GENDER_LCL|COUNTRY_CODE"
                                          lookupFKUid="C_LU_GENDER_LCL|GENDER_CODE"
                                          localizedNameUid="C_LU_GENDER_LCL|
LOCALIZED_STRING"/>
                    </column>
                    <column columnUid="C_PARTY|TAX_ID" editStyle="FIELD"
                            horizontalStyle="MEDIUM"/>
                    <column columnUid="C_PARTY|DISPLAY_NAME" editStyle="FIELD"
                            horizontalStyle="LARGE"/>
                </layout>
                <label existsFormat="{1},{2}">
                    <column columnUid="C_PARTY|LAST_NAME"/>
                    <column columnUid="C_PARTY|FIRST_NAME"/>
                    <column columnUid="C_PARTY_ELECT_ADDR|ELECTRONIC_ADDRESS"/>
                </label>
            </primaryObject>
            <search displayPackageUid="PKG_PERSON_SEARCH">
            </search>
            <match>
                <matchRuleSet uid="C_PARTY|IDL" type="BOTH"/>
            </match>
            <taskAssignmentConfig task="UpdateWithApproval">
                <securityRole roleUid="DataSteward"/>
            </taskAssignmentConfig>
            <taskAssignmentConfig task="UpdateWithOptionalApproval" >
                <securityRole roleUid="DataSteward"/>
            </taskAssignmentConfig>
            <taskAssignmentConfig task="UpdateRejectedRecord">
```

```
            <securityRole roleUid="DataSteward"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="ReviewNoApprove">
            <securityRole roleUid="Manager"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="FinalReview" >
            <securityRole roleUid="SrManager"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="Merge">
            <securityRole roleUid="DataSteward"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="Unmerge">
            <securityRole  roleUid="DataSteward"/>
        </taskAssignmentConfig>
        <dataSecurity>
            <securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|STATE_CD">
                <securityValue value='CA'>
                    <securityRole roleUid="Customer-CA"/>
                </securityValue
            </securityFilter>
        </dataSecurity>
    </subjectArea>
</subjectAreaGroup>
```

Consulte la documentación HTML para el esquema XML para obtener detalles sobre los elementos, atributos y valores permitidos.

Área de asunto

Los elementos descritos en esta sección pueden necesitar que se realicen modificaciones manuales directamente en el archivo IDDConfig.xml.

Columna de búsqueda

Una aplicación IDD rellena automáticamente una lista desplegable de valores aceptables para las columnas que están configuradas en el Administrador de esquema como búsquedas.

Se controla en el Administrador de configuración de IDD para columnas que tienen una clave externa a la tabla de búsqueda. Si la clave externa no existe (por ejemplo, por motivos de rendimiento), la información sobre la tabla de búsqueda se puede especificar en la configuración de XML.

Mediante el elemento columnLookup se define una búsqueda explícita, tal como se muestra en el siguiente ejemplo.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_GENDER|GENDER_CODE"
          lookupNameUid="C_LU_GENDER|GENDER_DISP"/>
   </column>
```

En este ejemplo, la columna C_PARTY|GENDER_CD debe tratarse como si tuviera una clave externa a la columna C_LU_GENDER|GENDER_CODE, mientras que la tabla C_LU_GENDER se trata como tabla de búsqueda. La aplicación IDD crea una lista desplegable para la columna GENDER_CD y esta lista se rellena con valores de la tabla C_LU_GENDER (los valores de visualización se obtienen de la columna GENDER_DISP).

El elemento columnI18NLookup puede especificarse junto con el subelemento columnLookup si se necesita la localización de los valores de visualización.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_GENDER|GENDER_CODE"
         lookupNameUid="C_LU_GENDER|GENDER_DISP"/>
```

```
      <columnI18NLookup languageCdUid="C_LU_GENDER_LCL|LANGUAGE_CODE"
         countryCdUid="C_LU_GENDER_LCL|COUNTRY_CODE"
         lookupFKUid="C_LU_GENDER_LCL|GENDER_CODE"
         localizedNameUid="C_LU_GENDER_LCL|LOCALIZED_STRING"/>
   </column>
```

TEMAS RELACIONADOS

- "Tablas de búsqueda" en la página 24

Tablas de búsqueda con columna de subtipo

Se puede usar una tabla de búsqueda única para almacenar valores de búsqueda para varios tipos de códigos diferentes.

En este caso, la tabla de búsqueda tiene un subtipo de columna que identifica el tipo de código.

El uso de una tabla de búsqueda con múltiples tipos de búsqueda se configura como se muestra en el siguiente ejemplo.

```
<column columnUid="C_AUTOMOBILE|DOORS_CODE" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_AUTO_ATTR|CODE"
            lookupNameUid="C_LU_AUTO_ATTR|DISPLAY_NAME">
         <subTypeQualifier columnUid="C_LU_AUTO_ATTR|ATTR_TYPE">
            <filter>
               <value>Doors</value>
               <value>Style</value>
            </filter>
         </subTypeQualifier>
      </columnLookup>
   </column>
```

En este ejemplo, la columna C_AUTOMOBILE|DOORS_CODE es una columna de búsqueda. Solo los valores de la tabla de búsqueda con ATTR_TYPE="Doors" se utilizan para esta búsqueda.

La localización de búsqueda también puede combinarse con subtipos de búsqueda, como se muestra en el siguiente ejemplo.

```
<column columnUid="C_AUTOMOBILE|DOORS_CODE" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_AUTO_ATTR|CODE"
         lookupNameUid="C_LU_AUTO_ATTR|DISPLAY_NAME">
         <subTypeQualifier columnUid="C_LU_AUTO_ATTR|ATTR_TYPE">
            <filter>
               <value>Doors</value>
               <value>Style</value>
            </filter>
         </subTypeQualifier>
      </columnLookup>
      <columnI18NLookup languageCdUid="C_LU_AUTO_ATTR_LCL|LANGUAGE_CODE"
         countryCdUid="C_LU_AUTO_ATTR_LCL|COUNTRY_CODE" lookupFKUid="C_LU_AUTO_ATTR_LCL|
CODE"
         localizedNameUid="C_LU_AUTO_ATTR_LCL|LOCALIZED_STRING">
         <subTypeQualifier columnUid="C_LU_AUTO_ATTR_LCL|ATTR_TYPE "
filterValue="Doors"/>
      </columnI18NLookup>
   </column>
```

Temas relacionados

- "Códigos de idioma" en la página 165

Valores de búsqueda estática

Los valores para una columna de búsqueda también pueden definirse directamente en el archivo de configuración de IDD, sin necesidad de usar una tabla de búsqueda.

El elemento columnStaticLookups se utiliza para definirlos, como se muestra en el siguiente ejemplo.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnStaticLookups>
         <columnStaticLookup code="M" name="MALE"/>
         <columnStaticLookup code="F" name="FEMALE"/>
      </columnStaticLookups>
   </column>
```

Este ejemplo especifica que solo se pueden almacenar los valores "M" y "F" en la columna C_PARTY|GENDER_CD. Para esta columna, la aplicación IDD crea una lista desplegable con los valores 'MALE' y 'FEMALE'.

Los valores de búsqueda estática también pueden localizarse, como se muestra en el siguiente ejemplo.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnStaticLookups>
         <columnStaticLookup code="M" name="MALE"/>
         <columnStaticLookup code="F" name="FEMALE"/>
         <columnStaticLookup code="M" name="MANN" languageCode="de" countryCode="DE"/>
         <columnStaticLookup code="F" name="FRAU" languageCode="de"  countryCode="DE"/>
      </columnStaticLookups>
   </column>
```

Mostrar los campos secundarios desde un objeto base de la ficha secundaria

Para mostrar los campos secundarios desde un objeto base (BO) de la ficha secundaria de IDD, utilice el tipo de elemento secundario **Parte del objeto principal** al crear el área de asunto (SA) secundaria en el Administrador de configuración de IDD.

Debe configurar el archivo de configuración IDD (`IDDConfig.xml`) para mostrar los campos secundarios de un BO en la ficha secundaria.

Para el siguiente ejemplo, en la Consola del concentrador debe crear el BO `C_EMPLOYEE` con cuatro columnas: `EMP_ID`, `EMP_NAME`, `STATE` y `COUNTRY`, así como la SA principal `Employee` y la SA secundaria `EmpDetails`.

El siguiente fragmento de código muestra `EMP_NAME` (que es un campo secundario) en la ficha secundaria `EmpDetails`.

```
primaryObjectUid="C_EMPLOYEE" searchOnly="false">
<subjectArea displayName="Employee" name="Employee" showXREF="false">
    <primaryObject>
        <layout columnsNum="3">
            <column columnUid="C_EMPLOYEE|EMP_ID"
                editStyle="FIELD" editable="true"
                hidden="false" horizontalStyle="MEDIUM"
                lineBreak="false"
                ns1:showInHMCompactView="false"
                required="false" xmlns:ns1="urn:siperian.dsapp.config"/>
            <column columnUid="C_EMPLOYEE|STATE"
                editStyle="FIELD" editable="true"
                hidden="false" horizontalStyle="MEDIUM"
                lineBreak="false"
                ns2:showInHMCompactView="false"
                required="false" xmlns:ns2="urn:siperian.dsapp.config"/>
```

```
                        <column columnUid="C_EMPLOYEE|COUNTRY"
                            editStyle="FIELD" editable="true"
                            hidden="false" horizontalStyle="MEDIUM"
                            lineBreak="false"
                            ns3:showInHMCompactView="false"
                            required="false" xmlns:ns3="urn:siperian.dsapp.config"/>
                    </layout>
                    <label existsFormat="{0}"
                        existsNoAttributesFormat="{0}" newFormat="New {0}"/>
                </primaryObject>
                <poPartOfChild displayName="EmpDetails"
                    name="EmpDetails" ns4:showInHMCompactView="false"
xmlns:ns4="urn:siperian.dsapp.config">
                    <ns4:layout columnsNum="3">
                        <ns4:column columnUid="C_EMPLOYEE|EMP_NAME"
                            editStyle="FIELD" editable="true"
                            hidden="false" horizontalStyle="MEDIUM"
                            lineBreak="false"
                            ns4:showInHMCompactView="false" required="false"/>
                    </ns4:layout>
                </poPartOfChild>
                <search displayPackageUid="PKG_EMPLOYEE"/>
                <dataSecurity/>
            </subjectArea>
        </subjectAreaGroup>
```

Visualizar un elemento primario de un objeto principal en una ficha secundaria

Cuando un objeto principal tiene un elemento primario, los atributos del objeto base principal se pueden visualizar en una ficha secundaria. Para configurar la visualización, es preciso editar el archivo XML de configuración de IDD. Puede configurar varias fichas secundarias, una para cada objeto base principal que desee visualizar.

En MDM Hub, la relación entre los objetos base debe ser de tipo 1:1 o bien 1:muchos. Por ejemplo, puede crear los objetos base C_ADDRESS y C_PARTY y crear una relación entre ellos.

1. En el administrador de configuración de IDD, cree un área de asunto para el objeto primario. Por ejemplo, puede crear un área de asunto para C_ADDRESS.
2. Guarde la configuración.
3. Abra el archivo XML de configuración de IDD.
4. Después del elemento `primaryObject`, añada el elemento `poParent` y defina los campos que desee visualizar.

   Por ejemplo, el siguiente código de ejemplo muestra cómo se configura el elemento `poParent` para que muestre tres campos de C_PARTY en la ficha secundaria.

```
<subjectArea displayName="Address" name="Address" showXREF="false">
    <primaryObject>
  ...
    </primaryObject>
    <poParent name="Party" displayName="Party" uid="C_PARTY"
mpcUid="C_MT_PARTY_ADDRESS">
  <layout columnsNum="3">
        <column columnUid="C_PARTY|FIRST_NAME" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
        <column columnUid="C_PARTY|LAST_NAME" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
   <column columnUid="C_PARTY|PARTY_TYPE" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
  </layout>
 </poParent>
    <search displayPackageUid="PKG_ADDRESS"/>
```

```
        <dataSecurity/>
    </subjectArea>
    </subjectAreaGroup>
```

5. Guarde el archivo.

Expandir un área de asunto secundaria en la vista de datos de forma predeterminada

Puede configurar un área de asunto secundaria para que se expanda de forma predeterminada al abrir un registro en la vista de datos.

Establezca el atributo `expanded` en `true` en `BDDConfig.xml` para el área de asunto secundaria. Al abrir el registro principal, el área de asunto secundaria aparecerá expandida. El resto de áreas de asunto secundarias aparecerán contraídas.

El siguiente ejemplo de código establece que el área de asunto C_PARTY_NAME se expanda de forma predeterminada al abrir el registro principal en la vista de datos:

```
<one2ManyChild name="Names" type="ONE_2_MANY" uid="C_PARTY_NAME"
mpcUid="C_MT_PARTY_NAME" expanded="true">
    <layout columnsNum="1">
        <column columnUid="C_PARTY_NAME|NAME" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
        <column columnUid="C_PARTY_NAME|AUTOMOBILE_ID" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
    </layout>
</ one2ManyChild>
```

Crear referencia de elemento del mismo nivel

Puede crear una referencia de elemento del mismo nivel para crear una relación de un registro de un área de asunto con un registro secundario de esa área de asunto. Por ejemplo, un cliente podría incluir registros secundarios de dirección y número de teléfono, y que el número de teléfono incluya una clave externa para asociarlo con una dirección específica.

Debe configurar el archivo de configuración de IDD (`IDDConfig.xml`) para crear la referencia de elemento del mismo nivel.

El siguiente fragmento de código crea una referencia de elemento del mismo nivel para el campo `ADDRESS_ID` de la columna en el área de asunto secundaria `PERSON DETAILS`.

```
<ns10:column
          columnUid="C_PERSON_DETAILS|ADDRESS_ID"
          editStyle="FIELD" editable="true"
          hidden="false" horizontalStyle="MEDIUM"
          lineBreak="false"
          ns10:showInHMCompactView="false" required="false">
       <siblingReference childName="Addresses">
          <label existsFormat=" {1}, {2} "
                    existsNoAttributesFormat="MailingAddress"
                    newFormat="New MailingAddress" taskFormat=" {1}, {2} ">
                         <column columnUid="C_ADDRESS|ADDRESS_LINE_1"/>
                         <column columnUid="C_ADDRESS|CITY_NAME"/>
          </label>
       </siblingReference>
</ns10:column>
```

Nota: Debe especificar el atributo `ChildName` en la etiqueta `siblingReference` con el nombre de referencia del área de asunto secundaria disponible.

Elementos secundarios de segundo nivel

Cuando un elemento secundario de segundo nivel se muestra en una vista de tabla, se muestran todos los registros secundarios de segundo nivel, no solo los relacionados con ese registro secundario seleccionado. IDD tiene una opción de configuración que ayuda a los usuarios a entender la relación de estos elementos secundarios de segundo nivel con el elemento secundario.

Se puede definir un parentReference para la columna que sea la clave externa al registro secundario. Esto define una etiqueta que se muestra en el registro secundario de segundo nivel que contiene datos del elemento secundario.

En el ejemplo siguiente, la columna de clave externa del elemento secundario de segundo nivel al elemento secundario está configurada como una referencia principal. Esta configura un elemento de etiqueta con el conjunto de columnas que utilizar para etiquetas y existsFormat. En este ejemplo, la etiqueta para el registro secundario será "<Número de teléfono>, (<Número de extensión>)".

```
<many2ManyChild name="TestPhone" displayName="Test Phone" type="PART_OF"
        uid="C_PHONE_CHILD4" mpcUid="C_MT_PHONE_CHILD4" defaultView="form">
            <layout columnsNum="3">
                <column columnUid="C_PHONE_CHILD4_REL|PHONE_ID"
editStyle="FIELD"
                    horizontalStyle="LARGE">
                    <parentReference>
                        <label existsFormat="{0} ({1})">
                            <column columnUid="C_PARTY_PHONE|PHONE_NUM"/>
                            <column columnUid="C_PARTY_PHONE|PHONE_EXT_NUM"/>
                        </label>
                    </parentReference>
                </column>
                <column … />
            </layout>
    </many2ManyChild>
```

Vínculos de área de asunto

Un área de asunto puede contener varios elementos secundarios de referencia de muchos a muchos.

Estos elementos muestran un área de asunto como un elemento secundario de otra área de asunto. El área de asunto secundaria no se puede editar directamente. El usuario de la aplicación IDD debe navegar a una vista de datos distinta para el área de asunto secundaria para editarla. El elemento `subjectAreaLinkColumn` se utiliza para definir una columna que se va a usar como vínculo activo.

Los datos de la columna identificados como el vínculo del área de asunto aparecen subrayados. Cuando el usuario de la aplicación IDD hace clic en esta columna, el área de asunto asociada se abre en una nueva ficha.

Tanto si una columna de vínculo de área de asunto está configurada como si no, el usuario de la aplicación IDD puede hacer clic con el botón derecho en el registro y seleccionar "Abrir en una ficha nueva" para abrir el área de asunto.

```
<many2ManyChild name="Organization" displayName="Org" type="REFERENCE"
        uid="C_PARTY" subjectAreaLinkColumn=”C_PARTY_ORGANIZATION_NAME”
        mpcUid="C_MT_ORG_CHILD"  hmEntityTypeUid="Organization">
        <layout columnsNum="2">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
                horizontalStyle="LARGE" required="true"/>
            …
        </layout>
    </many2ManyChild>
```

Agrupación de menús lógicos

Si tiene varios grupos de área de asunto, puede organizarlos o agruparlos para crear una estructura lógica de menús de nivel superior en la aplicación IDD.

Debe editar el archivo de configuración de IDD (`IDDConfig.xml`) para crear grupos lógicos de grupos de área de asunto.

El siguiente fragmento de código crea una agrupación lógica de grupos de área de asunto.

```
<sagGroups>
       <sagLogicalGroup name="Product" displayName="Product">
              <sagReference sagName="Account" />
              <sagReference sagName="AccountGroup" />
       </sagLogicalGroup>
</sagGroups>
```

Añadir grupos en la ventana Nuevo

Si tiene muchas áreas de asunto, defina grupos para usarlos en la ventana **Nuevo** en IDD. Establezca la propiedad global `enableCreateBeMenuGrouping=true` y, a continuación, defina los grupos en el archivo `IDDConfig.xml`.

1. Establezca la propiedad `enableCreateBEMenuGrouping` mediante el comando siguiente:

   ```
   insert into C_REPOS_DS_PREF_DETAIL (ROWID_DS_PREF_DETAIL, Create_Date, creator,
   Last_Update_Date, Updated_By, ROWID_DS_PREF, NAME, VALUE)
   select 'PREF_DET_4', sysdate, 'CMX', sysdate, 'admin', rowid_ds_pref,
   'enabeCreateBeMenuGrouping', 'true' from C_REPOS_DS_PREF where name =
   'SYSTEM_PREFERENCES_ROOT';
   ```

2. En IDD Configuration Manager, exporte el archivo `IDDConfig.xml` y, a continuación, añada los grupos al archivo como se muestra en el siguiente ejemplo:

   ```
   <sagGroups>
   <sagLogicalGroup name="CustomerGroup" displayName="CustomerGroup">
   <sagReference sagName="Customer" />
   <sagReference sagName="Household" />
   </sagLogicalGroup>
   </sagGroups>
   ```

3. Reinicie el servidor de aplicaciones.
4. Implemente el archivo `IDDConfig.xml` modificado.
5. Inicie sesión en la aplicación IDD y compruebe que la ventana **Nuevo** contiene los grupos.

Personalización de etiquetas de columnas

Puede personalizar etiquetas de columna en IDD a nivel de área de asunto para distinguir etiquetas de columna idénticas utilizadas en varias áreas de asunto o para modificar cualquier etiqueta de columna. Debe editar el archivo `MetadataBundle.properties` para personalizar la etiqueta de columna de área de asunto. Por ejemplo, imagine que tiene el objeto base Grupo con las áreas de asunto Persona y Organización. Si cuenta con la etiqueta de columna ID fiscal en ambas áreas de asunto, puede personalizar las etiquetas de columna para distinguir entre las áreas de asunto.

Para personalizar etiquetas de columnas de un área de asunto, realice los pasos siguientes:

1. Si ha cambiado los metadatos del almacén de referencias operativas, haga clic en **Borrar memoria caché**.
2. Exporte la aplicación IDD a un archivo .zip.
3. Extraiga el archivo .zip de la aplicación.

4. Edite el archivo `MetadataBundle.properties`.
   Por ejemplo: Para modificar la etiqueta de columna ID fiscal a ID fiscal de cliente en MetadataBundle.properties, edite Test.Person.COLUMN.C_PARTY|TAX_ID=ID fiscal de cliente.
5. En el Administrador de configuración de IDD, seleccione la aplicación IDD para reemplazar el archivo MetadataBundle.properties editado.
6. Haga clic en el botón **Importar** y seleccione **Importar a una aplicación IDD existente**.
7. En la ventana **Importar a una aplicación IDD existente**, para **Tipo de configuración** seleccione **Paquete de metadatos**.
8. Haga clic en **Examinar** para localizar y seleccionar el archivo MetadataBundle.properties apropiado.
9. Haga clic en **Importar**.

   Inicie sesión en la aplicación IDD para ver las etiquetas de columnas personalizadas.

Configurar la casilla de verificación Editar estilo

La asignación de valores permite definir valores que se deben almacenar en Informatica MDM Hub para columnas con la casilla de verificación Editar estilo.

La siguiente tabla proporciona información acerca de los estilos de edición que puede configurar para el tipo de datos compatible.

Tipo de datos	Editar estilo
DATE	Calendario y calendario largo
INT y CHAR(1)	Campo, Área de texto y Casilla
Otros	Campo y Área de texto

Nota:

- Para una columna de tipo de datos CHAR(1), puede definir tres pares de valores que puede configurar para una casilla de verificación: Valor 1/0, valor Y/N o valor T/F. Según el par de valores asignados, el valor correspondiente se guardará en el objeto base.
- Para una columna de tipo de datos INT, solo puede definir pares de valores de 0 y 1.

Para la configuración manual, debe asegurarse de que el elemento `column` con `editStyle="CHECKBOX"` no debe tener más de un elemento `valueMapping` anidado. El elemento `valueMapping` para `editStyle="CHECKBOX"` debe tener dos elementos `mappingItem` anidados. Asimismo, `mapping Item` debe incluir los valores `selected` de `true` y `false`.

En el siguiente ejemplo, el atributo `domainValue` es responsable del valor que se almacena en Informatica MDM Hub y el atributo `selected` es responsable de la presentación del control de la casilla de verificación. Los valores `true` o `false` se definen para los estados seleccionados y no seleccionados de la casilla de verificación respectivamente.

```
<column columnUid="C_PARTY_PHONE|IS_VALID_IND" editStyle="CHECKBOX"
horizontalStyle="SMALL">
<valueMapping>
<mappingItem domainValue="1" selected="true"/>
<mappingItem domainValue="0" selected ="false"/>
</valueMapping>
</column>
```

Configuración del Administrador de jerarquía

La configuración descrita aquí se aplica a la vista de jerarquía de IDD para todos los tipos de entidad de Administrador de jerarquía (HM).

El siguiente listado XML presenta ejemplos de todos los elementos descritos posteriormente en esta sección.

```
<hmConfiguration hmConfigurationUid="Default|Master" enableAddRel="false"
        simpleNodeLimit="100">
    <hmOneHopLimits totalRels="1000"/>
    <hmManyHopLimits hops="20" relsPerEntity="50" totalRels="1000"/>
    <hmRelationshipTypes>
        <hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.employs">
            <layout columnsNum="2">
                <column columnUid="C_RL_PARTY|REL_NAME" editStyle="FIELD"
                    horizontalStyle="LARGE" required="true"/>
                <column columnUid="C_RL_PARTY|REL_DESC" editStyle="FIELD"
                    horizontalStyle="MEDIUM"/>
                <column columnUid="C_RL_PARTY|NOTE" editStyle="FIELD"
                    horizontalStyle="SMALL"/>
            </layout>
        </hmRelationshipType>
        <hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.contains member">
            <layout columnsNum="2">
                <column columnUid="C_RL_PARTY_GROUP|HUB_STATE_IND" editStyle="FIELD"
                    horizontalStyle="MEDIUM"/>
            </layout>
        </hmRelationshipType>
    </hmRelationshipTypes>
    <hmFilter name="filter1" displayName="Filter 1">
        <showActiveRelOnly>false</showActiveRelOnly>
        <hideUnconnectedEntities>false</hideUnconnectedEntities>
        <getParents>true</getParents>
        <getChildren>true</getChildren>
        <getUndirected>true</getUndirected>
        <getBidirectional>true</getBidirectional>
        <getUnknown>true</getUnknown>
    </hmFilter>
    <hmFilter name="filter2" displayName="Filter 2">
        <showActiveRelOnly>false</showActiveRelOnly>
        <hideUnconnectedEntities>false</hideUnconnectedEntities>
        <getParents>true</getParents>
        <getChildren>true</getChildren>
        <getUndirected>true</getUndirected>
        <getBidirectional>true</getBidirectional>
        <getUnknown>true</getUnknown>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.member of account group
            </enabledRelationshipsUids>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.employs</
enabledRelationshipsUids>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.contains member 2
            </enabledRelationshipsUids>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.customer
            </enabledRelationshipsUids>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.contains member
            </enabledRelationshipsUids>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.associate
            </enabledRelationshipsUids>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.organization has
            </enabledRelationshipsUids>
        <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.is DNB parent of
            </enabledRelationshipsUids>
        <enabledHierarchiesUids>HM_HIERARCHY.Product</enabledHierarchiesUids>
        <enabledHierarchiesUids>HM_HIERARCHY.Customer</enabledHierarchiesUids>
        <enabledHierarchiesUids>HM_HIERARCHY.DNB</enabledHierarchiesUids>
    </hmFilter>
    <externalLinkAction callback="false" displayName="Graph Google Search"
            name="hm_google_search_action">
```

```
            <externalLink name="hm_google_search_link" type="IFRAME"
                    url="http://www.google.com/search">
                <param bddParamName="SELECTED_GRAPH_OBJECTS" name="q" />
                <param name="hl" staticValue="en" />
            </externalLink>
         </externalLinkAction>
        <externalLinkAction callback="true" displayName="Test graph callback"
                name="hm_test_callback_action">
            <externalLink name="hm_test_callback" type="IFRAME"
url="test_external_hm.html">
                <param bddParamName="USERNAME" name="username" />
                <param bddParamName="SELECTED_GRAPH_OBJECTS" name="selectedHmObjects" />
                <param bddParamName="ALL_GRAPH_OBJECTS" name="allHmObjects" />
            </externalLink>
        </externalLinkAction>
    </hmConfiguration>
```

Añadir relaciones

La vista de jerarquía puede configurarse para que sea una vista de solo lectura.

El usuario de la aplicación IDD puede navegar por las relaciones, pero las relaciones no se pueden añadir ni editar. El atributo enableAddRel que controla esto se establece de forma predeterminada en true. El ejemplo anterior muestra cómo deshabilitar las adiciones y ediciones de relaciones.

Optimización de representación

IDD proporciona una visualización enriquecida para entidades y relaciones de la vista de jerarquía.

Como un gráfico de esta vista puede alcanzar un tamaño considerable, el tiempo necesario para representar esta vista puede ser un problema. IDD define un umbral sobre el que los nodos se representan de forma simplificada, por lo que se reduce el tiempo de representación. El valor predeterminado es 300, pero se puede configurar manualmente mediante el atributo simpleNodeLimit.

Tipos de relación del Administrador de jerarquía

Utilice el elemento hmRelationshipType para configurar los tipos de relación. Puede configurar diseños, funciones de limpieza y salidas de usuario para las relaciones que se añaden o se editan en la vista Jerarquía.

La configuración se realiza por tipo de relación. Existen columnas estándar para cada relación que Data Director administra automáticamente; tipo de relación y jerarquía, fecha de inicio y de finalización, y referencias a las entidades relacionadas. El elemento hmRelationshipTypes especifica todos los atributos adicionales de un registro de relación.

Nota: Una relación de Administrador de jerarquía que se defina como relación de clave externa en la Consola del concentrador no puede tener campos personalizados ni una definición de diseño en Data Director. Esta restricción se basa en la naturaleza de la relación de clave externa. Para obtener más información, consulte la sección sobre la configuración de relación de clave externa entre los objetos base en la *Guía de configuración de Multidomain MDM*.

Filtro del Administrador de jerarquía

La vista de jerarquía tiene filtros que controlan qué tipos de relación y jerarquía, direcciones de relación y otros elementos se muestran.

Utilice el elemento hmFilter para definir la configuración del filtro que se puede asignar como configuración del filtro predeterminada para un área de asunto. Este ajuste se usa siempre que un usuario de la aplicación IDD no haya creado un filtro guardado y lo establezca como predeterminado para esa área de asunto.

Por ejemplo, el siguiente código establece `filter2` como el filtro predeterminado del área de asunto `A1`:

```
<subjectAreaGroup displayName="SAG1" name="SAG1" primaryObjectUid="C_TEST"
searchOnly="false">
<subjectArea displayName="A1" name="A1" showXREF="false">
<primaryObject hmEntityTypeUid="A1" hmFilterName="filter2">
...
</primaryObject>
```

Habilitar relaciones inactivas

Para permitir al usuario ver las relaciones inactivas en Administrador de jerarquía, establezca `hmInactiveRelationshipsAvailable` en `true`.

Para añadir este parámetro a la base de datos de Oracle y establecer el parámetro en true, ejecute el siguiente script:

```
insert into CMX_SYSTEM.C_REPOS_DS_PREF_DETAIL
(ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select 'INCTR', rowid_ds_pref, 'hmInactiveRelationshipsAvailable', 'true'
from CMX_SYSTEM.C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
```

Registros de la tabla de relaciones de la vista de jerarquía

Establezca el recuento máximo de registros para limitar el número de registros de relación que la tabla de relación de la vista de jerarquía muestra.

El archivo `cmxserver.properties` contiene el parámetro sif.api.hm.flyover.max.record.count. El valor predeterminado es 10 000.

Si no especifica una fecha efectiva en la vista de jerarquía, la tabla de relación muestra los registros de relación efectivos e inefectivos. Pueden existir muchos registros de relación efectivos e inefectivos para una entidad determinada. Si el número total de registros de relación excede el límite de recuento máximo de registros, Informatica Data Director muestra los registros de relación que se sitúan más arriba en el orden de clasificación. Informatica Data Director no muestra los registros de relación que superan el recuento máximo de registros.

Al especificar la fecha efectiva en la vista de jerarquía, la tabla de relación muestra todas las relaciones efectivas para la fecha efectiva, independientemente del límite del recuento máximo de registros.

Vista Jerarquía

En la vista de jerarquía, un usuario puede utilizar el comando Ver detalles para una entidad seleccionada para mostrar un cuadro de diálogo que proporciona una vista compacta de la entidad y algunos de sus registros secundarios.

El atributo compactViewChildrenNumber controla cuántos registros secundarios de cada tipo se deben mostrar (el valor predeterminado es 5).

Las columnas y tipos secundarios que se muestran en esta vista se controlan mediante el atributo showInHMCompactView en columnas y objetos secundarios. Para el objeto principal, se debe definir

showInHMCompatctView="true" para todas las columnas que se deban mostrar. Para los objetos secundarios, se debe definir showInHMCompatctView="true" para todos los objetos que se deban mostrar. Si este atributo no se define para ninguna columna del objeto principal ni para ningún elemento secundario, solo se mostrará la etiqueta para el área de asunto en este cuadro de diálogo.

```
<subjectArea name="Person">
        <primaryObject hmEntityTypeUid="Person">
            ...
            <layout columnsNum="3">
                <column columnUid="C_PARTY|NAME_PREFIX_CD" editStyle="FIELD"
                        horizontalStyle="SMALL"/>
                <column columnUid="C_PARTY|FIRST_NAME" editStyle="FIELD"
                        showInHMCompactView="true"
                        horizontalStyle="MEDIUM" required="true"/>
                <column columnUid="C_PARTY|MIDDLE_NAME" editStyle="FIELD"
                        showInHMCompactView="true"
                        horizontalStyle="MEDIUM"/>
                <column columnUid="C_PARTY|LAST_NAME" editStyle="FIELD"
                        showInHMCompactView="true"
                        horizontalStyle="MEDIUM" required="true"/>
                <column columnUid="C_PARTY|GENERATION_SUFFIX_CD" editStyle="FIELD"
                        horizontalStyle="SMALL"/>
                <column columnUid="C_PARTY|BIRTHDATE" editStyle="CALENDAR"
                        horizontalStyle="MEDIUM"/>
                </column>
            </layout>
            ...
            <one2ManyChild name="Email" type="ONE_2_ONE" uid="C_PARTY_ELECT_ADDR"
                showInHMCompactView="true"
                mpcUid="C_MT_ELECTRONIC_ADDRESS">
            </one2ManyChild>
            ...
        </primaryObject>
    </subjectArea>Subject Area settings
```

La configuración del objeto principal que se describe aquí controla el comportamiento predeterminado al abrir una vista de jerarquía como delimitador. Se pueden configurar los siguientes atributos.

Atributo	Descripción
hmManyHopLimits	Controla el gráfico que se obtiene. El valor predeterminado es un salto.
hmFilterName	Filtro inicial que aplicar al mostrar el gráfico. El nombre debe ser uno de los filtros definidos en hmFilters descritos anteriormente.
hmDefaultLayout	Diseño que se utiliza para mostrar el gráfico. Uno de los siguientes valores: hierarchy, taxonomy, tree, network, circular y explorerView.

```
<primaryObject hmEntityTypeUid="Person" hmFilterName="filter1" hmDefaultLayout="tree">
        ...
        <hmManyHopLimits hops="3" relsPerEntity="50" totalRels="1000"/>
    </primaryObject>
```

Personalizaciones

La vista de jerarquía se puede personalizar de las siguientes maneras:

- Salidas de usuario ejecutadas al añadir o modificar relaciones
- Salidas de usuario que se pueden invocar desde el menú Más acciones
- Acciones personalizadas que se pueden invocar desde el menú Más acciones y pueden transferir el contexto del gráfico que se visualiza

Extensiones de interfaz de usuario

Las extensiones de la interfaz de usuario se utilizan para añadir funciones personalizadas a una aplicación IDD.

Elemento	Descripción
uiExtensions	Se puede agregar a la configuración para añadir fichas de nivel superior y extensiones del Espacio de trabajo Inicio.
externalLinkChild	Se puede configurar para añadir fichas secundarias a un área de asunto.
externalLinkAction	Se puede configurar para añadir acciones a un área de asunto, a un elemento secundario de área de asunto o a resultados de búsqueda.

Estas extensiones se invocan mediante una URL a la que se pueden transferir parámetros. Estos parámetros pueden incluir el nombre de usuario y la contraseña del usuario que ha iniciado sesión. Además, pueden transferirse tanto sin cifrar como cifrados mediante la clave de cifrado simétrica de Blowfish. Use encryptionKey como elemento opcional en el elemento bddApplication.

```
<bddApplication xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      name="AppName"
      displayName="Application Name"
      defaultLocale="en"
      sessionTimeoutMinutes="30"
      xsi:noNamespaceSchemaLocation="./siperian-bdd-config-6.xsd">
    <encryptionKey>secretKey</encryptionKey>
    ...
  </bddApplication>
```

Fichas de espacio de trabajo de nivel superior

De forma predeterminada, Informatica Data Director muestra tres fichas de espacio de trabajo de nivel superior: Inicio, Datos y Tareas.

Nota: no puede deshabilitar las fichas Inicio, Datos y Tareas predeterminadas.

Se pueden configurar fichas adicionales que contengan una página solicitada desde una URL externa.

Fichas personalizadas de nivel superior

Puede agregar fichas personalizadas de nivel superior a Informatica Data Director.

Puede agregar una ficha para mostrar un vínculo externo en un iFrame. No puede utilizar sitios web como Google y Facebook con iFrame debido a las políticas de privacidad de estos sitios web. Asegúrese de que el vínculo externo corresponde a un sitio web que sea compatible con iFrames.

La muestra de código de ejemplo siguiente añade una página de búsqueda de Bing:

```
http://www.bing.com/search?q=bddUserName&hl=en

<bddApplication …>
    …
    <uiExtensions logicalOrsGroupName="CMX_ORS">
      <topLevelTab name="custom_bing_tab" displayName="Bing Search">
        <externalLink name="bing_username" type="IFRAME" url="http://www.bing.com/search"
            displayName="Bing search">
          <param name="q" bddParamName="USERNAME"/>
          <param name="hl" staticValue="en"/>
        </externalLink>
```

```
      </topLevelTab>
      …
    </uiExtensions>
    …
  </bddApplication>
```

Espacio de trabajo Inicio

El Espacio de trabajo Inicio de Informatica Data Director tiene tres tipos de componentes: una lista de tareas (Mis tareas), informes y componentes personalizados.

La lista de tareas siempre está disponible. Esta sección describe la configuración de componentes personalizados mediante el elemento externalLink.

De forma predeterminada, estos componentes se ordenan de la siguiente manera: lista de tareas, informes y componentes personalizados. Mediante el elemento dashboardLayout que se describe en esta sección se puede cambiar el orden. Los usuarios de la aplicación Informatica Data Director pueden personalizar aún más el conjunto de componentes que verán y el orden en que se muestran. Esta información se guarda como parte de las preferencias del usuario.

Vínculos externos (componentes del espacio de trabajo Inicio personalizados)

Los componentes personalizados se definen con el elemento externalLink.

Un elemento externalLink permite mostrar páginas solicitadas desde una URL externa o código HTML y JavaScript personalizado.

El siguiente fragmento de código es un ejemplo de un componente personalizado del Espacio de trabajo Inicio. Se transfieren dos parámetros como parte de la URL, como:

```
http://www.bing.com/search?q=bddUserName&hl=en
```

```
<bddApplication …>
    …
    <uiExtensions>
      …
      <dashboard>
        <externalLink name="bing_username" type="IFRAME" url="http://www.bing.com/search"
            displayName="Bing search">
          <param name="q" bddParamName="USERNAME"/>
          <param name="hl" staticValue="en"/>
        </externalLink>
        …
      </dashboard>
    </uiExtensions>
    …
  </bddApplication>
```

Parámetros de vínculos externos (estáticos y dinámicos)

Se puede configurar cualquier cantidad de parámetros para la URL especificada en el elemento externalLink. Los parámetros pueden ser estáticos o dinámicos.

Parámetro	Descripción
Estático	Tienen valores predefinidos especificados en el archivo de configuración de IDD. El siguiente ejemplo muestra una definición de parámetro estático que utiliza el atributo staticValue: `<param name="hl" staticValue="en"/>`
Dinámico	Se sustituyen en tiempo de ejecución. La definición de un parámetro dinámico contiene el atributo bddParamName y el valor de este atributo se sustituye por datos disponibles en tiempo de ejecución. Se admiten los siguientes parámetros dinámicos: - Nombre de inicio de sesión del usuario de la aplicación IDD conectado (bddParamName="USERNAME") - Nombre de inicio de sesión cifrado del usuario de la aplicación IDD conectado (bddParamName="USERNAME_ENCRYPTED") - Contraseña del usuario de la aplicación IDD conectado (bddParamName="PASSWORD") - Contraseña cifrada del usuario de la aplicación IDD conectado (bddParamName="PASSWORD_ENCRYPTED")

Componentes de vínculos externos (IFRAME e IGOOGLE)

Se admiten dos tipos de componentes de externalLink: IFRAME e IGOOGLE.

IFRAME

Los componentes de IFRAME (tipo = " IFRAME") muestran una página solicitada desde una URL externa. No puede utilizar sitios web como Google y Facebook con iFrame debido a las políticas de privacidad de estos sitios web. Asegúrese de que el vínculo externo corresponde a un sitio web que sea compatible con iFrames.

La URL se crea a partir del valor especificado mediante el atributo url y los parámetros de URL especificados.

El fragmento de XML anterior define un componente de IFRAME que muestra una página solicitada desde una URL generada dinámicamente. Esta URL se crea a partir de la cadena "http://www.bing.com/search", el parámetro estático de nombre "hl" y el valor "en", así como el parámetro dinámico de nombre "q" y el valor sustituido en tiempo de ejecución por el nombre del usuario de la aplicación IDD conectado actualmente.

Por ejemplo, si el usuario de la aplicación IDD conectado tiene el nombre de inicio de sesión "admin", este componente muestra una página solicitada desde la siguiente URL:

```
http://www.bing.com/search?q=admin&hl=en
```

IGOOGLE

Los componentes de IGOOGLE (tipo = "IGOOGLE") se utilizan para incrustar JavaScript importado desde una URL externa (creada a partir del valor especificado mediante el atributo URL y los parámetros de URL especificados) y código HTML personalizado.

Un componente definido como `' <externalLink name="component_name" type="IGOOGLE" url="<URL externa>"/>'` añade un componente del Espacio de trabajo Inicio creado a partir de una única etiqueta HTML <script>:

```
<script url="external URL"/>
```

Diseño del espacio de trabajo Inicio

Los componentes del Espacio de trabajo Inicio se disponen en una cuadrícula, de arriba a abajo y de izquierda a derecha.

De forma predeterminada, estos componentes se ordenan de la siguiente manera: lista de tareas, informes y componentes personalizados.

Puede especificar el orden predeterminado mediante el elemento dashboardLayout. Los usuarios de la aplicación IDD pueden personalizar aún más el conjunto de componentes que verán, así como el orden de esos componentes. Estos cambios se guardan como parte de las preferencias del usuario.

El diseño del Espacio de trabajo Inicio se define conceptualmente como una cuadrícula con *n* columnas. Cada elemento puede ocupar una fila y una o más celdas de la fila. No todas las celdas de una fila deben incluir elementos. En tal caso, el resto de la fila estará vacío.

El siguiente fragmento de código muestra un ejemplo de un diseño del Espacio de trabajo Inicio de dos columnas.

```
<dashboardLayout columns="2">
      <dashboardLayoutItem name="my_tasks" type="TASKS" columns="*"/>
                        <dashboardLayoutItem name="xref_composition"    type="REPORT" />
      <dashboardLayoutItem name="igoogle_visualization" type="EXTERNAL_LINK"/>
      <dashboardLayoutItem name="google_username" type="EXTERNAL_LINK"/>
  </dashboardLayout>
```

Cada elemento del diseño se representa con el elemento dashboardLayoutItem, que tiene los siguientes atributos posibles:

Parámetro	Tipo	Descripción
nombre	cadena	ID de elemento único dentro del elemento dashboardLayout.
tipo	TASKS, REPORT o EXTERNAL_LINK	Tipo del elemento.
Columnas	número o "*"	Número de columnas ocupadas por el elemento. El valor predeterminado es "1". El símbolo especial "*" es para elementos que ocupan toda la fila.

El orden de los elementos en el Espacio de trabajo Inicio es el orden en el que se especifican en el elemento dashboardLayout.

Fichas secundarias personalizadas

Se pueden añadir fichas secundarias personalizadas a un área de asunto.

Se muestran en el mismo panel de fichas que las fichas secundarias de uno a muchos y de muchos a muchos. Se configuran mediante el elemento externalLinkChild.

Las fichas secundarias personalizadas con el tipo externalLinkChild se configuran para mostrar el contenido de una página HTML solicitada desde una URL externa. A continuación, se incluye un ejemplo de la definición de externalLinkChild:

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
               <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
         </layout>
      </primaryObject>
```

```
    <externalLinkChild name="org_name_bing_search_child" displayName="Bing Search">
       <externalLink name="org_name_bing_search_action_link" type="IFRAME"
          url="http://www.bing.com/search">
          <param name="q" bddParamName="C_PARTY|ORGANIZATION_NAME"/>
                      <param name="hl" staticValue="en"/>
       </externalLink>
    </externalLinkChild>
 </subjectArea>
```

Atributos de fichas secundarias personalizadas

Las fichas secundarias personalizadas se definen mediante el elemento externalLinkChild de un área de asunto.

Este elemento tiene los siguientes atributos:

Atributos	Descripción
nombre	Nombre usado internamente de esta ficha secundaria personalizada. Debe ser único entre todas las fichas secundarias personalizadas. Utilice únicamente caracteres alfanuméricos; no se permiten caracteres especiales.
displayName	Título de la ficha secundaria. El valor especificado en el XML de configuración se utiliza de forma predeterminada, pero se puede reemplazar en el paquete de recursos.

Propiedades de vínculo externo

El elemento externalLinkChild debe contener el elemento externalLink, que define la URL que aparece en la ficha secundaria.

Este elemento tiene los siguientes atributos:

Atributos	Descripción
nombre	Nombre usado internamente de este vínculo. Debe ser único en todos los vínculos externos. Utilice únicamente caracteres alfanuméricos; no se permiten caracteres especiales.
tipo	Los vínculos externos definidos para fichas secundarias personalizadas deben tener el tipo "IFRAME".
url	La URL que se muestra en la ficha secundaria personalizada.

Parámetros

Los parámetros se pueden anexar a la URL mediante el elemento param. Los parámetros de URL pueden ser estáticos o dinámicos.

Parámetros estáticos

Los parámetros estáticos tienen valores predefinidos especificados en la configuración.

Aquí se incluye un ejemplo de definición de parámetro estático (que utiliza el atributo staticValue):

```
<param name="hl" staticValue="en"/>
<param name="loginName" bddParamName="USERNAME"/>
```

Parámetros dinámicos

Los valores de los parámetros dinámicos se sustituyen en tiempo de ejecución.

La definición de un parámetro dinámico contiene el atributo bddParamName y el valor de este atributo se sustituye por los siguientes datos disponibles en tiempo de ejecución:

- Nombre de inicio de sesión del usuario de la aplicación IDD conectado (bddParamName="USERNAME")
- Nombre de inicio de sesión cifrado del usuario de la aplicación IDD conectado (bddParamName="USERNAME_ENCRYPTED")
- Nombre de inicio de sesión cifrado del usuario de la aplicación IDD conectado (bddParamName="USERNAME_ENCRYPTED")
- Contraseña cifrada del usuario de la aplicación IDD conectado (bddParamName="PASSWORD_ENCRYPTED")
- Columna del sistema 'ROWID_OBJECT ' del elemento PrimaryObject del área de asunto (bddParamName="<UID de tabla de primaryObject>|ROWID_OBJECT")
- Para elementos PrimaryObjects habilitados para la línea temporal, el formato largo en milisegundos de la fecha efectiva del elemento PrimaryObject del área de asunto (bddParamName="EffectiveDate")
- Datos de las columnas del elemento PrimaryObject del área de asunto (bddParamName="<UID de columna de la columna de PrimaryObject>")
- Datos de las columnas de los elementos secundarios de uno a uno lógicos del área de asunto (bddParamName=" <UID de columna de la columna secundaria de uno a uno de PrimaryObject>")
- Puede especificar los parámetros @LOCALHOST@ y @LOCALPORT@ en el archivo de configuración de Informatica Data Director. Cuando una URL de externalLinkAction de devolución de llamada apunta a una aplicación implementada en el mismo servidor que MDM Hub, debe especificar de forma dinámica el nombre del host local en la URL. Especifique dinámicamente el nombre del host local en la URL de modo que la ventana externalLinkAction pueda interactuar con la ventana del navegador de Informatica Data Director sin restricciones de navegador entre sitios. El siguiente código muestra cómo definir el elemento externalLinkAction con el parámetro @LOCALHOST@ en la URL:

```
<externalLinkAction callback="false" displayName="View Lineage"
name="per_view_lineage">
<externalLink name="per_view_lineage_link" type="IFRAME" url="http://@LOCALHOST@:
10250/external_app "/>
</externalLinkAction>
```

Para transferir nombres de usuario y contraseñas cifrados, debe definir la clave de cifrado. Debe definir la clave de cifrado del archivo de configuración de IDD (IDDConfig.xml) con el elemento `encryptionKey`.

El siguiente código de ejemplo muestra cómo definir el elemento `encryptionKey`:

```
<bddApplication xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                name="test"
                displayName="Test BDD application"
                defaultLocale="en"
                sessionTimeoutMinutes="30"
                xsi:noNamespaceSchemaLocation="siperian-bdd-config-6.xsd">
    <description>Description for test ds app configuration</description>
    <configSubVersion>2</configSubVersion>
    <encryptionKey>secretKey</encryptionKey>
...
...
                <externalLinkAction callback="true" displayName="Test callback"
name="person_test_callback_action">
                 <externalLink name="person_test_callback" type="IFRAME"
url="test_external.html">
                 <param bddParamName="SiperianRowID" name="SiperianRowID" />
                 <param bddParamName="EffectiveDate" name="date" />
                 <param bddParamName="USERNAME_ENCRYPTED" name="username" />
                 <param bddParamName="PASSWORD_ENCRYPTED" name="password" />
                 </externalLink>
                </externalLinkAction>
```

Por ejemplo, en el archivo de configuración, puede definir la clave de cifrado de IDD de la siguiente manera:

```
<encryptionKey>{C5869460-4830-4231-9D6E-8A073A97F099}</encryptionKey>
```

Acciones personalizadas

Una *acción personalizada* es una solicitud de HTTP invocada en una ventana de navegador emergente.

Se pueden configurar acciones personalizadas para las siguientes áreas de la aplicación IDD:

- SubjectArea (la definición de acción se coloca dentro de la definición de SubjectArea). Estas acciones personalizadas se añaden al menú Más acciones del área de asunto (este menú está disponible en la vista de datos y la vista de jerarquía) y al menú contextual que se muestra para los nodos en la vista de jerarquía.
- Búsqueda de SubjectArea (la definición de acción se coloca dentro de la definición de Búsqueda de SubjectArea). Estas acciones personalizadas se añaden al menú contextual de resultados de búsqueda.
- Elementos secundarios de uno a muchos y de muchos a muchos (la definición de acción se coloca dentro de la definición del elemento secundario). Estas acciones personalizadas se añaden al menú contextual de la tabla secundaria.
- Vista de jerarquía (la definición de acción se coloca dentro de la definición hmConfiguration). Estas acciones personalizadas se añaden al menú Más acciones de la vista de jerarquía.

Nota: Según las funciones de usuario, no se pueden configurar las acciones personalizadas.

Las acciones personalizadas se definen mediante el elemento externalLinkAction, que tiene los siguientes atributos:

Atributos	Descripción
nombre	Nombre usado internamente de esta acción personalizada. Este nombre debe ser único en todas las acciones personalizadas.
displayName	Texto para el elemento de menú creado para esta acción personalizada. El valor especificado en el XML de configuración se utiliza de forma predeterminada, pero se puede reemplazar en el paquete de recursos.
devolución de llamada	El atributo debe tener el valor "true" para la acción de devolución de llamada (consulte más abajo una descripción de acciones de devolución de llamada).
windowWidth	Ancho de la ventana modal que muestra el resultado de una acción de devolución de llamada. El valor predeterminado es 700.
windowHeight	Ancho de la ventana modal que muestra el resultado de una acción de devolución de llamada. El valor predeterminado es 600.

El elemento externalLinkAction debe contener un elemento externalLink que define la URL de acción personalizada.

El elemento externalLink definido para externalLinkAction admite la misma configuración que el elemento externalLink definido para externalLinkChild. Para obtener más información, consulte la descripción de externalLink incluida en la sección "Fichas secundarias personalizadas" anterior de este documento.

En lo que respecta al elemento externalLink de la ficha secundaria personalizada, el elemento externalLink definido para externalLinkAction admite parámetros dinámicos sustituidos en tiempo de ejecución. Cuando la acción se ejecuta para varios registros (por ejemplo, si el usuario de la aplicación IDD selecciona varios registros en los resultados de búsqueda y ejecuta una acción desde el menú contextual de búsqueda) y la URL de la acción tiene un parámetro dinámico sustituido por los datos de las columnas del registro. El valor del parámetro se crea a partir de los valores de las columnas de todos los registros seleccionados,

separados por comas. Por ejemplo, una acción se define para la búsqueda de organización con la siguiente definición de URL:

```
<externalLink name="org_name_google_search_action_link" type="IFRAME"
        url="http://www.google.com/search">
      <param name="q" bddParamName="C_PARTY|ORGANIZATION_NAME"/>
      <param name="hl" staticValue="en"/>
   </externalLink>
```

Cuando el usuario de la aplicación IDD selecciona tres organizaciones en los resultados de búsqueda con los nombres 'name1', 'name2', 'name3' y ejecuta la acción, la URL de la acción será la siguiente:

```
http://www.google.com/search?q=name1,name2,name3&hl=en
```

Acción personalizada estándar

Una acción estándar personalizada abre una nueva ventana del navegador que muestra la página solicitada desde una URL externa.

Aquí se incluye un ejemplo de una acción personalizada definida para SubjectArea:

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
            …
         </layout>
      </primaryObject>
      <externalLinkAction name="org_name_google_search_action" displayName="Google
Search">
         <externalLink name="org_name_google_search_action_link"
               type="IFRAME" url="http://www.google.com/search">
            <param name="q" bddParamName="C_PARTY|ORGANIZATION_NAME"/>
                  <param name="hl" staticValue="en"/>
         </externalLink>
      </externalLinkChild>
      …
   </subjectArea>
```

Si el usuario de la aplicación IDD abre la organización llamada 'Informatica' y selecciona el elemento 'Búsqueda en Google' en el menú 'Más acciones', IDD abre una ventana que muestra la siguiente URL:

```
http://www.google.com/search?q=Informatica&hl=en
```

Acción personalizada con devolución de llamada

Una acción personalizada también puede incluir una devolución de llamada.

Esto resulta útil cuando el proceso externo invocado por la acción personalizada puede modificar los datos del área de asunto. Después de realizar esta modificación, la acción personalizada puede invocar la devolución de llamada para ordenar a la aplicación IDD que actualice el área de asunto.

IDD define una función de JavaScript llamada refreshObject para actualizar el área de asunto. Esta función requiere un parámetro, el ID de IDD interno del registro modificado. Para que este ID esté disponible para aplicaciones externas, la solicitud de HTTP de la acción personalizada debe transferirlo como un parámetro (en este caso, la aplicación externa puede obtener este ID de una solicitud y devolverlo a la aplicación IDD). Para añadir un ID de registro interno a una URL de acción, se debe añadir un parámetro de URL dinámica con bddParamName='SiperianRowID' a la definición de la URL (consulte el ejemplo de definición de acción de devolución de llamada más adelante en esta sección).

Cuando una acción personalizada de devolución de llamada se invoca, IDD abre una ventana modal que contiene el elemento <iframe>, que muestra la página HTML recibida como resultado de solicitud de HTTP

de la acción. Esta página HTML puede llamar a la función refreshObject mediante el siguiente código de JavaScript:

```
var modifiedRecordID = // get modified record ID from HTTP request
    var opener = window.parent.dialogArguments;
    opener.refreshObject(modifiedRecordID);
```

Es posible acceder a la ventana modal en la que se muestra el resultado de la solicitud de acción desde JavaScript como window.parent. Por ejemplo, una página HTML generada como respuesta a una acción puede contener la siguiente función de JavaScript, que cierra la ventana modal de la acción y actualiza las vistas de IDD:

```
function closeWindowAndRefreshBDD() {
      var modifiedRecordID = // get modified record ID from HTTP request
      var opener = window.parent.dialogArguments;
      opener.refreshObject(modifiedRecordID);
      window.parent.close();
   }
```

Nota importante: Debido a las restricciones de seguridad del navegador, la página HTML puede llamar a la función de JavaScript definida en la aplicación IDD solo si esta página está ubicada en el mismo dominio que la aplicación IDD (el mismo servidor de aplicaciones en el que está implementada la aplicación IDD sirve esta página).

Aquí se incluye un ejemplo de la acción de devolución de llamada definida para SubjectArea:

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
            …
         </layout>
      </primaryObject>
      <externalLinkAction callback="true" name="organization _callback_action"
            displayName="Org Callback">
         <externalLink      name="org_name_google_search_action_link"
               type="IFRAME" url="http://external/application/url">
            <param name="InternalID" bddParamName="SiperianRowID"/>
            <param name="organization_id" bddParamName="C_PARTY|ROWID_OBJECT"/>
         </externalLink>
      </externalLinkChild>
      …
</subjectArea>
```

Si un usuario de la aplicación IDD abre una organización con ROWID_OBJECT=1222 y, a continuación, invoca esta acción personalizada, IDD abre una ventana modal que muestra la página solicitada desde la siguiente URL:

```
http://external/application/url?InternalID=BASE_OBJECT.C_PARTY|1222&organization_id=1222
```

A continuación, esta página puede llamar a la función de JavaScript refreshObject de la aplicación IDD con el parámetro 'BASE_OBJECT.C_PARTY|1222' (este es el ID interno del registro de la organización abierta), que hace que la aplicación IDD actualice todas las vistas abiertas para este registro.

Seguridad para extensiones personalizadas

El acceso a fichas secundarias personalizadas y acciones personalizadas se controla mediante SAM.

Cuando una aplicación IDD se implementa, se crean recursos personalizados para cada ficha personalizada y para cada acción personalizada definida en la configuración de IDD. Los privilegios de estos recursos deben configurarse con la Consola del concentrador.

Fichas secundarias personalizadas

Para fichas secundarias personalizadas, los recursos se denominan de la siguiente manera:

`CUSTOM_EXTENSION/CUSTOM_CHILD_TAB:<name>`

donde <*name*> es el nombre exclusivo de la ficha secundaria tal y como se especifica en la configuración.

Si el usuario de la aplicación IDD tiene privilegios de lectura (READ) en el recurso de la ficha correspondiente, podrá ver una ficha secundaria personalizada.

Acciones personalizadas

Para las acciones personalizadas, los recursos se denominan de la siguiente manera:

`CUSTOM_EXTENSION/CUSTOM_ACTION:<name>`

donde <*name*> es el nombre exclusivo de la acción tal y como se especifica en la configuración.

Una acción personalizada se muestra y puede ejecutarse si el usuario de la aplicación IDD tiene el privilegio de ejecución (EXECUTE) para el recurso de la acción correspondiente.

Salidas de usuario

Las salidas de usuario permiten añadir lógica empresarial personalizada a operaciones de Informatica Data Director estándar. Puede usar las salidas de usuario dentro del espacio de trabajo Datos.

Las salidas de usuario se implementan en Java. Para obtener información detallada sobre las interfaces que se utilizan para implementar salidas de usuario, consulte el Javadoc para `siperian-bdd.jar` incluido en el kit de recurso de MDM Hub. En el kit de recursos también se incluyen salidas de usuario de ejemplo. El conjunto de salidas de usuario incluye un proyecto de Ant que puede usar como una plantilla para construir un archivo JAR de salida de usuario.

Salidas de usuario y marco de Entidad 360

Las salidas de usuario no están admitidas para el uso con espacios de trabajo creados a partir del marco de Entidad 360, como el espacio de trabajo **Inicio** y el espacio de trabajo de entidad.

Con el marco de Entidad 360, puede usar las funciones de limpieza y la validación del lado del servidor para reemplazar alguna funcionalidad de las salidas de usuario. Para obtener más información, consulte la *Guía de la herramienta de aprovisionamiento de Multidomain MDM*.

Nota: Para la compatibilidad con versiones anteriores, puede continuar usando las salidas de usuario con el espacio de trabajo **Datos**. Para visualizar el espacio de trabajo **Datos**, habilite la propiedad `cmx.dataview.enabled` en el archivo `cmxserver.properties`. Para obtener más información, consulte la *Guía de configuración de Multidomain MDM*.

Operaciones de salida de usuario

Las salidas de usuario tienen definidas operaciones y puntos de entrada.

Para cada área de asunto, puede implementar salidas de usuario para añadir funcionalidades personalizadas a las siguientes operaciones:

- Guardar

- Enviar para aprobar
- Operaciones de tarea
- Fusionar
- Marcar no coincidente
- Operaciones personalizadas
- Relación de guardado de HM
- Operaciones personalizadas de HM
- Abrir

La siguiente tabla describe los puntos de entrada de la salida de usuario disponibles para cada operación. Guardar, Enviar para aprobar y las Operaciones de tareas son variaciones del proceso de guardar los cambios en la servicio del área de asunto y proporcionan el mismo conjunto de puntos de entrada.

Operación	Punto de entrada	Descripción
Guardar, Enviar para aprobar, Operaciones de tareas	beforeValidation	**Nota:** Este punto de entrada ya no es compatible. Utilice el punto de entrada beforeEverything en su lugar.
	afterValidation	**Nota:** Este punto de entrada ya no es compatible. Utilice el punto de entrada beforeEverything en su lugar.
	beforeEverything	Se llama a este punto de entrada antes de que se realice cualquier proceso. Utilícelo para realizar una validación o aumento personalizados de los datos en el área de asunto. Informatica Data Director guarda los cambios que la salida de usuario realiza en los datos del área de asunto. Puede notificar errores, advertencias y confirmaciones. Puede establecer las fechas de inicio y fin de un período. Se ejecuta fuera de la transacción para guardar.
	beforeSave	Se le llama después de realizar una búsqueda de duplicados, justo antes de realizar el guardado compuesto. Utilícelo para ejecutar la lógica empresarial personalizada que aumenta los datos en el área de asunto. Informatica Data Director guarda los cambios que la salida de usuario realiza en los datos del área de asunto. Puede notificar errores. Se ejecuta como parte de la transacción compuesta para guardar. Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.
	afterSave	Se le llama después de que se guarden los cambios en el área de asunto. Utilícelo para realizar el mantenimiento de los datos que no forman parte del área de asunto. Puede notificar errores que revierten la transacción. Se ejecuta como parte de la transacción compuesta para guardar. Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.

Operación	Punto de entrada	Descripción
	afterEverything	Se le llama después de que se confirme la transacción de guardado. Utilícelo para proporcionar notificaciones de usuario o para realizar el mantenimiento de los datos que no forman parte del área de asunto cuando los cambios no se pueden ejecutar como parte de la transacción. Puede notificar advertencias. Se ejecuta fuera de la transacción para guardar.
Fusionar	beforeEverything	Se llama a este punto de entrada antes de que se realice cualquier proceso. Utilícelo para realizar una validación o aumento personalizados de los datos en el área de asunto. Puede notificar errores, advertencias y confirmaciones. Puede establecer las fechas de inicio y fin de un período. Se ejecuta fuera de la transacción para guardar.
	beforeMerge	Se le llama justo antes de que se realice la fusión. Utilícelo para ejecutar la lógica empresarial personalizada para proporcionar mensajes de error o de confirmación. Puede notificar errores. Se ejecuta como parte de la transacción de fusión. Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.
	afterMerge	Se le llama después de que se complete la operación de fusión. Utilícelo para realizar el mantenimiento de los datos que no forman parte del área de asunto. Puede notificar errores que revierten la fusión. Se ejecuta como parte de la transacción de fusión. Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.
	afterEverything	Se le llama después de que se confirme la transacción de fusión. Utilícelo para proporcionar notificaciones de usuario o para realizar el mantenimiento de los datos que no forman parte del área de asunto cuando los cambios no se pueden ejecutar como parte de la transacción. Puede notificar advertencias. Se ejecuta fuera de la transacción.
Marcar no coincidente	beforeEverything	Se llama a este punto de entrada antes de que se realice cualquier proceso. Utilícelo para realizar una validación o aumento personalizados de los datos en el área de asunto. Puede notificar errores, advertencias y confirmaciones. Puede establecer las fechas de inicio y fin de un período. Se ejecuta fuera de la transacción para guardar.

Operación	Punto de entrada	Descripción
	beforeMarkNotAMatch	Se le llama justo antes de que se realice la operación "no es una coincidencia". Utilícelo para ejecutar la lógica empresarial personalizada para proporcionar mensajes de error o de confirmación. Puede notificar errores. Se ejecuta como parte de la transacción "no es una coincidencia". Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.
	afterMarkNotAMatch	Se le llama después de que se realice la operación "no es una coincidencia". Utilícelo para realizar el mantenimiento de los datos que no forman parte del área de asunto. Puede notificar errores que revierten la fusión. Se ejecuta como parte de la transacción "no es una coincidencia". Las solicitudes de SIF al Almacén de referencias operativas formarán parte de esta transacción.
	afterEverything	Se le llama después de que se confirme la transacción "no es una coincidencia". Utilícelo para proporcionar notificaciones de usuario o para realizar el mantenimiento de los datos que no forman parte del área de asunto cuando los cambios no se pueden ejecutar como parte de la transacción. Puede notificar advertencias. Se ejecuta fuera de la transacción.
Operación de usuario	processOperation	Se le llama cuando el usuario de Informatica Data Director invoca la salida de usuario de la operación personalizada en el menú Más acciones de la servicio. Utilícelo para ejecutar lógica empresarial personalizada. La salida de usuario puede devolver mensajes de error o de advertencia. La servicio se actualiza si esta operación finaliza sin errores de modo que los cambios en el área de asunto realizados por la salida de usuario se reflejen en Informatica Data Director.
Relación de guardado de HM	beforeEverything	Se llama a este punto de entrada antes de que se realice cualquier proceso. Utilícelo para realizar una validación o aumento personalizados de la relación. Puede notificar errores, advertencias y confirmaciones. Puede establecer las fechas de inicio y fin de un período. Se ejecuta fuera de la transacción para guardar.
	afterValidation	Se le llama después de que se complete la ejecución de la validación y la función de limpieza. Utilícelo para realizar una validación o aumento personalizados de la relación. Puede notificar errores, advertencias y confirmaciones. Se ejecuta fuera de la transacción para guardar.

Operación	Punto de entrada	Descripción
	beforeSave	Se le llama justo antes de guardar. Utilícelo para ejecutar la lógica empresarial personalizada que aumenta los datos asociados con la relación. Puede notificar errores. Se ejecuta como parte de la transacción de guardado. Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.
	afterSave	Se le llama después de que se guarden los cambios de relación. Utilícelo para realizar el mantenimiento de los datos asociados con la relación. Puede notificar errores que revierten el guardado. Se ejecuta como parte de la transacción de guardado. Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.
	afterEverything	Se le llama después de que se confirme la transacción de guardado. Utilícelo para proporcionar notificaciones de usuario o para realizar el mantenimiento de los datos asociados con la relación cuando los cambios no se pueden ejecutar como parte de la transacción. Puede notificar advertencias. Se ejecuta fuera de la transacción para guardar.
Operación de usuario de HM	processOperation	Se le llama cuando el usuario de Informatica Data Director invoca la salida de usuario de la operación personalizada en el menú Más acciones de la servicio. Utilícelo para ejecutar lógica empresarial personalizada. La salida de usuario puede devolver mensajes de error o de advertencia. La salida de usuario indica qué partes del gráfico necesitan actualizarse como resultado de la operación de salida de usuario.
Abrir	beforeOpen	Se le llama antes de que se realice una operación de apertura. Utilícelo para marcar columnas como de solo lectura en el modo de edición y para sobrescribir valores de columna. Puede notificar errores, advertencias, confirmaciones y mensajes personalizados. Se ejecuta fuera de la transacción de apertura.
	afterOpen	Se le llama después de que se complete la operación de apertura. Utilícelo para enviar diversas notificaciones a los datos del área de asunto. Además, puede utilizarlo para realizar una comprobación personalizada de los datos cargados en la base de datos. Puede notificar errores, advertencias, confirmaciones y mensajes personalizados. Se ejecuta como parte de la transacción para abrir. Las solicitudes de SIF al Almacén de referencias operativas forman parte de esta transacción.

Cada salida de usuario se proporciona con los siguientes datos, que se describen en detalle en el Javadoc:

- los datos del área de asunto sobre los que se opera

- un objeto SiperianClient que se puede utilizar para realizar operaciones de SIF en la base de datos del Almacén de referencias operativas, así como el ID del Almacén de referencias operativas y las credenciales de usuario que se utilizarán en solicitudes de SIF
- datos específicos de la operación

Creación de salidas de usuario

Los pasos básicos para generar salidas de usuario para una aplicación IDD son los siguientes:

1. Desarrolle el código Java de la salida de usuario.
2. Compile y genere un archivo .jar que contenga las clases de salida de usuario.
   Utilice el archivo `siperian-bdd.jar` del kit de recurso de MDM. Este archivo contiene todas las definiciones de interfaz y clases específicas de IDD necesarias para generar la implementación de salidas de usuario. Para obtener más información, consulte la *Guía del kit de recursos de Multidomain MDM*.

   Nota: El archivo .jar debe llamarse `UserExitsImplementation.jar`.
3. Utilice el Administrador de configuración de IDD para importar el archivo .jar en la aplicación IDD (también puede incluir el archivo .jar en un archivo .zip de la aplicación IDD importado).
4. Registre clases de salida de usuario con el área de asunto.
5. Implemente la aplicación IDD.

Configuración de una salida de usuario

Las salidas de usuario se configuran por área de asunto.

Un área de asunto puede tener salidas de usuario definidas para cada una de las operaciones de salida de usuario descritas anteriormente en esta sección.

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
            …
         </layout>
      </primaryObject>
      …
      <userExits className="com.siperian.bdd.userexits.sample.SaveHandler"/>
      <userExits className="com.siperian.bdd.userexits.sample.SendForApprovalHandler"/>
      <userExits className="com.siperian.bdd.userexits.sample.CustomActionProvider"
         actionName="Custom User Exit"/>
   </subjectArea>
```

El siguiente fragmento de código es un ejemplo de configuración de ClassName para las salidas de usuario de relación de guardado de HM del archivo IDDConfig.xml.

```
<hmRelationshipTypes>
<hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.contains member">
<layout columnsNum="2">
<column columnUid="C_RL_PARTY_GROUP|HUB_STATE_IND" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
</layout>
<userExit className="com.siperian.bdd.userexits.sample.HMRelationshipSaveHandler"/>
<userExit className="com.siperian.bdd.userexits.sample.HMRelationshipHandler"/>
</hmRelationshipType>
</hmRelationshipTypes>
```

Nota: Según las funciones de usuario, no se pueden configurar las salidas de usuario.

Configuración de una salida de usuario para establecer la fecha de inicio y la fecha de finalización de un período

Para establecer la fecha de inicio y la fecha de finalización de un período en Informatica Data Director, puede usar la interfaz `IEffectivePeriodSetters` de la salida de usuario beforeEverything.

Nota: La interfaz `IEffectivePeriodSetters` solo funciona con el controlador Guardar. No funciona con el controlador Guardar de relación de HM.

El siguiente fragmento de código es un ejemplo de cómo establecer las fechas efectivas de inicio y finalización:

```
// get existing start end date from effective period
IEffectivePeriodSetters epd = ((IEffectivePeriodSetters)
getOperationContext().getValue(OperationContext.EFFECTIVE_PERIOD));
Date stDate = epd.getStartDate();
Date eDate = epd.getEndDate();
// set new effective start and end date
epd.setPeriod(DateUtils.addDays(stDate, 1), DateUtils.addDays(eDate, -1));
```

Mensajes de salida de usuario

Las salidas de usuario pueden devolver un mensaje (como un error, advertencia o confirmación) para mostrarlo al usuario.

IDD gestiona estos mensajes del mismo modo que sus propios mensajes. Cada mensaje tiene un código que es una clave al paquete de recursos ErrorCodeBundle.properties. IDD busca el nivel de error (error, advertencia o confirmación) y el texto del mensaje en este paquete de recursos.

Nota: Asegúrese de utilizar códigos exclusivos para todos los mensajes personalizados.

Estas cadenas de mensajes se pueden localizar al igual que otras cadenas.

Los mensajes pueden tener parámetros que se sustituyen con datos especificados en la salida de usuario. Estos parámetros se gestionan mediante la clase MessageFormat de Java.

El formato de los mensajes en ErrorCodeBundle.properties es:

```
error code=error level|title|main message[|secondary message]
```

donde

Elemento	Descripción
Código de error	Clave única para el mensaje.
Nivel de error	Uno de los siguientes valores: ERROR, WARNING o CONFIRMATION.
Título	Título para el cuadro de diálogo. El título debe describir la ubicación y el contexto en el que se ha producido el problema. Si no se especifica, el título será 'Informatica Data Director'.
mensaje principal	Mensaje de error principal. Este texto debe describir el problema desde el punto de vista del usuario de la aplicación IDD, en lugar de un punto de vista técnico interno. Por ejemplo, algo similar a `"Problema al guardar xxx", en lugar de "Error de colocación"`.
Mensaje secundario	Parte secundaria del mensaje que indica al usuario de la aplicación IDD qué hacer respecto al problema. En el cuadro de diálogo, esta parte estará separada del mensaje principal al menos por una línea en blanco. Este mensaje no debe ser demasiado largo.

Solución de problemas

Al intentar comprender por qué una salida de usuario no funciona correctamente, utilice las herramientas estándar siguientes.

Herramienta	Descripción
Registros	Las excepciones que se generan en la salida de usuario se pueden encontrar en los registros de Informatica MDM Hub. La salida de usuario también puede crear entradas en el registro mediante log4j, como se muestra en las salidas de usuario de ejemplo.
Depurador	El depurador de Java se puede utilizar para completar paso a paso la ejecución del código. Esto es igual a depurar cualquier aplicación Java implementada en un entorno de servidor de aplicaciones.

Localización

Los paquetes de recursos contienen las cadenas que aparecen en una aplicación Informatica Data Director.

Existen cuatro conjuntos de paquetes de recursos:

- BDDBundle
- ErrorCodeBundle
- MessagesBundle
- MetadataBundle

Cada conjunto incluye el archivo predeterminado, un archivo de marcador de posición de idioma inglés y versiones localizadas del archivo, si existen.

Por ejemplo, para el conjunto MessagesBundle, encontramos el archivo predeterminado `MessagesBundle.properties` y el archivo en inglés de marcador de posición `MessagesBundle_en.properties`.

Cada archivo de paquete de recursos es un archivo de propiedades con codificación UTF-8. Cada entrada del archivo es un par de nombre y valor, como <*nombre*>=<*valor*>.

- <*nombre*> es un valor fijo al que hace referencia la aplicación Informatica Data Director. No es posible cambiar este valor.
- <*valor*> es la parte que se puede localizar.

Algunos ejemplos:

```
title=Business Data Director
locale=Locale
search=Search
```

Para agregar archivos de paquetes de mensajes a la aplicación Informatica Data Director, puede incluirlos en el archivo .zip de la aplicación que importe. Como alternativa, también puede importar archivos de paquetes de mensajes directamente en una aplicación existente en Informatica Data Director.

Nota: En el archivo `MetadataBundle.properties` localizado, evite los espacios en los nombres de los tipos de relación del Administrador de jerarquía y los tipos de jerarquía. Informatica Data Director reemplazará los espacios por guiones bajos cuando muestre estos valores localizados.

Cuando cree por primera vez una aplicación Informatica Data Director, Informatica Data Director Configuration Manager generará los paquetes de recursos predeterminados de cada tipo. Estos paquetes de recursos tienen entradas para todas las etiquetas que se utilizan en la aplicación Informatica Data Director.

Para cambiar o localizar estos paquetes de recursos, realice los pasos siguientes:

1. Exporte la aplicación Informatica Data Director.
2. Extraiga los archivos del archivo .zip de la aplicación.
3. Cree un paquete de recursos con el sufijo de código de idioma ISO correspondiente del idioma que haya seleccionado.
4. En el idioma seleccionado, edite las etiquetas en el paquete de recursos.

   Nota: Para localizar las etiquetas de los grupos de área de asunto, los nombres del área de asunto y del grupo de menú lógico, utilice el archivo `BDDBundle.properties` con el sufijo de código de idioma apropiado.
5. Repita los pasos 3 y 4 para cada paquete de recursos que desee localizar.

Definición del idioma de visualización predeterminado de la página de inicio de sesión y el Administrador de configuración

El idioma de su navegador web determina el idioma de visualización de la página de inicio de Informatica Data Director y Configuration Manager. Puede ejecutar un script para establecer el idioma que se muestre en la página de inicio de sesión y en la interfaz de usuario de Configuration Manager.

El script no establece el idioma de visualización predeterminado de la aplicación Informatica Data Director. Puede establecer el idioma de visualización de la aplicación Informatica Data Director en la opción de menú Cambiar idioma en su nombre de usuario. Cuando el idioma de visualización predeterminado para la página de inicio y Configuration Manager, Informatica Data Director ignorará la configuración de idioma de su navegador web.

1. Ejecute el siguiente script para establecer el código de idioma para el parámetro globalLocale:

```
INSERT
INTO CMX_SYSTEM.C_REPOS_DS_PREF_DETAIL
  (
    ROWID_DS_PREF_DETAIL,
    CREATE_DATE,
    CREATOR,
    LAST_UPDATE_DATE,
    UPDATED_BY,
    ROWID_DS_PREF,
    NAME,
    VALUE
  )
  VALUES
  (
    'MST1.5AB',
    sysdate,
    'admin',
    sysdate,
    'admin',(SELECT ROWID_DS_PREF
FROM CMX_SYSTEM.C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___'),
    'globalLocale',
    '<ISO language code>'
  );
```

   El código de idioma ISO es un código de dos letras que representa el idioma. Por ejemplo, el código de país 'ja' representa el japonés. Si no define un código de idioma ISO válido, el idioma de visualización será el inglés.
2. Reinicie el servidor de aplicaciones.

Páginas de error personalizadas

Puede configurar Informatica Data Director (IDD) para visualizar páginas de error personalizadas en lugar de los mensajes de error del servidor de aplicaciones. Por ejemplo, cuando un usuario introduce una URL incorrecta, puede configurar IDD para que redireccione el usuario hacia la página de inicio de sesión o a una página de error más descriptiva.

Para crear páginas de error personalizadas, edite el archivo `web.xml` y configure la página que desee que aparezca cuando un usuario recibe un error en una sesión de IDD.

El archivo `seed.log` reside en la siguiente ubicación:

`<directorio de instalación de infamdm>/hub/server/siperian-mrm.ear/zds-gui.war`

Configurar una página de error personalizada

Para crear páginas de error personalizadas, edite el archivo `web.xml` y configure la página que desee que aparezca para un código de error determinado.

1. Extraiga los archivos del directorio `zds-gui.war`.

   El directorio contiene varios archivos, incluido web.xml.

2. Use un editor de texto para editar el archivo `web.xml`.
   En el siguiente ejemplo, la respuesta 404 HTTP de la aplicación redirige al usuario a la página `error_custom.html`.

   ```
   <error-page>
   <error-code>404</error-code>
   <location>/error_custom.html</location>
   </error-page>
   ```

   Nota: Para asegurarse de que la página personalizada se muestra para los usuarios, añada la página `error_custom.html` al directorio zds-gui.war.

3. Guarde el archivo `web.xml` y, a continuación, vuelva a implementar la aplicación de IDD.

Ayuda en línea

De forma predeterminada, una aplicación de Informatica Data Director (IDD) incluye la ayuda de la Guía del usuario. También puede añadir ayuda personalizada.

Ayuda de la Guía del usuario

En la ayuda de la Guía del usuario se describen las tareas que se pueden llevar a cabo con una aplicación de IDD. Por ejemplo, en la ayuda se describe cómo se añaden o se fusionan las entidades de negocio. El desarrollador de las aplicaciones de IDD pueden reemplazar el archivo de ayuda enviado con un archivo de ayuda revisado. También hay disponibles versiones traducidas del archivo de ayuda. Si cambia la configuración regional de una aplicación de IDD, la aplicación mostrará la ayuda en el mismo idioma.

Ayuda personalizada

En la ayuda personalizada se describen las entidades de negocio o las áreas de asunto que se han definido en la aplicación. El desarrollador de la aplicación de IDD crea la ayuda personalizada y la añade a la aplicación.

Guía del usuario de Data Director

La Guía del usuario describe las tareas que los usuarios profesionales pueden realizar en Data Director (IDD). Por ejemplo, en la guía se describe cómo se añaden o se fusionan las entidades de negocio.

De forma predeterminada, Data Director incluye la Guía de usuario como un archivo de ayuda en línea. El desarrollador de las aplicaciones IDD pueden reemplazar el archivo de ayuda enviado con un archivo de ayuda revisado. Podrá encontrar los archivos de ayuda revisados en Informatica Network.

Descargar un archivo de ayuda revisado de la Guía del usuario

Puede buscar y descargar los archivos de ayuda revisados de la Guía de ayuda en Informatica Network.

1. En un explorador, abra Informatica Network.
2. Busque "**Ayuda de la Guía del usuario de Informatica Data Director**".

   Si ve **Ayuda de la Guía del usuario de Informatica Data Director** en los resultados, habrá un archivo de ayuda revisado disponible para la versión especificada.
3. Seleccione el vínculo.
4. Anote el número de revisión. Puede usar este número para verificar que se muestra la ayuda correcta.
5. Descargue el archivo de ayuda.

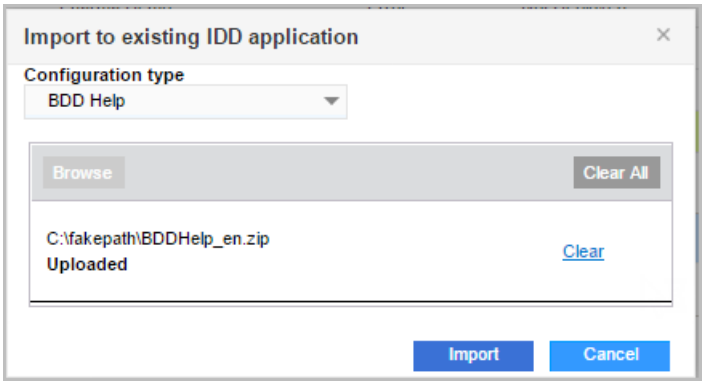
Importar un archivo de ayuda revisado de la Guía del usuario

Puede importar un archivo de ayuda revisado en las aplicaciones de IDD.

El formato del nombre del archivo de ayuda es `BDDHelp_xx.zip`, donde `xx` es un código de idioma ISO. Si ofrece soporte en varios idiomas, importe los archivos de ayuda traducidos en cada uno de los idiomas que incluya. La ayuda traducida se muestra cuando un usuario selecciona la configuración regional en la aplicación de IDD.

1. Inicie sesión en el administrador de configuración de IDD.
2. Seleccione una aplicación.
3. Haga clic en **Importar** > **Importar a la aplicación IDD existente**.
4. En el cuadro de diálogo **Importar a la aplicación IDD existente**, seleccione **Ayuda de BDD** de la lista **Tipo de configuración**.
5. Haga clic en **Examinar**.
6. En el cuadro de diálogo **Abrir**, seleccione el archivo de ayuda revisado y haga clic en **Abrir**.

   La siguiente imagen muestra que la versión en inglés del archivo de ayuda está lista para la importación:



7. Haga clic en **Importar**.

   El proceso de importación actualiza la aplicación con la ayuda de la Guía de usuario revisada.

Probar la ayuda revisada

Después de importar un archivo de ayuda revisado, abra la aplicación y verifique que la ayuda visualiza el número de revisión correcto.

1. Si la aplicación está abierta, ciérrela.
2. Inicie sesión en Informatica Data Director.
3. Si se le solicita, seleccione la aplicación que contiene la ayuda revisada.
4. En el menú **Ayuda**, haga clic en **Ayuda**.
5. Verifique que el Número de revisión en la parte inferior del tema Bienvenido coincida con el número asociado con el archivo de ayuda que ha descargado.

Ayuda personalizada

Puede crear ayuda personalizada que describa las entidades de negocio o las áreas de asunto que ha definido en la aplicación de IDD. Después de importar el archivo personalizado y de implementar la aplicación, un elemento de menú **Ayuda personalizada** aparece en el menú **Ayuda**.

Si ofrece soporte en varios idiomas, puede crear archivos de ayuda traducidos en cada uno de los idiomas que incluya. Cuando un usuario selecciona la configuración regional en la aplicación de IDD, se utiliza la ayuda traducida.

Crear un archivo de ayuda personalizado

Puede crear un archivo de ayuda personalizado para documentar sus aplicaciones de IDD. Si ofrece soporte en varios idiomas, también puede crear archivos de ayuda traducidos en cada uno de los idiomas que incluya.

1. Con una herramienta de creación de HTML, cree temas de ayuda personalizados y genere el proyecto de ayuda.
2. Cambie el nombre del archivo `index.htm` a `bdd_help_CSH.htm`.
3. Cree un directorio denominado `bdd_help`.
4. Copie los directorios y los archivos de ayuda generados en el directorio `bdd_help`.
5. Seleccione el directorio `bdd_help` y cree un archivo .zip que conserve la estructura de directorios.
6. Asigne al archivo .zip el nombre `CustomBDDHelp_xx.zip`, donde `xx` es un código de idioma ISO de dos caracteres.
7. Verifique que el tamaño del archivo `CustomBDDHelp_xx.zip` sea inferior a 20 MB.

Importar un archivo de ayuda personalizado

Puede importar un archivo de ayuda personalizado en las aplicaciones de IDD. Si ha traducido el archivo personalizado, importe también los archivos de ayuda traducidos.

1. Inicie sesión en el administrador de configuración de IDD.
2. Seleccione una aplicación.

3. Haga clic en **Editar**.
4. En el panel Editar aplicación, active la casilla de verificación **Ayuda personalizada** y, a continuación, haga clic en **Guardar**.

   En el archivo de configuración de la aplicación, la propiedad `help` se actualiza para establecer `customBddHelp` en `true`:

   ```
   <help bddHelp="true" customBddHelp="true"/>
   ```
5. En el árbol de navegación, haga clic en **Aplicaciones**.

   Aparece la lista de aplicaciones.
6. Seleccione la misma aplicación.
7. Haga clic en **Importar** > **Importar a la aplicación IDD existente**.
8. En el cuadro de diálogo **Importar a la aplicación IDD existente**, seleccione **Ayuda de BDD personalizada** de la lista **Tipo de configuración**.
9. Haga clic en **Examinar**.
10. En el cuadro de diálogo **Abrir**, desplácese hasta el archivo `CustomBDDHelp_xx.zip` y selecciónelo y, a continuación, haga clic en **Abrir**.
11. Haga clic en **Importar**.

    El proceso de importación actualiza la aplicación con el archivo de ayuda personalizado.
12. Haga clic en **Volver a implementar**.

CAPÍTULO 6

Propiedades globales de IDD

Este capítulo incluye los siguientes temas:

Referencia de propiedades globales de Informatica Data Director

La siguiente tabla muestra las propiedades globales que controlan el comportamiento en tiempo de ejecución de todas las aplicaciones de Informatica Data Director (IDD) en un único servidor del concentrador.

La tabla describe cada propiedad y su valor predeterminado. Estas propiedades se almacenan en la tabla CMX_SYSTEM.C_REPOS_DS_PREF_DETAIL. Si no se definen propiedades, se utilizarán los valores predeterminados especificados.

Importante: El servidor de aplicaciones debe reiniciarse para que se apliquen los cambios en las siguientes propiedades globales.

Propiedad	Valor predeterminado	Uso
allowDsEmptyChildren	false	Determina si los usuarios pueden ver registros secundarios cuando se configura un filtro de seguridad en una columna secundaria de segundo nivel, pero no hay registros secundarios de segundo nivel. Si es `true`, los usuarios pueden ver los registros secundarios cuando no hay registros secundarios de segundo nivel. Si es `false`, los usuarios no pueden ver los registros secundarios cuando no hay registros secundarios de segundo nivel.
asyncChildLoading	false	Carga los datos secundarios en la vista de datos, al abrir de forma explícita el registro secundario del objeto principal. Puede establecer el valor de propiedad en true para cargar los datos secundarios al abrir el registro en la vista de datos.
bulkexportloadsize	500	Tamaño máximo de la carga para cada subproceso cuando se exportan datos a un archivo de Microsoft Excel. El valor predeterminado es `500` registros. El máximo es `1000` registros. Si se establece en más de `1000`, se utiliza el tamaño de carga predeterminado.
CompositePagerTotalRecords	500	Número máximo de tareas de ActiveVOS que IDD clasifica al mismo tiempo sin tener en cuenta las mayúsculas y minúsculas. Si las tareas superan el valor establecido, IDD clasifica las tareas de ActiveVOS en función del tipo de base de datos. Si la base de datos es Microsoft SQL Server, la clasificación no tiene en cuenta las mayúsculas y minúsculas. Si la base de datos es Oracle o IBM Db2, la ordenación distingue entre mayúsculas y minúsculas.

Propiedad	Valor predeterminado	Uso
convert2DigitYearTo4Digit	false	Permite el ajuste de una entrada de año de dos dígitos a una entrada de año de cuatro dígitos. Establezca la propiedad en `true` para permitir el ajuste de las fechas que se introducen hasta 80 años antes y 20 años después de la fecha actual. Por ejemplo, si introduce la fecha `1/ene/30`, IDD interpreta la entrada como 1 de enero de 2030. Si introduce la fecha `1/ene/70`, IDD interpreta la entrada como 1 de enero de 1970.
credentialsAutofillDisabled	false	Por motivos de seguridad, si desea impedir que el navegador del usuario guarde las credenciales de inicio de sesión, como el nombre de usuario y la contraseña, puede establecer este valor en "true".
CSVColumnSeparator	Coma (,)	Determina el carácter que se utilizará como separador de columnas al exportar los datos a un archivo de valores separados por comas (CSV). También puede utilizar una ficha, un punto y coma y un espacio como delimitador.
deleteMovedRelInExplorerView	true	Determina si se elimina la relación anterior al crear una nueva relación en la vista de explorador del Administrador de jerarquías. Establezca la propiedad en false para finalizar la antigua relación.
enableCreateBEMenuGrouping	false	Especifica si se pueden definir grupos lógicos para la ventana **Nuevo**. Es obligatorio si tiene un gran número de áreas de asunto. Establezca la propiedad en `true` para definir grupos lógicos para ventana el **Nuevo**. Establezca la propiedad en `false` si no quiere definir grupos lógicos para la ventana **Nuevo**.
enableRememberCredentials	true	Cuando se establece en true, la casilla de verificación Recordar cuenta se muestra en la página de inicio de sesión. La sesión de los usuarios permanece abierta durante el periodo determinado por rememberCredentialsPeriod..

Propiedad	Valor predeterminado	Uso
enableSaveForPeriodDialogForHmRel	true	Habilita el cuadro de diálogo del período efectivo que aparece al actualizar un registro habilitado para el Administrador de jerarquías en IDD. Establezca la propiedad en `false` para deshabilitar el cuadro de diálogo del período efectivo.
enableTaskAttachments	false	Especifica si los usuarios pueden adjuntar archivos a tareas mediante las vistas heredadas con Data Director. Establezca la propiedad en `false` para deshabilitar los adjuntos y ocultar la sección **Archivos adjuntos** en el cuadro de diálogo **Detalles de tarea** y en el cuadro de diálogo **Crear tarea**. Establezca la propiedad en `true` para habilitar los datos adjuntos. **Importante:** Para ver el cambio en la aplicación IDD, use el Administrador de configuración de IDD para borrar la memoria caché de la aplicación IDD.
expandDropDownListShowFullValue	false	Permite expandir la lista desplegable en la ficha **Buscar** para ver los registros de búsqueda. Establezca la propiedad en `true` para permitir que la lista se ajuste y acomode el elemento de la lista más largo.
exportusingmultithread	false	Permite la creación de subprocesos para exportar datos a un archivo de Microsoft Excel. Establezca la propiedad en `true` para habilitar la creación de multiprocesos para exportar los datos.
handleUserExitBeforeShowingDialog	false	Determina si IDD llama a la salida de usuario SendForApprovalHandler. Se define en `true` para que IDD llame a la salida de usuario SendForApprovalHandler cuando el usuario haga clic en **Enviar para aprobar**. Se define en `false` para que IDD llame a la salida de usuario SendForApprovalHandler cuando el usuario haga clic en **Aceptar** en el cuadro de diálogo **Enviar para aprobar**.
HeaderBgColor	#000000	Especifica el código de color HTML del color de fondo del área de encabezado de IDD.

Propiedad	Valor predeterminado	Uso
hideSystemColumnsInResult	false	Especifica si se muestran columnas del sistema en los resultados de búsqueda de IDD. Establezca la propiedad en `true` para ocultar las columnas del sistema en los resultados de búsqueda de IDD. Cuando está como `true`, se puede personalizar la vista de tabla para seleccionar manualmente las columnas del sistema que se deben mostrar.
hmInactiveRelationshipsAvailable	false	Se establece en `true` para que el usuario pueda ver relaciones inactivas en el administrador de jerarquía.
IDD2COCSConverter.prefixCoNames	false	Cuando la configuración de Informatica Data Director se convierte a una configuración de entidad de negocio, determina si se utiliza un nombre de área de asunto con prefijo para el nombre de entidad de negocio. Establézcalo en `false` para utilizar el nombre de área de asunto como el nombre de la entidad de negocio. Establézcalo en `true` para utilizar el nombre de área de asunto con prefijo con el nombre de la aplicación de Informatica Data Director como el nombre de la entidad de negocio.
isEffectiveDateIncluded	false	Especifica si desea incluir el campo Fecha efectiva en las consultas de búsqueda en Informatica Data Director. Establezca su valor en `true` para mostrar la fecha actual en el campo Fecha efectiva. Establezca su valor en `false` para ocultar el campo Fecha efectiva.
isFillOnGap	false	Especifica si se debe habilitar la propiedad Rellenar intervalo para las operaciones de Informatica Data Director. Se establece en `true` para habilitar la propiedad Rellenar intervalo. Se establece en `false` para deshabilitar la propiedad Rellenar intervalo.

Propiedad	Valor predeterminado	Uso
lookupCacheUpdatePeriod	300000 (5 min)	El número de milisegundos durante los cuales pueden estar los datos de búsqueda en la memoria caché de IDD antes de que se vuelvan a cargar.
minModalWidth	1100	Determina el ancho mínimo en píxeles de la ventana **Buscar**.
maxCopiedChildrenNumber	10	Determina el número máximo de registros secundarios para cada tipo de elemento secundario que se copian cuando un usuario copia un área de asunto.
maxCopiedGrandChildrenNumber	10	Determina el número máximo de registros secundarios de segundo nivel para cada tipo de elemento secundario que se copian cuando un usuario copia un área de asunto.
maxImportThreads	5	Determina el número máximo de subprocesos que utilizar durante la importación de datos.
maxParallelPromoteThreads	1	Determina el número máximo de subprocesos que utilizar cuando aprueba una tarea. Cuando maxParallelPromoteThreads es mayor que 1 y promueve registros de varios objetos base, el proceso de promoción se ejecuta en paralelo. El valor máximo de maxParallelPromoteThreads es igual al número de núcleos de CPU del servidor.
maxParallelISavedQueriesThreads	true	Determina si las consultas se cargan a través de varios subprocesos. Las consultas de multiproceso se cargan más rápidamente. Se establece en `true` para habilitar el multiproceso. Se establece en `false` para deshabilitar el multiproceso.
maxParallelBvtThreads	1	Determina el número máximo de subprocesos que utilizar cuando IDD carga una tarea para visualizarla.
maxSearchResultsExportedRows	5000	Número máximo de filas de datos de resultados de búsqueda que se exportarán.

Propiedad	Valor predeterminado	Uso
maxXrefSearchReturnCount	100	Especifica el número máximo de registros de referencias cruzadas que una solicitud de búsqueda devuelve.
needLoadChildOnOpen	false	Establezca la propiedad en `true` para mostrar inicialmente solo los registros principales en la vista Coincidencias. Los registros secundarios se muestran cuando se expanden las fichas de los registros secundarios. Establezca la propiedad en `false` para mostrar inicialmente los registros principales y todos los registros secundarios en la vista Coincidencias.
openDashboardAfterTaskClose	false	Se establece en `true` para que Informatica Data Director abra el Espacio de trabajo Inicio después de completar cualquier tarea. Se establece en `false` para que Informatica Data Director abra la ficha anterior en la vista de datos después de completar cualquier tarea.
overrideTextAreaColumnOrder	true	De manera predeterminada, si configura una columna como un área de texto en un área de asunto, la columna de área de texto aparecerá siempre en la parte inferior del diseño independientemente del orden de las columnas. Establezca la propiedad en `true` para asegurarse de que las columnas de área de texto en un área de asunto aparecen en la parte inferior del diseño independientemente del orden de las columnas. Establezca la propiedad en `false` para asegurarse de que las columnas de área de texto aparecen en el orden especificado en un diseño.

Propiedad	Valor predeterminado	Uso
proactiveMatchResultSort	sortbyscorethenaction	Especifica el orden de clasificación en el que aparecen las posibles coincidencias. Establezca la propiedad en `sortbyscorethenaction` para ordenar por resultados de coincidencia y después por acción. Establezca la propiedad en `sortbyactionthenscore` para ordenar por acción, como abrir e importar, y después por resultados de coincidencia.
qrytaskidfromprocessidtotalretry	2	Número de intentos que IDD hace para volver a cargar una tarea de ActiveVOS. Establezca un valor de número entero más alto si utiliza una salida de usuario para controlar las tareas de ActiveVOS y las tareas que no aparecen correctamente en IDD.
qrytaskidfromprocessidwaitintrvlmillis	1000	Número de milisegundos que Informatica Data Director espera antes de intentar volver a cargar una tarea de ActiveVOS. Establezca un valor de número entero más bajo si utiliza una salida de usuario para controlar las tareas de ActiveVOS y las tareas que no aparecen correctamente en IDD.
rememberCredentialsPeriod	24 (horas)	Periodo de tiempo (en horas) que las credenciales de usuario se recuerdan si la casilla de verificación "Recordar cuenta" está seleccionada.
samCacheUpdatePeriod	600000 (10 min)	Determina cuánto tiempo (en milisegundos) pueden estar las funciones de SAM (recursos con asignaciones de privilegios) en la memoria caché de IDD antes de que se vuelvan a cargar.
serverPageSize	100	Afecta a la paginación de los resultados de búsqueda y los datos secundarios. IDD muestra al usuario una página de 10 registros. Sin embargo, el número de registros que obtiene de Informatica MDM Hub está determinado por esta propiedad. Con la configuración predeterminada, IDD no solicitará datos adicionales hasta que el usuario vaya a la página 11 de los datos.

Propiedad	Valor predeterminado	Uso
search_empty_date	false	Determina si el campo de fecha efectiva del cuadro de diálogo de búsqueda está vacío o contiene la fecha efectiva de la vista de datos al crear un registro secundario. Se establece en `true` para que el campo de fecha efectiva esté vacío. Se establece en `false` para que aparezca la fecha efectiva de la vista de datos en el campo de fecha efectiva.
searchForDuplicatesBeforeTaskDialog	false	Determina si el cuadro de diálogo **Duplicados potenciales** aparece antes o después de enviar una tarea para su aprobación. Se establece en `true` para que el cuadro de diálogo **Duplicados potenciales** aparezca antes que el cuadro de diálogo **Crear tarea**. Se establece en `false` para que el cuadro de diálogo **Duplicados potenciales** aparezca después de hacer clic en **Aceptar** en el cuadro de diálogo **Enviar para aprobar**.
shouldDisableSearchFieldIfDependentFieldAbsence	false	Habilita o deshabilita el campo de búsqueda dependiente en el formulario de búsqueda cuando el campo de búsqueda principal no está presente en el formulario de búsqueda o cuando el campo de búsqueda principal no tiene ningún valor. Se establece en `true` para habilitar el campo de búsqueda dependiente en el formulario de búsqueda. Se establece en `false` para deshabilitar el campo de búsqueda dependiente en el formulario de búsqueda.
showMatchedColumns	#DBF5EC	Especifica el código de color HTML del color que identifica las columnas coincidentes.
showShadowColumns	true	Especifica si se muestran las columnas de respaldo en la vista Referencias cruzadas. Se establece en `true` para mostrar las columnas de respaldo. Se establece en `false` para ocultar las columnas de respaldo.

Propiedad	Valor predeterminado	Uso
subjectAreaCopyDisabled	false	Determina si los usuarios pueden seleccionar Copiar desde el menú Acciones de un área de asunto para copiar un área de asunto. Se establece en `true` para deshabilitar la opción de copiar un área de asunto. Se establece en `false` para permitir la opción de copiar un área de asunto.
table_default_width_key	-1	Determina el porcentaje de ancho mínimo de las columnas de resultados de búsqueda.
tableMaxColumns	25	Determina la cantidad de columnas que se muestran en la vista de la tabla de registros secundarios y secundarios de segundo nivel. El valor predeterminado admite 20 columnas visibles y 5 columnas ocultas. Para garantizar que haya columnas visibles, especifique un número entero mayor de 5.
tabsExpandByDefault	n/d	Determina qué registros secundarios se expanden de manera predeterminada en la vista de datos. Para expandir registros secundarios de manera predeterminada en la vista de datos, especifique el nombre de cada área de asunto separados por comas. Para expandir la ficha **XREF** de manera predeterminada, especifique `xref`. Para expandir la ficha **Relaciones** de manera predeterminada, especifique `hm_relationship`. Por ejemplo, para expandir de manera predeterminada la ficha XREF, la ficha Dirección de envío y la ficha Organización, especifique `xref, ShipAddress, Organization`. Si no establece un valor para tabsExpandedByDefault, no se expandirá ningún registro secundario son ampliados de manera predeterminada en la vista de datos.
threadSchedulerIdleTime	5000 (segundos)	Determina el tiempo de inactividad máximo del programador de subprocesos.

Propiedad	Valor predeterminado	Uso
transactionTimeout	30 (segundos)	El número de segundos que tienen las transacciones para completar la ejecución antes de agotar el tiempo de espera.
updateExistingPeriodByDefault	false	Determina si la casilla de verificación Actualizar el periodo existente está habilitada de forma predeterminada. Establézcala en `true` para habilitarla de forma predeterminada. Establézcala en `false` para deshabilitarla de forma predeterminada.
writeBOM	false	Exporta los resultados de búsqueda de Informatica Data Director como archivo CSV con codificación UTF-8 con una marca de orden de bytes. Si la búsqueda contiene caracteres ASCII extendidos, defina writeBOM en `true` para ver datos válidos al abrir el archivo CSV.

TEMAS RELACIONADOS

- "Los metadatos de Informatica Data Director no se han actualizado" en la página 181

Actualizar las propiedades globales

Para actualizar las propiedades globales, puede ejecutar el siguiente script SQL en el esquema CMX_SYSTEM.

Cuando el siguiente script SQL se aplica a CMX_SYSTEM, inicializa las propiedades globales con sus valores predeterminados. Actualice el campo VALUE de este script para modificar estos valores.

```
insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.1', rowid_ds_pref, ' asyncChildLoading', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.2', rowid_ds_pref, 'bulkexportloadsize', '1000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.3', rowid_ds_pref, 'CompositePagerTotalRecords', '5000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
```

```
 'BDDGP.4', rowid_ds_pref, 'convert2DigitYearTo4Digit', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.5', rowid_ds_pref, 'credentialsAutofillDisabled', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.6', rowid_ds_pref, 'CSVColumnSeparator', ','
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, Create_Date, creator, Last_Update_Date, Updated_By,
ROWID_DS_PREF, NAME, VALUE)
select
 'PREF_DET_4', sysdate, 'CMX', sysdate, 'admin', rowid_ds_pref,
'enableCreateBeMenuGrouping', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.7', rowid_ds_pref, 'enableRememberCredentials', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'IDDATT.0', rowid_ds_pref, 'enableTaskAttachments', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';


insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.8', rowid_ds_pref, 'expandDropDownListShowFullValue', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.9', rowid_ds_pref, 'exportusingmultithread', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.10', rowid_ds_pref, 'handleUserExitBeforeShowingDialog', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.11', rowid_ds_pref, 'HeaderBgColor', '#000000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.12', rowid_ds_pref, 'hmInactiveRelationshipsAvailable', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.13', rowid_ds_pref, 'IDD2COCSConverter.prefixCoNames', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
```

```
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.14', rowid_ds_pref, 'lookupCacheUpdatePeriod', '300000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.15', rowid_ds_pref, 'maxCopiedChildrenNumber', '10'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.16', rowid_ds_pref, 'maxCopiedGrandChildrenNumber', '10'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.17', rowid_ds_pref, 'maxImportThreads', '5'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.18', rowid_ds_pref, 'maxParallelPromoteThreads', '1'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.19', rowid_ds_pref, 'maxParallelBvtThreads', '1'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.20', rowid_ds_pref, 'maxSearchResultsExportedRows', '5000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.21', rowid_ds_pref, 'maxXrefSearchReturnCount', '100'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.22', rowid_ds_pref, 'openDashboardAfterTaskClose', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.23', rowid_ds_pref, 'proactiveMatchResultSort', 'sortbyscorethenaction'
from C_REPOS_DS_PREF where name = '__SYSTEM_PREFERENCES_ROOT__';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.24', rowid_ds_pref, 'rememberCredentialsPeriod', '24'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.25', rowid_ds_pref, 'samCacheUpdatePeriod', '600000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
```

```
insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.26', rowid_ds_pref, 'search_empty_date', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.27', rowid_ds_pref, 'searchForDuplicatesBeforeTaskDialog', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.28', rowid_ds_pref, 'serverPageSize', '100'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.29', rowid_ds_pref, 'shouldDisableSearchFieldIfDependentFieldAbsence', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.30', rowid_ds_pref, 'showMatchedColumns', '#DBF58C'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.31', rowid_ds_pref, 'subjectAreaCopyDisabled', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.32', rowid_ds_pref, 'table_default_width_key', '20'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.33', rowid_ds_pref, 'threadSchedulerIdleTime', '5000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.34', rowid_ds_pref, 'transactionTimeout', 300
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.35', rowid_ds_pref, 'updateExistingPeriodByDefault', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.36', rowid_ds_pref, 'writeBOM', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.37', rowid_ds_pref, 'isFillOnGap', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
```

```
insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.38', rowid_ds_pref, 'maxXrefSearchReturnCount', '1000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.39', rowid_ds_pref, 'deleteMovedRelInExplorerView', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

commit;
/
```

APÉNDICE A

Requisitos de tamaño y plataforma

Este apéndice incluye los siguientes temas:

Tamaño del servidor de base de datos

Las implementaciones de IDD no afectan directamente al tamaño del servidor de base de datos.

Al definir la sección de API del modelo de tamaño, se deben tener en cuenta los requisitos de transacción de IDD.

Tamaño del servidor de aplicaciones

Una aplicación IDD se ejecuta en el servidor de aplicaciones y se ubica conjuntamente con el resto de componentes del servidor de Informatica MDM Hub.

Los servidores de aplicaciones deben tener un tamaño que permita un núcleo de CPU/1 GB de memoria para cada 10 sesiones de "usuarios intensivos" de IDD simultáneas. Para el objeto del modelo de tamaño, un usuario intensivo es un usuario de una aplicación IDD que produce un carga constante de 5 o 6 operaciones de IDD por minuto.

Tamaño de cliente y red

A continuación, se indican los requisitos de configuración mínimos y recomendados para equipos cliente que acceden a Informatica Data Director:

Nota: La resolución de pantalla configurada para Informatica Data Director es 1280 X 1024.

Parámetro	Valor
CPU	Mínimo: 1,6 GHz Recomendado: 2 GHz
Memoria	Mínimo: 1 GB Recomendado: 2GB
Ancho de banda de red efectivo al servidor de aplicaciones	Mínimo: 10 Mbps Recomendado: 100 Mbps

Para obtener más información sobre los requisitos y las plataformas compatibles con el producto, consulte la tabla de disponibilidad del producto en Informatica Network: https://network.informatica.com/community/informatica-network/product-availability-matrices

Requisitos de configuración del navegador

Debe habilitar el navegador en los equipos cliente para permitir cookies.

Desactive el bloqueador de elementos emergentes si ejecuta Informatica Data Director en Google Chrome.

APÉNDICE B

Componentes de aplicación

Referencia de componentes de aplicación

Una aplicación IDD se almacena en la base de datos del sistema (CMX_SYSTEM.C_REPOS_DS_CONFIG) como un archivo .zip que contiene archivos de componentes.

Este archivo .zip se puede exportar del Administrador de configuración de IDD o importar al Administrador de configuración de IDD.

Nombre de archivo	Uso
IDDConfig.xml	Archivo de configuración principal para la aplicación. Debe ajustarse al esquema XML `siperian-bdd-config-6.xsd`.
BDDBundle.properties BDDBundle_XX.properties	Paquetes de recursos con etiquetas para objetos definidos en la aplicación IDD (como áreas de asunto y objetos secundarios).
MetadataBundle.properties MetadataBundle_XX.properties	Paquetes de recursos con etiquetas para objetos definidos en el ORS (como objetos base, columnas, etc.).
ErrorCodeBundle.properties ErrorCodeBundle_XX.properties	Paquetes compuestos de recursos con el texto de los mensajes de error generados por una aplicación IDD.
MessageBundle.properties MessageBundle_XX.properties	Paquetes compuestos de recursos con el texto mostrado en la aplicación IDD.
BDDHelp.zip BDDHelp_XX.zip	Archivos de ayuda de IDD genérica. Ayuda que describe genéricamente las características de una aplicación IDD.
CustomBDDHelp.zip CustomBDDHelp_XX.zip	Archivos de ayuda de IDD personalizada. Ayuda que se ha desarrollado para que sea específica y exclusiva de una aplicación IDD determinada. Además de facilitar instrucciones de uso específicas de la implementación, este archivo de ayuda puede proporcionar todo tipo de información relevante, como los procedimientos y políticas de una organización.
logo.gif, logo.png, logo.jpg o logo.jpeg	Un sustituto del logotipo que la aplicación IDD muestra en la parte superior izquierda de la pantalla. El tamaño del logotipo de Informatica es de 147 píxeles de ancho por 31 píxeles de alto. Para obtener mejores resultados, el logotipo de reemplazo debería tener dimensiones similares.

APÉNDICE C

Configuración de seguridad de IDD

Referencia de configuración de seguridad de IDD

Las siguientes tablas muestran las opciones de configuración de seguridad de IDD. Los permisos en la Consola del concentrador se establecen mediante el administrador de acceso de seguridad.

Sugerencia: El administrador de acceso de seguridad incluye los siguientes grupos de recursos: ALL_GLOBAL_RESOURCES, ALL_XREF y ALL_XREF_HISTORY. Utilice estos grupos cuando desee asignar el mismo permiso a todos los recursos especificados. Por ejemplo, para establecer el permiso DELETE en todas las referencias cruzadas, puede activar la casilla de verificación DELETE en la fila ALL_XREF.

Tabla 1. General

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
Área de asunto nueva de barra de herramientas	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos lógicos uno a uno	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		S	S	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	S	-

Tabla 2. Vista Datos

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
Crear área de asunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos	S	-	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	lógicos uno a uno	-	S	-	-	-	-
Leer área de asunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos lógicos uno a uno	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-
Actualizar área de asunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos lógicos uno a uno	-	S	S	-	-	-
	BASE_OBJECT	NAME	-		-	S	S	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	S	-
Eliminar área de asunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal, la administración de estado está habilitada	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	-	-	S	-	-
Copiar área de asunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos lógicos uno a uno	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		S	S	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	S	-
Mostrar columnas del sistema del objeto base	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	El objeto base no es nuevo.	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-
Crear objeto secundario	BASE_OBJECT	NAME	-	Para elementos secundarios de uno a muchos, solo el objeto base; para elementos secundarios de muchos a muchos, se seleccionan el objeto base y su objeto base de relación.	S	S	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	S	-

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
Leer objeto secundario	BASE_OBJECT	NAME	-	-	-	S	-	-	-	-
Actualizar objeto secundario	BASE_OBJECT	NAME	-	Para elementos secundarios de uno a muchos, solo el objeto base; para elementos secundarios de muchos a muchos, se seleccionan el objeto base y su objeto base de relación.	-	-	S	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	S	-
Eliminar objeto secundario	BASE_OBJECT	NAME	-	Administración de estado habilitada. Para elementos secundarios de uno a muchos, solo el objeto base; para elementos secundarios de muchos a muchos, se seleccionan el objeto base y su objeto base de relación.	-	-	-	S	-	-

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
	BASE_OBJECT	NAME	XREF	Se deben seleccionar las referencias cruzadas para el objeto secundario.	-	-	-	S	-	-
	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Esta es la configuración obligatoria al utilizar la vista Entidad.	-	S	-	-	S	-

Tabla 3. CM

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
Ver referencia cruzada	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	El objeto base no es nuevo.	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-
	BASE_OBJECT	NAME	XREF	Objeto base principal y todos los objetos lógicos uno a uno. Para elementos secundarios de uno a muchos, solo el objeto base secundario. Para elementos secundarios de muchos a muchos, el objeto base secundario y el objeto base de relación.	-	S	-	-	-	-
Buscar duplicados	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-
Fusionar	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	S
	BASE_OBJECT	NAME	-		-	-	-	-	-	S
Anular fusión	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
	BASE_OBJECT	NAME	-		-	-	-	-	-	S
Ver datos sin formato	BASE_OBJECT	NAME	RAW	-	-	S	-	-	-	-

Tabla 4. Tareas

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
Enviar para aprobar (nuevo objeto principal)	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos lógicos uno a uno. La administración de estado está habilitada.	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		S	S	-	-	-	-
	BASE_OBJECT	NAME	-	Elementos secundarios de muchos a muchos. La administración de estado está habilitada.	S	S	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	Objeto principal y todos los objetos lógicos uno a uno	-	-	-	-	S	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Valor predeterminado para aprobación	S	-	-	-	-	-
Enviar para aprobar (objeto principal existente)	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos lógicos uno a uno. La administración de estado está habilitada.	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	S	-	-	-

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
	BASE_OBJECT	NAME	-	Elementos secundarios de muchos a muchos. La administración de estado está habilitada.	-	S	S	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	Objeto principal y todos los objetos lógicos uno a uno	-	-	-	-	S	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Valor predeterminado para aprobación	S	-	-	-	-	-
Tarea de envío para aprobación	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Los botones Enviar para aprobar y Editar están habilitados para un nuevo registro creado. El botón Guardar está deshabilitado.	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		S	S	S	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ ReviewNoApprove		S	-	-	-	-	-
Abrir tarea desde el Espacio de trabajo Inicio	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA		-	-	-	-	S	-
Crear tarea	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los objetos lógicos uno a uno. La administración de estado está habilitada.	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-
	BASE_OBJECT	NAME	-	Elementos secundarios de muchos a muchos. La administración de estado está habilitada.	-	-	-	-	-	-

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	Objeto principal y todos los objetos lógicos uno a uno	-	-	-	-	S	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Cualquier tipo de tarea de creación	S	-	-	-	-	-
Ver detalles de tarea	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	-	-	-	-	-	S	-
Tarea de fusión	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Merge		S	-	-	-	-	-
Tarea de anular fusión	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Unmerge		S	-	-	-	-	-
Cola para la fusión	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	El botón Cola para la fusión está habilitado.	-	S	S	-	-	S
	BASE_OBJECT	NAME	-		-	S	-	-	-	S
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Merge		-	-	-	-	S	-
Ejecutar acción de tarea	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA		-	-	-	-	S	-

Tabla 5. Vista del historial

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
Ver el historial de área de asunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	El objeto base principal persiste. El historial está habilitado para el objeto base principal.	-	S	-	-	-	-
Vista Historial del	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objeto base principal y todos los	-	S	-	-	-	-

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
objeto principal	BASE_OBJECT	NAME	HISTORY	objetos lógicos uno a uno.	-	S	-	-	-	-
	BASE_OBJECT	NAME	-	El historial debe estar habilitado para el objeto base.	-	S	-	-	-	-
Vista Historial del objeto base secundario	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Para elementos secundarios de muchos a muchos, se tienen en cuenta los privilegios de relación.	-	S	-	-	-	-
	BASE_OBJECT	NAME	HISTORY		-	S	-	-	-	-
	BASE_OBJECT	NAME	-	El historial debe estar habilitado para el objeto base.	-	S	-	-	-	-
Ver historial de referencias cruzadas del objeto base	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	El historial debe estar habilitado para el objeto base.	-	S	-	-	-	-
	BASE_OBJECT	NAME	XREF_HISTORY		-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-
Ver historial de fusión del objeto base	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	S	-	-	-	-
	BASE_OBJECT	NAME	-		-	S	-	-	-	-

Tabla 6. Gráficos

Caso de uso	Grupo de recursos	Nombre	Nombre secundario	Requisitos especiales/ comentarios	C	R	U	D	E	M
Ver gráfico	CUSTOM_RESOURCE	BDD_NAME	CHART/View	-	-	S	-	-	-	-

APÉNDICE D

Seguridad de datos

Este apéndice incluye los siguientes temas:

Resumen de seguridad de datos

La seguridad de datos es la protección de los datos frente al acceso, la modificación, la corrupción, la destrucción, la duplicación o la divulgación accidentales o no autorizados durante operaciones como la entrada, el procesamiento, el almacenamiento, la transmisión y la salida, así como el control adecuado de ese acceso a los datos.

La seguridad de datos de IDD garantiza que los usuarios puedan acceder a los datos en función de los siguientes criterios:

- Función de usuario
- Configuración de seguridad de datos
- Datos almacenados en el concentrador

Seguridad de datos mediante filtros

La seguridad de datos en Informatica Data Director se configura mediante el cuadro de diálogo **Área de asunto** de Informatica Data Director Configuration Manager. Puede definir filtros en la columna de área de asunto para limitar y proteger los datos de área de asunto a los que pueden acceder usuarios individuales. Se pueden definir filtros en la columna del objeto principal, en la columna secundaria y en la columna secundaria de segundo nivel. Puede configurar todos los filtros que desee para un área de asunto y para una columna de grupo de área de asunto.

La seguridad de datos de Informatica Data Director admite los siguientes tipos de valores para los filtros de seguridad en el tipo de columna de tabla de la base de datos:

- Cadena
- Entero
- Flotante

Nota: Los filtros de seguridad de datos de Informatica Data Director no admiten el valor de la columna de tabla de tipo Fecha.

Tenga en cuenta las siguientes reglas y directrices cuando trabaje con filtros:

- Cada filtro de seguridad se define en columnas del área de asunto y tiene un valor de filtro que se aplica a una lista de funciones.
- Los filtros de seguridad se basan en valores exactos, en lugar de en intervalos o comparaciones comodín.
- Se deben definir filtros en las columnas de coincidencia para aplicar filtros de seguridad de forma uniforme en las búsquedas básica, ampliada y avanzada.
- Los filtros pueden combinarse. Un usuario con varias funciones puede tener aplicadas combinaciones de filtros. Como resultado, un usuario tendrá acceso a todos los datos disponibles en cada función asignada gracias a la unión de las asignaciones de filtro.
- Es posible combinar filtros en distintas columnas para crear seguridad de datos multidimensional.
- Varios filtros en una única columna para una sola función. Un usuario tiene acceso a una unión de todos los datos que cumplen cada filtro.
- Filtros en varias columnas para una sola función. Un usuario tiene acceso a la intersección de todos los datos que cumplen cada filtro.
- En entornos de IBM Db2, los filtros de las columnas con un tipo de datos de valor flotante no filtran los valores situados fuera de la escala de la columna. Por ejemplo, si la escala de la columna es 1 y establece el filtro para 1,2, también se podrá acceder a los valores situados fuera de la escala de la columna, como 1,21.

Para obtener más información, consulte la ayuda en línea del *Administrador de configuración*.

Parámetros de seguridad de datos

Para restringir los datos a los que pueden acceder los usuarios que pertenecen a una determinada función, puede configurar los parámetros de seguridad de datos del archivo `BDDConfig.xml`.

Puede configurar los siguientes parámetros de seguridad de datos:

securityFilter

Especifica la columna en la que Informatica Data Director (IDD) basa el filtrado. El atributo "columnUid" especifica el ID de columna o la ruta de coincidencia.

securityValue

Especifica el valor que debe tener la columna securityFilter para permitir que el usuario vea los datos de un registro.

securityRole

Especifica la función a la que se aplica el filtro de seguridad. El atributo "roleID" especifica el ID de función de la función cuyo acceso está restringido por el filtro de seguridad de datos.

Ejemplo de configuración de objeto principal para la seguridad de datos

Debe configurar la seguridad en el archivo `BDDConfig.xml` para que los gestores de datos puedan ver el contenido que se aplica a sus países. Los gestores de datos de Francia ven los registros principales con un valor de país de "FR" y los gestores de datos de Japón ven los registros principales con un valor de país de "JA".

Para filtrar según la ubicación de un gestor de datos, cree una función en MDM Hub para cada región. En este ejemplo, asigna a los gestores de datos de Francia la función "DSFrance" y asigna al gestor de datos de Japón la función "DSJapan".

El siguiente fragmento del archivo `BDDConfig.xml` muestra cómo configurar la seguridad de los datos para este ejemplo:

```
<dataSecurity>
  <securityFilter columnUid="COUNTRY">
    <securityValue value="FR">
      <securityRole roleUid="DSFrance"/>
    </securityValue>
    <securityValue value="JA">
      <securityRole roleUid="DSJapan"/>
    </securityValue>
  </securityFilter>
</dataSecurity>
```

Ejemplo de configuración de objeto secundario de segundo nivel para la seguridad de datos

Quiere que los gestores de datos de Francia vean registros secundarios y registros secundarios de segundo nivel cuando la columna "País" del registro secundario de segundo nivel C_MT_ADDRESS tenga el valor "FR".

Para filtrar según la ubicación de un gestor de datos, cree una función en MDM Hub para los gestores de datos de Francia. En este ejemplo, asigne a los gestores de datos de Francia la función "DSFrance". Utilice el componente de ruta de coincidencia para el objeto secundario de segundo nivel cuando especifique el valor "columnUid".

El siguiente fragmento del archivo `BDDConfig.xml` muestra cómo configurar la seguridad de los datos para este ejemplo:

```
<subjectArea name=”Organization”>
  <one2ManyChild name="Employee">
    <dataSecurity>
      <securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|COUNTRY">
        <securityValue value="RUS">
          <securityRole roleUid="DSFrance"/>
        </securityValue>
      </securityFilter>
    </dataSecurity>
    <one2ManyChild name="Address" mpcUid="C_MT_ADDRESS">
    </one2ManyChild>
  </one2ManyChild>
</subjectArea>
```

De manera predeterminada, los usuarios no pueden ver el registro secundario si configura un filtro para una columna secundaria de segundo nivel, pero el registro secundario no tiene registros secundarios de segundo nivel. Para permitir a los usuarios ver registros secundarios sin registros secundarios de segundo nivel, establezca la propiedad global 'allowDsEmptyChildren' en `true`.

Aplicar seguridad de datos

La seguridad de datos proporciona una solución para proteger los datos organizativos (como datos estáticos, jerárquicos, dinámicos, históricos y transaccionales) que las organizaciones obtienen, almacenan, crean, eliminan y actualizan para llevar a cabo sus procesos empresariales.

En una aplicación IDD, la seguridad de datos definida en un área de asunto se aplica a los siguientes tipos de contenido:

- Datos de búsqueda
- Datos de entidad

- Datos jerárquicos
- Datos históricos
- Datos de tareas

Seguridad de datos en datos de búsqueda

La búsqueda de IDD permite a un usuario buscar registros por área de asunto y por grupo de área de asunto. Si un área de asunto tiene filtros de seguridad de datos del usuario, los resultados de la búsqueda solo deberán contener los registros conformes con la seguridad de datos. La seguridad de datos se aplica tanto a búsquedas básicas como a búsquedas parciales. Por ejemplo, cuando un usuario realiza una búsqueda y tiene acceso solo a personas residentes en California, el resultado de la búsqueda solamente muestra los registros de personas de California.

Nota:

- Si un usuario con seguridad de datos realiza una búsqueda mediante un término de búsqueda, el resultado de la búsqueda es una intersección de los registros que cumplen la seguridad de datos y lo que devuelve la búsqueda.
- Si la eliminación de duplicados de búsqueda de un registro secundario no está habilitada y el usuario con seguridad de datos en los objetos primarios tiene más de un registro secundario, los resultados de búsqueda mostrarán todos los registros relacionados con el objeto principal.
- Cuando se realiza la búsqueda en un grupo de área de asunto, se utilizan distintos filtros de seguridad de datos.
- IDD contrae todos los duplicados en caso de que la cantidad de registros encontrados sea inferior al tamaño de la página del servidor configurada; por ejemplo, cuando se obtienen todos los resultados después de la primera solicitud.

Seguridad de datos en datos de entidad

IDD permite a un usuario acceder al registro del objeto principal (PO), al registro secundario, al registro secundario de segundo nivel y a los vínculos de área de asunto por área de asunto y grupo de área de asunto. Si un área de asunto tiene filtros de seguridad de datos para un usuario, el usuario solo podrá acceder a los registros conformes con la seguridad de datos. Las siguientes secciones describen cómo se aplica la seguridad de datos para distintas operaciones en la vista de datos.

Abrir un registro

Los filtros de seguridad de datos garantizan que solo los usuarios autorizados puedan abrir registros en la vista de datos.

Abrir un registro con una función única

Los usuarios con una sola función pueden abrir registros del objeto principal si se cumplen las siguientes condiciones:

- El objeto principal debe cumplir todos los filtros de seguridad de datos aplicados en la columna del objeto principal.
- El objeto principal debe tener al menos un registro que supere las restricciones de seguridad habilitadas en cada ficha secundaria con seguridad de datos.

Por ejemplo, piense en un modelo de seguridad de datos en el que un usuario tenga la función SalesManager-NY y tenga configurados los siguientes filtros de seguridad:

- Filtro 1: El código de estado es NY.
- Filtro 2: El tipo de teléfono es Trabajo y Casa.
- Filtro 3: El código de tratamiento personal es Sr.

Con este modelo de seguridad de datos, imagine una situación en la que la base de datos tenga un registro del objeto principal para el Sr. Steve Nash, con la dirección de facturación en el estado de Nueva York (NY) y el tipo de teléfono definido en Trabajo. El usuario con la función SalesManager-NY puede abrir el registro del Sr. Steve Nash en la lista de datos, puesto que el objeto principal cumple el filtro 3 y sus objetos secundarios cumplen los filtros 1 y 2.

Con el mismo modelo de seguridad de datos, imagino otra situación en la que la base de datos tenga un registro del objeto principal para el Sr. Carlos Booser, con la dirección de facturación en el Estado de Nueva York (NY) y el tipo de teléfono definido en Móvil. El usuario con la función SalesManager-NY no podrá abrir el registro del Sr. Carlos Booser en la vista de datos, ya que no supera la restricción habilitada en la ficha secundaria de tipo de teléfono.

Filtrar un registro con una función única

Los usuarios con una sola función únicamente pueden acceder a los detalles de un objeto secundario o secundario de segundo nivel si satisface todos los filtros de seguridad de datos que se aplican en la columna secundaria o secundaria de segundo nivel del objeto principal.

Por ejemplo, piense en un modelo de seguridad de datos en el que el usuario tenga la función SalesManager-NY y tenga configurados los siguientes filtros de seguridad:

- Filtro 1: El código de estado es NY.
- Filtro 2: El tipo de teléfono es Trabajo y Casa.
- Filtro 3: El código de tratamiento personal es Sr.

Con el modelo de seguridad de datos indicado anteriormente, imagine una situación en la que la base de datos tenga un registro del objeto principal: Sr. Robin Cameron, con dirección de facturación en el estado de California (CA), Texas (TX) y Nueva York (NY), y el tipo de teléfono definido en Trabajo y Fax. El usuario con la función SalesManager- NY solo puede ver la dirección en el estado de Nueva York (NY) y el teléfono del trabajo en la ficha de teléfonos. El filtro no mostrará el resto de registros de ambas fichas.

Filtrar registros con varias funciones

De manera predeterminada, un usuario que pertenece a varias funciones puede acceder a los registros secundarios o a registros secundarios de segundo nivel según los filtros de seguridad de datos combinados.

Por ejemplo, considere un modelo de seguridad de datos en el que el usuario pertenece a la función "Sales Manager NY" y a la función "Car Sales Manager NJ".

La función "Sales Manager NY" tiene los siguientes filtros de seguridad de datos:

- Filtro 1: El código de estado es "NY".
- Filtro 2: El tipo de teléfono es "Business" o "Home".

La función "Car Sales Manager NJ" tiene los siguientes filtros de seguridad de datos:

- Filtro 1: El código de estado es "NJ".
- Filtro 2: El año del vehículo es "2009".

Tenga en cuenta un escenario en el que la base de datos tiene un registro de objeto principal para John Smith. John tiene direcciones de facturación con valores de código de estado de "NY", "NJ" y "TX". John tiene

números de teléfono con valores de tipo de teléfono de "Business" y "Facsimile". John tiene un coche producido en el año 2009 y un coche producido en el año 2001. El usuario con la función "Sales Manager NY" y la función "Car Sales Manager NJ" ve la siguiente información:

- El usuario ve las direcciones de facturación NY y NJ porque el filtro de código de estado está configurado para ambas funciones.
- Si el atributo "affectFilter" de "securityValue" es `false`, el usuario verá números de teléfono para todos los tipos de teléfono y registros de coches de todos los años. Informatica Data Director (IDD) no aplica los filtros de seguridad de datos al tipo de teléfono o al año del coche porque los filtros no se han configurado para las dos funciones.
- Si el atributo "affectFilter" de "securityValue" es `true`, el usuario verá los números de teléfono del tipo de teléfono "Business" y los datos de coches del año 2009. IDD aplica todos los filtros de seguridad de datos que están configurados para cada función. El valor predeterminado del atributo "affectFilter" es `true`.

Filtros de seguridad de datos de las funciones heredadas

Puede configurar los filtros de seguridad de datos de las funciones heredadas que descienden de una función de elemento primario. Para configurar los filtros de seguridad de datos de las funciones heredadas, establezca el atributo affectFilter del parámetro securityFilter en el archivo `BDDConfig.xml`.

Por ejemplo, considere una jerarquía de funciones con una función DataSteward_NY que es descendiente de una función DataSteward. Un usuario que pertenece a la función DataSteward_NY también pertenece a la función DataSteward.

Quiere configurar un filtro de seguridad que solamente afecte a los usuarios que pertenecen a la función DataSteward_NY. Desea que los usuarios que pertenecen a la función DataSteward_NY puedan ver los registros que tienen un valor STATE_CD de `NY`. Deberá establecer el atributo affectFilter en `false` para filtrar los datos de la función DataSteward_NY. Cuando el atributo affectFilter es `false`, Informatica Data Director filtra los datos de la función DataSteward_NY independientemente de la filtros de seguridad de datos de la función DataSteward.

El siguiente fragmento del archivo `BDDConfig.xml` muestra cómo configurar los filtros de seguridad de los datos para este ejemplo:

```
<securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|STATE_CD">
  <securityValue value="NY">
    <securityRole roleUid="DataSteward_NY"/>
  </securityValue>
  <securityValue affectFilter="false">
    <securityRole roleUid="DataSteward"/>
  </securityValue>
</securityFilter>
```

Ver relaciones

En IDD, una relación describe la afiliación entre dos entidades específicas. Por ejemplo, una entidad de cliente puede estar vinculada lógicamente a una entidad de dirección.

La ficha **Relación** de la vista de datos contiene información sobre las relaciones del Administrador de jerarquía del objeto principal con otras entidades del Administrador de jerarquía. Es posible transformar algunas de las entidades del Administrador de jerarquía en objetos principales que pueden estar afectados por la seguridad de datos.

La ficha **Relación** sólo debe contener esas relaciones que conectan entidades del Administrador de jerarquía asociadas con los objetos principales conformes con los ajustes de seguridad de datos.

Fusionar datos

La fusión es el proceso de combinar dos o más registros porque son idénticos o lo suficientemente similares para considerarse duplicados. Los registros se funcionan para consolidar datos duplicados en una sola entidad (entidad principal) que representa la mejor versión de confianza (BVT). Si los valores de atributo difieren, es posible determinar qué valores se conservarán en función de diferentes factores. Por ejemplo, los valores que se conservan se pueden determinar en función de la configuración de confianza de esos registros, o bien, en función de los valores proporcionados por un usuario que ha decidido editar el valor de anulación en su lugar.

En la aplicación IDD, el cuadro de diálogo **Buscar candidatos de fusión** solo debe mostrar aquellos registros que son válidos para la seguridad de datos del área de asunto del objeto principal.

Exportar datos y perfiles

Todos los filtros de seguridad de datos y el enmascaramiento de datos se pueden aplicar para datos exportados, así como para los datos que se muestran al usuario.

Guardar un registro

Un usuario solo podrá guardar un registro después de que se complete la validación y de que se apliquen todos los filtros de seguridad de datos del área de asunto. Si un registro no cumple los requisitos de los filtros de seguridad de datos, el usuario verá un mensaje de advertencia.

Si selecciona **Sí** en el cuadro de diálogo del mensaje de advertencia, se guardará el objeto principal y la ficha se cerrará. Si selecciona **No**, no se guardará el objeto principal, pero el usuario podrá seguir rellenando los detalles del objeto principal.

Buscar duplicados (coincidencias potenciales)

Los duplicados son entidades en las que los datos de determinadas columnas (como el nombre, la dirección o los datos de organización) son idénticos o suficientemente parecidos para considerarse prácticamente idénticos. IDD utiliza una lógica de coincidencia especial y atributos que aceptan coincidencias para determinar si dos entidades son lo suficientemente similares para considerarlas coincidencias. Los duplicados son entidades que se plantea fusionar.

Para buscar posibles coincidencias, haga clic en **Más acciones** y seleccione **Buscar duplicados**. Si un área de asunto tiene filtros de seguridad de datos para el usuario, los resultados de la búsqueda de duplicados solo deberán contener los registros del objeto principal conformes con la seguridad de datos.

Por ejemplo, imagine un modelo de seguridad de datos en el que el usuario tenga una sola función, SalesManager-CA, y ejecute una búsqueda de duplicados para una persona. Los resultados de la búsqueda mostrarán a individuos que tengan al menos una dirección de facturación en el estado de California (CA), mientras que el resto de duplicados se filtrarán.

Nota: Si un usuario tiene más de una función y ejecuta una búsqueda de duplicados, el usuario podrá ver una unión de los resultados que cada función puede ver.

Seguridad de datos en datos jerárquicos

En IDD, una jerarquía es un conjunto de tipos de relación. Simplemente son tipos de relación que se agrupan para facilitar la clasificación y la identificación. Cuando está abierta a la vista del Administrador de jerarquía, primero comprueba si se puede transformar la entidad de anclaje del Administrador de jerarquía en un objeto principal y, en tal caso, si es visible para la seguridad de datos.

Añadir entidades del Administrador de jerarquía

La entidad del Administrador de jerarquía se puede añadir al lienzo mediante las operaciones Buscar y Crear.

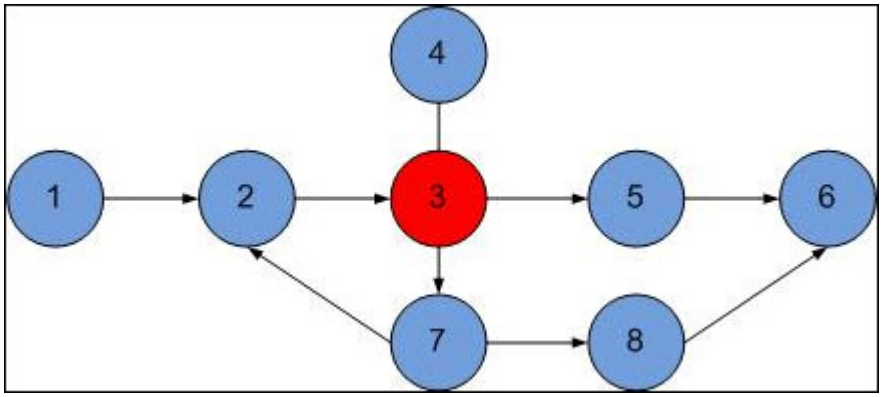
En los resultados de la búsqueda de datos, solo se muestran los registros permitidos por el objeto principal de la seguridad de datos del área de asunto. Por lo tanto, solo se pueden añadir objetos válidos al usar la opción de búsqueda.

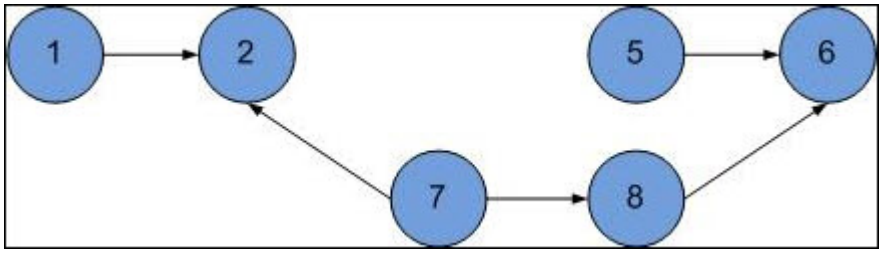
Cuando un usuario crea una entidad de HM, puede guardar el objeto principal en la vista de datos que la seguridad de datos no valida. Si el usuario confirma que se guarde el objeto principal que no es visible para la seguridad de datos, esta entidad de HM no se añade al lienzo.

Representar gráficos del Administrador de jerarquía

Las entidades del Administrador de jerarquía se pueden transformar en objetos principales. Los objetos principales que no se pueden ver como consecuencia de la seguridad de datos no se representan en el gráfico del Administrador de jerarquía como entidades del Administrador de jerarquía. Si un usuario no puede ver una entidad del Administrador de jerarquía, el gráfico del Administrador de jerarquía no debe mostrar esta entidad ni su subárbol

Por ejemplo, imagine el siguiente gráfico del Administrador de jerarquía, en el que un usuario no puede ver la entidad 3 debido a la seguridad de datos. En este caso, el gráfico debe ser visible para el usuario sin la entidad 3 ni su componente de subárbol, la entidad 4.





Nota: Los usuarios con varias funciones pueden acceder a la unión de todos los objetos a los que pueden acceder las diversas funciones.

Seguridad de datos en datos históricos

IDD le permite ver el historial de datos que procesan eventos como actualizaciones, eliminaciones y funciones que se producen en la entidad seleccionada. Si un objeto base cumple los requisitos de seguridad

de datos, se mostrará el historial de este objeto base incluso si estaba oculto anteriormente por seguridad de datos.

La seguridad de datos en el historial afecta las siguientes áreas:

- Historial para objetos principales
- Eventos de historial
- Historial compuesto de objetos principales.

Abrir detalles del historial

Un usuario puede abrir el historial de datos mediante un vínculo profundo o como un componente de historial en IDC. En este caso, IDD aplica la seguridad de datos para garantizar que los usuarios autorizados puedan ver el objeto principal para el que se ha creado el historial.

Ver eventos del historial

Los eventos de la vista de historial hacen referencia a objetos de área de asunto, objetos principales o elementos secundarios de objetos principales. Si el objeto principal no se ve debido a la seguridad de datos, la vista de historial no se muestra. Si un registro secundario no se ve debido a la seguridad de datos, se muestra la vista de historial para el objeto principal pero los eventos del historial del registro secundario no se agregan a la línea temporal.

Seguridad de datos en vínculos profundos

La característica de vinculación profunda de la aplicación IDD le permite administrar el estado de la aplicación con parámetros URL. Permite definir parte de la ruta de navegación interna en URL, que puede abrirse en la aplicación IDD.

Esta característica también se utiliza para:

- Facilitar la navegación entre el componente de IDC y la aplicación IDD.
- Proporcionar marcadores de partes específicas de la aplicación.

La seguridad de datos de IDD afecta a las siguientes áreas de vínculos profundos:

- **Abrir un registro**: Antes de que una nueva ficha muestre los datos del registro en la vista de datos, se comprueba que el objeto principal y sus datos secundarios se ajustan a los valores de seguridad de datos.
- **Abrir una tarea**: Todos los valores de seguridad de datos mencionados en la sección “Seguridad de datos en datos de tarea” en la página 162 son aplicables. Estos valores de seguridad de datos determinan si un usuario puede abrir una tarea.

APÉNDICE E

Ejemplo de configuración de seguridad basada en funciones

Este apéndice incluye los siguientes temas:

Resumen del ejemplo de configuración de seguridad basada en funciones

Este apéndice describe un escenario sencillo para configurar el acceso basado en funciones a recursos seguros de Informatica Data Director (IDD).

Introduce conceptos clave y repasa las tareas de configuración de seguridad necesarias para implementar un escenario de muestra. El objetivo de este apéndice es proporcionar a los implementadores de IDD conocimientos básicos sobre lo que pueden necesitar para configurar la seguridad en sus proyectos de implementación de IDD.

Nota: No se trata de un tutorial práctico para crear una aplicación de muestra operativa. Simplemente es un tutorial narrativo de las herramientas y tareas necesarias en un escenario determinado.

Conceptos clave

Esta sección describe los conceptos clave que necesita conocer antes de implementar la seguridad para IDD.

IDD, Administrador de acceso de seguridad (SAM) y Marco de servicios de integración (SIF)

La mayoría de las funciones de IDD se implementan mediante llamadas de SIF.

SIF requiere la configuración de SAM, de alta granularidad, para proporcionar los derechos y privilegios necesarios para ejecutar las llamadas de SIF. La configuración de SAM conlleva la definición de los usuarios,

las funciones, los recursos seguros y los privilegios necesarios para admitir el acceso basado en funciones a datos y operaciones.

Herramientas para configurar la seguridad de IDD

Utilice las siguientes herramientas en la Consola de Informatica MDM Hub para configurar SAM: Usuarios, Grupos y usuarios, Funciones y Recursos seguros/Grupos de recursos (incluidos los paquetes y las funciones de limpieza).

Utilice también el Administrador de configuración de IDD para vincular su configuración de SAM con objetos de IDD.

Lectura relacionada

La siguiente documentación de Informatica proporciona una importante información de referencia sobre el Administrador de acceso de seguridad, el Marco de servicios de integración y la seguridad de Data Director:

- *Guía de seguridad de Multidomain MDM*
- *Guía del marco de servicios de integración de Multidomain MDM*, "Uso del Administrador de acceso de seguridad con la API de SIF"

Temas relacionados

- "Referencia de configuración de seguridad de IDD" en la página 117

Seguridad de objetos y tareas

Es útil estructurar la seguridad de IDD en dos amplias categorías:

- Seguridad de objetos: acceso a datos de área de asunto y capacidad de realizar operaciones en esos datos (como ver, crear, actualizar y fusionar) en IDD.
- Seguridad de tareas (flujo de trabajo): acceso a las tareas y acciones basadas en funciones definidas en el flujo de trabajo.

Nota: Aunque este escenario de ejemplo se centra únicamente en la seguridad de objetos, muchos de los conceptos también se pueden aplicar a la seguridad de tareas en IDD, ya que la seguridad de tareas también depende de SAM.

Temas relacionados

- "Flujos de trabajo y tareas" en la página 22

Consejos para diseñar la seguridad para el uso de IDD

La implementación de la seguridad de IDD es un proceso iterativo y continuo.

Para empezar, debe conocer los diversos tipos de acceso a los recursos (objetos y operaciones) que los usuarios de IDD necesitarán en su aplicación de IDD.

En SAM, la *función* es el mecanismo principal que determina el nivel de acceso que tiene un usuario a los recursos de IDD. SAM tiene muchas opciones que se pueden configurar y proporciona un control granular sobre los recursos. Considere la posibilidad de crear una función independiente para el acceso a cada combinación única de objetos y operaciones, y asigne privilegios a esa función. Las funciones se pueden basar en otras funciones para crear capas de privilegios en expansión. Tras realizar la configuración, asignará los usuarios a la función que mejor se ajuste a sus responsabilidades.

Este escenario de ejemplo sigue el principio de *menos privilegios*; el acceso a los recursos se concede según se necesite. De forma predeterminada, los usuarios no tienen permisos. A continuación, concede a los usuarios que desea únicamente los permisos necesarios para completar las operaciones de las que son responsables.

Importante: La configuración de SAM debe coincidir con la configuración de IDD. Para cualquier opción que configure en la aplicación IDD, necesitará configurar SAM para proporcionar suficientes privilegios para admitir las funciones de IDD configuradas.

Otras consideraciones

Al planificar la seguridad para su aplicación IDD, tenga en cuenta las siguientes consideraciones:

- Para que IDD acceda a los recursos de Informatica MDM Hub, los recursos deben configurarse como SECURE (seguros, no privados) en la herramienta Recursos seguros de la Consola del concentrador.
- SAM se configura por ORS. Al añadir usuarios de IDD, debe establecer el esquema de IDD como base de datos predeterminada para estos usuarios.
- En el espacio de trabajo Datos, los usuarios de IDD por lo general no verán mensajes de error explícitos de privilegios insuficientes. Por ejemplo, un recurso determinado podría simplemente ocultarse al usuario porque no se haya configurado el acceso del usuario a ese recurso. Al probar su configuración de seguridad, consulte el registro del servidor para obtener información sobre depuración.
- En un espacio de trabajo de entidad, IDD visualiza todos los recursos independientemente de la función de usuario. Cuando los usuarios realizan acciones para las que no tienen los permisos de seguridad necesarios, IDD visualiza mensajes de error.
- La configuración de seguridad se almacena en dos lugares: en la memoria caché del servidor del concentrador y en la memoria caché de IDD. Se produce un leve retraso (1 minuto) para sincronizar los cambios. En un entorno de desarrollo, puede reiniciar el servidor para actualizar la memoria caché.

Tareas de configuración de seguridad de IDD

Esta sección recorre la serie de tareas para implementar un escenario de muestra basado en funciones: proporcione a los usuarios de IDD cuatro niveles de privilegios distintos (sin permisos, solo lectura, creación y actualización) para acceder a un objeto base de Grupo y a los recursos asociados.

Por ejemplo, imagine un escenario con dos áreas de asunto, como Grupo y Organización, en la que el área de asunto Grupo tenga una relación de uno a uno lógica con el área de asunto Organización. En la vista de datos, para editar los atributos del registro, debe tener el privilegio de creación (CREATE) y el de actualización (UPDATE) en ambas áreas de asunto, C_PARTY y C_ORGANIZATION. Si algunos campos del objeto principal o del objeto con una relación de uno a uno lógica con el objeto principal son de solo lectura (READ-ONLY), aún podrá editar el objeto principal. Los campos de solo lectura se pueden ver en la vista de datos, pero no se pueden editar. Si todos los campos del objeto principal o del objeto con una relación de uno a uno lógica con el objeto principal tienen permisos de solo lectura (READ-ONLY), no podrá editar el objeto principal en la vista de datos.

Configurar objetos de diseño en la Consola del concentrador

Antes de comenzar, debe configurar todos los objetos de diseño en la Consola del concentrador que usará la aplicación IDD.

En este escenario, son necesarios los siguientes objetos:

- Objeto base de Grupo (Administrador de esquema)
- Paquetes (herramienta Consultas y herramienta Paquetes) que afectan a la búsqueda
- Reglas de coincidencia (Administrador de esquema) que afectan a la búsqueda de duplicados (posibles coincidencias)
- Funciones de limpieza (herramienta Funciones de limpieza) que afectan a la entrada de datos (limpieza en línea de datos al guardar)

Para obtener más información acerca de los objetos y las herramientas de la Consola del concentrador, consulte la *Guía de configuración de Multidomain MDM*.

Nota: Aunque este escenario describe cómo configurar un solo objeto base, los modelos de datos de cliente implican una serie de relaciones entre objetos base. Lo importante es configurar toda la estructura de objetos base y otros objetos de diseño a los que accederán los usuarios de la aplicación IDD.

Configurar usuarios de la aplicación IDD (herramienta Usuarios)

Empiece por configurar SAM añadiendo cuentas de usuario de IDD a la base de datos principal de su implementación de Informatica MDM Hub.

Por ejemplo, en la Consola del concentrador, podría ejecutar la herramienta Usuarios y añadir las siguientes cuentas de usuario:

Cuenta de usuario	Asignada a una función que
user_1	No concede permisos (predeterminado).
user_2	Concede permiso de solo lectura al objeto base de Grupo.
user_3	Concede permiso de creación al objeto base de Grupo.
user_4	Concede permiso de actualización al objeto base de Grupo.

Nota: Asegúrese de que cada usuario tenga acceso a todos los Almacenes de referencias operativas (ORS) asociados a la aplicación IDD. También puede hacer esto en la ficha Usuarios asignados a la base de datos de la herramienta Usuarios y grupos.

Configurar recursos seguros (herramienta Recursos seguros)

Para que IDD tenga acceso a un recurso, debe indicarse como seguro (SECURE) en la herramienta Recursos seguros.

Debe asegurarse de que todos los objetos de diseño configurados anteriormente se definen como recursos seguros (SECURE).

- Objeto base de Grupo, que incluye los siguientes elementos asociados:
  - conjuntos de reglas de coincidencia, que se utilizan en IDD para la búsqueda de duplicados (coincidencias potenciales)
  - metadatos de contenido (HISTORY, RAW y XREF), que se usan en IDD para mostrar el historial de cambios, las referencias cruzadas y los registros sin formato
- funciones de limpieza utilizadas para la entrada de datos
- paquetes utilizados para resultados de búsqueda

Nota:

- Considere la posibilidad de crear grupos de recursos para organizar recursos a los que IDD pueda acceder y para agilizar la configuración de seguridad.
- Si desea evitar que todos los usuarios de IDD tengan acceso a un determinado recurso, defínalo como privado (PRIVATE). Por ejemplo, de esta manera puede ocultar globalmente el acceso de IDD a registros sin formato (RAW).

Crear y configurar una nueva aplicación IDD (Administrador de configuración de IDD)

En el Administrador de configuración de IDD, cree una nueva aplicación IDD y, a continuación, configúrela. Añada un grupo de área de asunto (como un Grupo de partes) y, a continuación, el área de asunto de grupo.

En este escenario, debe especificar todas las columnas de Grupo, el conjunto de reglas de coincidencia de Grupo para comprobaciones de duplicados (debe estar configurado como SECURE) y una función de limpieza (debe estar configurada como SECURE). Cuando haya terminado, guarde los cambios e implemente la aplicación IDD.

Nota: Una manera de restringir el acceso de los usuarios a la información consiste en especificar únicamente un subconjunto de columnas que mostrar en la interfaz gráfica del usuario de IDD. Posteriormente, puede configurar permisos para funciones en el nivel de columna y permitir a algunos usuarios ver una columna y a otros no.

Ver recursos personalizados (herramienta Recursos seguros)

Al implementar por primera vez una aplicación IDD en el Administrador de configuración de IDD, se añade automáticamente un nodo para la aplicación bajo el nodo Recursos personalizados.

Si vuelve a implementar la aplicación, el Administrador de configuración de IDD añade o actualiza todos los objetos de diseño de soporte especiales como recursos seguros (SECURE). Estos objetos de soporte son necesarios para integrar IDD con SAM. Tras guardar los cambios realizados en el área de asunto y volver a implementar la aplicación, vuelva a visitar la herramienta Recursos seguros y preste atención a los recursos personalizados que el archivo de configuración de IDD ha añadido automáticamente.

Nota: Recuerde que puede haber un leve retraso entre el momento en que guarda la configuración de su aplicación y el momento en el que se muestra en la herramienta Recursos seguros.

A continuación, se incluye una breve descripción de estos recursos:

Recurso personalizado	Muestra la capacidad de
REPORT/View	Visualizar informes en el Espacio de trabajo Inicio.
SEARCH_QUERY/Create	Crear consultas privadas.
SEARCH_QUERY/CreatePublic	Crear consultas públicas.
SUBJECT_AREA/ *BaseObject*	Acceder al área de asunto en IDD. Es posible que vea diversos recursos SUBJECT_AREA que obtienen sus datos del mismo objeto base, pero representan vistas distintas. Incluso si la función tiene acceso al objeto base, adicionalmente puede restringir privilegios en estos recursos para limitar el recurso SUBJECT_AREA que la función puede buscar, visualizar, etc.
TASK_TYPE/ *SubjectArea*:*TaskType*	Acceda a la tarea especificada para el área de asunto asociada.

Configurar funciones y privilegios de recurso (herramienta Funciones)

Las funciones proporcionan un control de alta granularidad para definir qué privilegios se asignan a qué recursos.

Para agilizar la configuración de seguridad, incluso puede crear una jerarquía de funciones para asignar funciones a otras funciones. En la Consola del concentrador, utilice la herramienta Funciones para configurar los permisos necesarios para las operaciones de IDD realizadas por esta función.

Crear funciones

Empiece por crear las funciones que desee, como:

Nombre de función	Descripción
party_no_privileges_role	Valor predeterminado inicial. No hay permisos para acceder a nada (equivalente a un usuario sin ninguna función asignada). Este no es un escenario real; se proporciona para mostrar lo que ocurre cuando se añaden privilegios con otras funciones.
party_read_only_role	Concede permiso de solo lectura al objeto base de Grupo.
party_create_role	Concede permiso de creación al objeto base de Grupo.
party_update_role	Concede permiso de actualización al objeto base de Grupo.

Configurar privilegios de recurso para objetos base y objetos afiliados

A continuación, para cada función, debe configurar los privilegios de recursos para objetos base y objetos afiliados.

Para configurar permisos de objetos base en la herramienta Funciones, seleccione la función que desea configurar, expanda el nodo Objetos base, expanda el nodo Grupo y configure privilegios para el objeto base, los metadatos de contenido y los conjuntos de reglas de coincidencia.

La siguiente tabla muestra los privilegios que se deben configurar para este escenario.

Nombre de función	Privilegios del recurso
party_no_privileges_role	Sin permisos.
party_read_only_role	- Privilegios de lectura (READ) en todas las columnas del objeto base de Grupo (PARTY). - Privilegios de lectura (READ) en un conjunto de reglas de coincidencia aplicable. - Privilegios de lectura (READ) en metadatos de contenido (HISTORY, RAW y XREF).
party_create_role	- Privilegios de lectura (READ) en todas las columnas del objeto base de Grupo (PARTY). - Privilegios de lectura (READ) en un conjunto de reglas de coincidencia aplicable. - Privilegios de lectura (READ) en metadatos de contenido (HISTORY, RAW y XREF). - Privilegios de creación (CREATE) en todas las columnas del objeto base de Grupo (PARTY) (necesarios para crear un nuevo registro). - Privilegios de actualización (UPDATE) en todas las columnas del objeto base de Grupo (PARTY) (si desea que esta función también pueda actualizar un registro existente).
party_update_role	- Privilegios de lectura (READ) en todas las columnas del objeto base de Grupo (PARTY). - Privilegios de lectura (READ) en un conjunto de reglas de coincidencia aplicable. - Privilegios de lectura (READ) en metadatos de contenido (HISTORY, RAW y XREF). - Privilegios de actualización (UPDATE) en todas las columnas del objeto base de Grupo (PARTY) (necesarios para guardar cambios en un registro).

Consejos:

- Si su objeto base tiene relaciones con otros objetos base (por ejemplo, relaciones de elemento principal con elementos secundarios, búsquedas de claves externas o relaciones de uno a uno), también debe configurar el acceso a todos estos recursos. Las búsquedas requieren acceso de lectura (READ), mientras que los objetos base relacionados requieren permisos equivalentes al objeto base principal.
- Puede deshabilitar los privilegios de lectura (READ) en determinadas columnas para que los usuarios no puedan verlas en la aplicación IDD. Del mismo modo, puede habilitar privilegios de lectura (READ) y deshabilitar privilegios de actualización (UPDATE) para que los usuarios puedan ver las columnas pero no puedan modificar sus datos.
- Debe configurar el acceso de lectura (READ) a un conjunto de reglas de coincidencia para que funcione la búsqueda de duplicados.
- Puede controlar si una función puede ver el historial (necesita privilegios de lectura [READ] para HISTORY), ver referencias cruzadas (necesita privilegios de lectura [READ] para XREF) y ver registros sin formato (necesita privilegios de lectura [READ] para RAW).
- Seleccione (marque) **Mostrar solo los recursos de esta función** para ver rápidamente los recursos asignados a la función actual.

Configurar privilegios de recurso para paquetes

Las aplicaciones IDD utilizan paquetes para mostrar resultados de búsqueda al ejecutar consultas en la ficha Búsqueda.

Se deben configurar las funciones para que tengan acceso de lectura (READ) en los paquetes asociados al objeto base. Para configurar los permisos de los paquetes en la herramienta Funciones, seleccione la

función que desee configurar, expanda el nodo Paquetes y configure privilegios para los paquetes correspondientes.

Nombre de función	Privilegios del recurso
party_no_privileges_role	Sin privilegios.
party_read_only_role	Privilegios de lectura (READ) en el paquete de Grupo.
party_create_role	Privilegios de lectura (READ) en el paquete de Grupo.
party_update_role	Privilegios de lectura (READ) en el paquete de Grupo.

Configurar privilegios de recurso para funciones de limpieza

Si se configura un área de asunto para que utilice una función de limpieza en línea (se configura en el archivo de configuración de IDD), la función debe tener privilegios de ejecución (EXECUTE) en esa función de limpieza para que dicha función se active al guardar.

Configurar privilegios de recurso para recursos personalizados

A continuación, para cada función (excepto party_no_privileges_role), expanda el nodo Recursos personalizados, expanda el nodo de la aplicación IDD y asigne los siguientes privilegios:

Nombre de función	Privilegios del recurso
party_no_privileges_role	Sin permisos.
party_read_only_role	- Privilegios de lectura (READ) en el recurso CHART/View para que los usuarios puedan ver gráficos en el Espacio de trabajo Inicio. - Privilegios de creación (CREATE) en los recursos SEARCH_QUERY/Create y SEARCH_QUERY/CreatePublic (o de lectura [READ] si desea que los usuarios ejecuten únicamente consultas existentes y no creen nuevas consultas). - Privilegios de lectura (READ) en el recurso SUBJECT_AREA/Party.
party_create_role	- Privilegios de lectura (READ) en el recurso CHART/View para que los usuarios puedan ver gráficos en el Espacio de trabajo Inicio. - Privilegios de lectura (READ) y creación (CREATE) en los recursos SEARCH_QUERY/Create y SEARCH_QUERY/CreatePublic. - Privilegios de lectura (READ) y actualización (UPDATE) en SUBJECT_AREA/Party (solo si desea permitir que la función omita el flujo de trabajo completamente). Normalmente, los usuarios tienen privilegios de lectura (READ) y creación (CREATE) en TASK_TYPE/Party: ReviewNoApprove, que concede a los usuarios acceso al botón **Enviar para aprobar**. - Privilegios de lectura (READ) y actualización (UPDATE) en el recurso SUBJECT_AREA/Party.
party_update_role	- Privilegios de lectura (READ) en el recurso CHART/View para que los usuarios puedan ver gráficos en el Espacio de trabajo Inicio. - Privilegios de lectura (READ) y creación (CREATE) en los recursos SEARCH_QUERY/Create y SEARCH_QUERY/CreatePublic. - Privilegios de lectura (READ) y actualización (UPDATE) en el recurso SUBJECT_AREA/Party (solo si desea permitir que la función omita el flujo de trabajo completamente). Normalmente, los usuarios tienen privilegios de lectura (READ) y actualización (UPDATE) en TASK_TYPE/Party:ReviewNoApprove, que concede a los usuarios acceso al botón **Enviar para aprobar**.

El modo en que configure el acceso a estos recursos personalizados afecta a lo que los usuarios ven en la aplicación IDD. Por ejemplo:

- Si un usuario no tiene privilegios de creación (CREATE) en SEARCH_QUERY/Create, no tendrá la opción de crear ni guardar una nueva consulta en IDD.
- Si un usuario no tiene privilegios de creación (CREATE) en SEARCH_QUERY/CreatePublic, no verá la opción de consulta pública en el cuadro de diálogo Guardar consulta como.
- En general, los usuarios necesitan permisos de lectura (READ) y ejecución (EXECUTE) en las tareas que se les asignan. Si un usuario no tiene privilegios de creación (CREATE) para un recurso TASK_TYPE determinado, no podrá crear esa tarea en IDD.

Consejos de configuración adicionales

- Si desea permitir que una función fusione o anule la fusión de datos, necesita conceder a esa función privilegios de fusión (MERGE) en el objeto base.
- Si desea permitir que una función abra registros en la ficha de vista de jerarquía, necesita concederle acceso de lectura (READ) en el recurso HM_PROFILE (el perfil predeterminado u otro recurso HM_PROFILE aplicable).

  Asimismo, conceda los privilegios de lectura (READ), creación (CREATE), actualización (UPDATE) y/o eliminación (DELETE) adecuados para los recursos HM_RELATIONSHIP_TYPE y HM_HIERARCHY_TYPE.

  Para añadir una entidad (Añadir entidad), la función debe tener privilegios de creación (CREATE) en el área de asunto. Para añadir una relación (Añadir relación), la función debe tener privilegios de creación (CREATE) en la tabla REL, y de lectura (READ) y creación (CREATE) en los recursos HM:PROFILE, HM_RELATIONSHIP_TYPE y HM_HIERARCHY_TYPE.

Asignar funciones a usuarios (herramienta Usuarios y grupos)

En la Consola del concentrador, utilice la herramienta Usuarios y grupos para asignar a los usuarios de IDD las funciones que ha definido.

Cuenta de usuario	Asignar a función
user_1	party_no_privileges_role
user_2	party_read_only_role
user_3	party_create_role
user_4	party_update_role

Qué ejemplo de IDD pueden ver los usuarios y qué pueden hacer

Después de que se hayan asignado privilegios de recursos a las funciones para recursos seguros (SECURE) y de que se hayan asignado funciones a los usuarios, los usuarios podrán iniciar sesión en la aplicación IDD y ver los elementos disponibles.

En este ejemplo, los usuarios pueden ver y hacer lo siguiente:

Nombre de función	Qué puede ver y hacer el usuario
user_1 (sin privilegios)	- En el Espacio de trabajo Inicio, el usuario no puede ver gráficos. - En la ficha de datos, el usuario puede ver la ficha Búsqueda, pero no puede ver consultas públicas ni crear consultas. - En la ficha de datos, el usuario puede ver las diferentes áreas de asunto de la ficha de datos, pero no puede hacer nada con ellas.
user_2 (privilegios de solo lectura)	- En el Espacio de trabajo Inicio, el usuario puede ver gráficos. - En la ficha de datos (ficha Búsqueda), el usuario puede ejecutar una consulta, ver consultas públicas y ver los resultados de la búsqueda (incluidos todos los campos de registros individuales), pero no puede crear ni actualizar una consulta. - En la ficha de datos (área de asunto de Grupo), el usuario no puede crear un nuevo registro.
user_3 (privilegios de creación)	- En el Espacio de trabajo Inicio, el usuario puede ver gráficos. - En la ficha de datos (ficha Búsqueda), el usuario puede ejecutar, crear y actualizar una consulta. - En la ficha de datos (área de asunto de Grupo), el usuario puede crear un nuevo registro de Grupo, añadir datos y guardar cambios.
user_4 (privilegios de actualización)	- En el Espacio de trabajo Inicio, el usuario puede ver gráficos. - En la ficha de datos (ficha Búsqueda), el usuario puede ejecutar, crear y actualizar una consulta. - En la ficha de datos (área de asunto de Grupo), el usuario puede editar un registro de Grupo existente y guardar cambios, pero no puede crear un nuevo registro de Grupo.

APÉNDICE F

Enmascaramiento de datos

Este apéndice incluye los siguientes temas:

Temas relacionados

- "Enmascaramiento de datos" en la página 24

Resumen de enmascaramiento de datos

Este apéndice describe el mecanismo de enmascaramiento de datos.

Este mecanismo se utiliza para ocultar información crítica a los usuarios de IDD que no tienen autorización para acceder a esa información. Para campos enmascarados, IDD reemplaza parte de los caracteres (o todo el valor del campo) por un asterisco (*).

El patrón de enmascaramiento se describe en términos de expresiones regulares. Las partes de la expresión que se deben enmascarar están entre paréntesis.

Expresiones

El patrón de enmascaramiento se describe en términos de expresiones regulares.

Las partes de la expresión que se deben enmascarar están entre paréntesis.

.

Los puntos representan cualquier carácter.

.*

Un punto seguido de un asterisco indica una secuencia de caracteres o una secuencia vacía.

.+

Un punto seguido de un signo más indica uno o más caracteres. Esta expresión no coincide con una secuencia vacía.

.{n}

Un punto seguido de un número entero entre llaves indica hasta n caracteres.

[.]

Un punto entre corchetes representa un carácter de punto.

Patrones de ejemplo

Los siguientes ejemplos muestran patrones de ejemplo.

Enmascarar todo el valor del campo:

```
(.+)
```

Enmascarar todo excepto los tres últimos caracteres:

```
(.+)…
```

No enmascarar los cuatro primeros caracteres:

```
….(.+)
```

Patrón que oculta los cinco primeros caracteres, no enmascara los tres siguientes y oculta el resto del valor salvo los cuatro últimos caracteres:

```
(.{5})…(.+)….
```

Si el patrón especificado no coincide con el valor de campo, se enmascara todo el valor. Por ejemplo, la cadena "ABS" no coincide con el patrón `(.+)…` dado que espera al menos cuatro caracteres (uno al principio que se debe enmascarar y tres al final que no se enmascaran). En este caso, "ABS" se reemplaza por `"***"`.

Ejemplo de definición de enmascaramiento

Las definiciones de enmascaramiento pueden aparecer en el archivo de configuración XML en cualquier sección Diseño.

```
<layout columnsNum="3">
   <column columnUid="C_PRODUCT|PRODUCT_NUMBER" editStyle="FIELD"
horizontalStyle="MEDIUM"
           required="true" showInHMCompactView="true">
      <dataMask value="...(.+)">
         <securityRole roleUid="Customer-CA"/>
      </dataMask>
   </column>
   <column 1columnUid="C_PRODUCT|PRODUCT_NAME" editStyle="FIELD" horizontalStyle="MEDIUM"
           Requi1red="true" showInHMCompactView="true"/>
   <column columnUid="C_PRODUCT|PRODUCT_DESC" editStyle="TEXT_AREA"
horizontalStyle="MEDIUM"/>
...
</layout>
```

El ejemplo anterior muestra la definición de enmascaramiento para la columna Número de producto. El enmascaramiento se aplica a usuarios con la función de seguridad Customer-CA.

Nota: Si no se establecen funciones de seguridad para la definición de enmascaramiento de datos, el enmascaramiento se aplica a todos los usuarios no administradores.

APÉNDICE G

Motor de flujos de trabajo Siperian BPM

Este apéndice incluye los siguientes temas:

Siperian BPM no se admite

En la versión 10.0.0, el motor de flujos de trabajo Siperian BPM ya no se admite y se eliminará en una futura versión. Anteriormente, el motor de flujos de trabajo Siperian BPM era el motor de flujos de trabajo predeterminado en MDM Hub.

Informatica recomienda que actualice las aplicaciones Data Director (IDD) para utilizar la Servidor ActiveVOS.

Para obtener más información, consulte *Guía de migración de Multidomain MDM Data Director*.

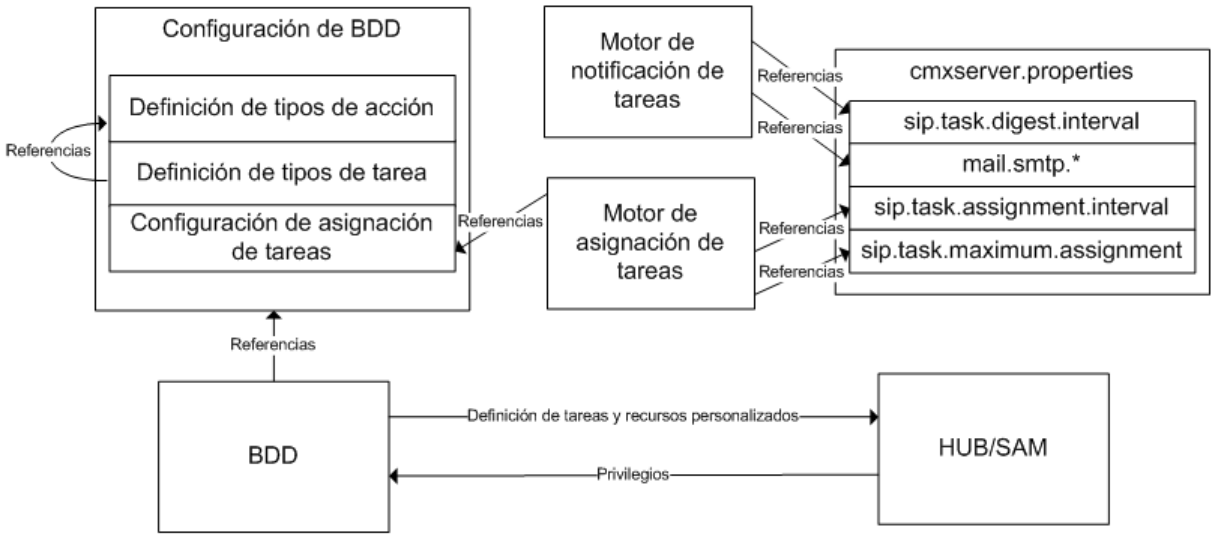
Flujos de trabajo y tareas

Cuando utiliza la herramienta Siperian BPM heredada o herramientas de BPM de otros fabricantes, debe configurar las tareas y la administración de tareas para su aplicación IDD.

Nota: esta sección no se aplica a Informatica ActiveVOS, ya sea incrustado o independiente. La versión incrustada utiliza tareas predefinidas. La versión independiente requiere que defina las tareas en Informatica ActiveVOS.

Diagrama de componentes de configuración de tareas y flujo de trabajo

El siguiente diagrama muestra los componentes de flujo de trabajo y configuración de tareas y sus relaciones.



Descripciones de componentes de configuración de tareas y flujo de trabajo

Componente	Descripción
Definición de tipo de acción	Los *tipos de acción* son bloques de construcción reutilizables para las tareas de un flujo de trabajo. Definen lo que hará una tarea cuando se realice una acción en el contexto de la tarea. Son reutilizables porque muchas tareas proporcionarán subconjuntos similares de acciones que se pueden realizar. **Nota:** La definición del tipo de acción solo se puede personalizar de forma muy limitada en esta versión. No obstante, está planeado que en futuras versiones se incluyan nuevas opciones de personalización.
Definición de tipo de tarea	Los *tipos de tareas* definen los tipos de tareas que pueden utilizarse para crear flujos de trabajo en una aplicación IDD. Esta sección de la configuración permite personalizar las tareas disponibles, así como su comportamiento general. Para obtener más información, consulte "Tipos de tareas" más adelante en este documento.
Configuración de asignación de tareas	Se utiliza para especificar el comportamiento de los mecanismos automático y manual de asignación de tareas. Se configura mediante el Administrador de configuración de IDD (consulte la sección "Administrador de configuración de IDD" anterior en este documento).
Motor de notificación de tareas	Se ejecuta en Informatica MDM Hub y envía notificaciones por correo electrónico a usuarios en un intervalo configurado.
Motor de asignación de tareas	Se ejecuta en Informatica MDM Hub y asigna periódicamente todas las tareas no asignadas a usuarios configurados.
Archivo cmxserver.properties	Especifica varias propiedades que se pueden establecer para configurar el comportamiento de la tarea. Estas propiedades se describen en detalle en las secciones correspondientes más adelante en este documento.
IDD	La aplicación principal carga la configuración al inicio (y a la implementación). IDD también sincroniza la configuración de tarea con SAM al crear metadatos de tarea y personalizar recursos seguros en Informatica MDM Hub.
SAM	Proporciona información a IDD sobre los privilegios concedidos a los usuarios para tipos de tareas.

Nota: Al utilizar flujos de trabajo y tareas como una aplicación, las funciones de las tareas solo estarán disponibles si todos los objetos base de un área de asunto tienen habilitada la administración de estado en el Administrador de esquema de la Consola del concentrador. Esto es necesario porque determinadas tareas utilizan registros pendientes, que solo están disponibles cuando está habilitada la administración de estado.

Configuración de tarea

Cada aplicación IDD se inicializa con una definición de tarea y un flujo de trabajo predeterminados.

Las asignaciones de tareas se configuran en el Administrador de configuración de IDD. En muchos casos, la definición predeterminada será la adecuada. Sin embargo, siempre es necesario configurar la asignación de tareas. Cada una de las siguientes subsecciones se centra en una parte de esta configuración.

Nota: De forma predeterminada, la configuración de tareas para IDD es un proceso de aprobación de dos pasos.

Tipos de tarea

Esta sección del archivo de configuración de IDD especifica los tipos de tareas que se pueden usar en una aplicación IDD.

Los tipos de tarea son el componente de tarea que más se puede configurar. Esta sección determina el comportamiento de tareas en Informatica MDM Hub, así como el flujo de una tarea a la siguiente.

La configuración predeterminada de IDD incluye siete tareas predefinidas:

Tareas predefinidas	Descripción
UpdateWithApproval	Actualice un registro y los próximos pasos requerirán que el usuario complete un proceso de aprobación antes de finalizar la tarea.
UpdateWithOptionalApproval	Actualice un registro y los próximos pasos no requerirán que el usuario complete un proceso de aprobación antes de finalizar la tarea. El paso de aprobación es opcional.
ReviewNoApprove	Revise un cambio y remítalo a una instancia superior o rechácelo. Esta tarea no proporciona una opción de aprobación y requiere que al menos otra persona revise también los cambios.
FinalReview	Revise un cambio y apruébelo, rechácelo o remítalo a una instancia superior.
Fusionar	Fusione registros.
Anular fusión	Anule la fusión de un registro XREF desde un registro de un objeto base.
UpdateRejectedRecord	Actualice un registro rechazado en un proceso de aprobación.

Tipos de tareas: ejemplo de XML

El siguiente ejemplo de fragmento del archivo de configuración de IDD pertenece a tipos de tareas (más adelante en esta subsección se hará referencia a este fragmento).

```
<!-- Task Definitions -->
        <taskType name="UpdateWithApproval" displayName="Update With Approval"
                  creationType="create">
            <description>Update a record and require the user to go through
                         an approval process before completing the task.
            </description>
            <action name="SubmitForApproval">
                <targetTask>ReviewNoApprove</targetTask>
            </action>
            <action name="Augment">
                <targetTask>UpdateWithApproval</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
         <taskType name="UpdateWithOptionalApproval" displayName="Update With Optional
Approval"
```

```
                creationType="create">
            <description>Update a record and do not require the user to go through
                        an approval process before completing the task. The approval
step
                        is optional.
            </description>
            <action name="CompleteUpdate"/>
            <action name="SubmitForApproval">
                <targetTask>ReviewNoApprove</targetTask>
            </action>
            <action name="Augment">
                <targetTask>UpdateWithOptionalApproval</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="ReviewNoApprove" displayName="Review" defaultApproval="true"
                  creationType="none" pendingBVT="true">
            <description>Review a change and either escalate or reject it. This task
                        does not provide an Approve option and requires at least one
                        other person to review the changes as well.
            </description>
            <action name="Reject">
                <targetTask>UpdateWithApproval</targetTask>
            </action>
            <action name="Escalate">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="Reassign">
                <targetTask>ReviewNoApprove</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="FinalReview" displayName="Final Review" creationType="none"
                  pendingBVT="true">
            <description>Review a change and approve, reject or escalate it.</
description>
            <action name="Approve"/>
            <action name="Reject">
                <targetTask>UpdateWithApproval</targetTask>
            </action>
            <action name="Escalate">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="Reassign">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="Merge" displayName="Merge" creationType="merge"
displayType=”merge”>
            <description>Merge two records together.</description>
            <action name="Reassign">
                <targetTask>Merge</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="Unmerge" displayName="Unmerge" creationType="unmerge"
                  displayType=”unmerge”>
            <description>Unmerge an XREF record from a Base Object record.</description>
            <action name="Unmerge"/>
            <action name="Reassign">
                <targetTask>Unmerge</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
```

Puede personalizar flujos de trabajo y tareas modificando las propiedades de los tipos de tarea. Se debe tener cuidado siempre que se modifique la definición de tarea, porque un error podría dejar las tareas inutilizables en una aplicación IDD. La definición de tarea incluye las siguientes propiedades.

Atributos y etiquetas TaskType

nombre

El atributo name es el identificador del tipo de tarea. No utilice espacios ni caracteres que no sean ASCII en el atributo name.

El atributo name es para uso interno de la aplicación IDD y de Informatica MDM Hub, por lo que no es necesario que modifique estos valores. Si introduce un nuevo tipo de tarea, asígnele cualquier nombre, puesto que no será relevante.

displayName

El atributo displayName especifica el nombre de la tarea que debe aparecer en una aplicación IDD.

Sin embargo, el nombre que se muestra en una aplicación IDD se obtiene de un paquete de recursos, por lo que es posible que los cambios en el valor displayName no generen los correspondientes cambios visibles en la aplicación IDD implementada. El nombre de visualización se utiliza como valor predeterminado cuando IDD recupera el nombre de visualización localizado desde un paquete de recursos.

creationType

Este atributo no debe modificarse para las tareas existentes.

Se utiliza para determinar dónde se puede crear una tarea en una aplicación IDD. Los valores posibles son:

creationType	Descripción
crear	Las tareas se crean cuando el usuario de la aplicación IDD selecciona Crear tarea en un menú de una aplicación IDD. **Nota:** Al crear una tarea mediante **Más acciones** > **Crear tarea**, en la ventana **Crear tarea**, solo las tareas configuradas como **CREATE** para la opción **Tipo de creación** aparecerán en el campo desplegable **Tipo**.
fusionar	Se crea una tarea cuando el usuario de la aplicación IDD selecciona el comando para crear una tarea en la vista Coincidencias potenciales. **Nota:** Solo debe haber un tipo de tarea con esta designación.
anular fusión	Se crean tareas cuando el usuario de la aplicación IDD selecciona el comando para crear una tarea en cuadro de diálogo Referencias cruzadas. **Nota:** Solo debe haber un tipo de tarea con esta designación.
ninguna	Los usuarios de la aplicación IDD no pueden crear tareas en la aplicación IDD. Este designación significa que estos tipos de tareas solo puede crearse como resultado de un flujo de trabajo.

Ejemplo: El tipo de tarea FinalReview tiene este designación en el ejemplo de código anterior porque este tipo de tarea solo puede crearse como parte de un flujo (cuando se ejecuta la acción Escalar en una tarea ReviewNoApprove).

displayType

Este atributo especifica cómo debe mostrarse una tarea cuando se abre en la vista de datos.

Los valores posibles son:

displayType	Descripción
Normal	La tarea se abre en la vista de datos con el menú de acciones de tarea disponible. La vista de datos mostrará el registro de datos asociado a la tarea.
Fusionar	La tarea se abre en la vista de datos con el menú de acciones de tarea disponible. La ficha secundaria Coincidencias potenciales está visible y seleccionada en la vista de datos. La coincidencia potencial asociada a la tarea se resalta y se selecciona automáticamente en la ficha secundaria Coincidencias potenciales.
anular fusión	La tarea se abre en la vista de datos con el menú de acciones de tarea disponible. El cuadro de diálogo Referencias cruzadas está abierto en la parte superior de la vista de datos. El registro de referencias cruzadas de anulación de fusión está seleccionado en el cuadro de diálogo.

dataUpdateType

Uno de los siguientes valores.

dataUpdateType	Descripción
ACTIVO	Todas las modificaciones realizadas en el registro que se muestran en la vista de la tarea antes de ejecutar esta acción se guardan con el estado ACTIVO.
PENDIENTE	Todas las modificaciones realizadas en el registro que se muestran en la vista de la tarea antes de ejecutar esta acción se guardan con el estado PENDIENTE. Este valor se utiliza para todos los flujos de aprobación para guardar los cambios como pendientes hasta que se aprueban.
NINGUNO	Todas las modificaciones realizadas en el registro que se muestran en la vista de la tarea antes de ejecutar esta acción se perderán. En este caso, el usuario de la aplicación IDD ve un cuadro de diálogo de confirmación para asegurarse de que desea descartar todos los cambios realizados en el registro. Los cambios se pueden guardar con el botón **Guardar** en la vista de datos antes de ejecutar la acción de tarea.

pendingBVT

Este atributo especifica si la vista de datos debe incluir valores de referencias cruzadas pendientes al crear la vista de BVT en una aplicación IDD.

Si se establece en true, todas las referencias cruzadas pendientes a las que hace referencia la tarea se incluirán en la vista de BVT, de forma que se mostrará al usuario de la aplicación una vista simulada del registro del mismo modo que si se activaran las referencias cruzadas pendientes. Esto es útil para aprobar los cambios pendientes y para intentar decidir si el registro resultante sería correcto.

defaultApproval

Este atributo debe establecerse en true en un tipo de tarea exactamente.

El tipo de tarea que tiene un valor de true para este atributo es el tipo de tarea que se creará cuando se haga clic en el botón **Enviar para aprobar** en la vista de datos de IDD.

Nota: Si varios tipos de tarea tienen este atributo definido en true, se pueden producir resultados inesperados si se crea el tipo de tarea al hacer clic en el botón **Enviar para aprobar**.

Etiqueta de descripción

Este elemento proporciona una breve descripción del objetivo del tipo de tarea.

Etiqueta de acción

Este elemento es una referencia a un tipo de acción que se describe en la siguiente sección.

Etiqueta de tarea de destino

Esta etiqueta es opcional en cada acción de tarea.

Cuando se define, especifica el nombre del tipo de tarea que representa el siguiente paso del flujo de trabajo cuando se ejecuta la acción de incorporación.

Ejemplo: Cuando se invoca la acción Escalar en el tipo de tarea ReviewNoApprove, se crea una nueva tarea FinalReview como próximo paso del flujo de trabajo.

Si se omite esta etiqueta, la acción finalizará el proceso de flujo de trabajo cuando se ejecute.

Ejemplo: La acción de cancelación de tarea, presente en todos los tipos de tarea, finalizará el flujo de trabajo.

Personalización de tipo de tarea

Los tipos de tarea son muy personalizables.

Se pueden crear nuevos tipos de tarea siempre que se sigan las reglas descritas anteriormente. Se pueden modificar flujos existentes al cambiar los valores de las etiquetas de tarea de destino de un tipo de tarea determinado. El siguiente fragmento de código es un ejemplo de un proceso de aprobación de dos pasos y de un proceso de aprobación de un paso.

```
<taskType creationType="NONE" dataUpdateType="ACTIVE"
            defaultApproval="false" displayName="Final Review"
            displayType="NORMAL" name="FinalReview" pendingBVT="true">
            <description>Review a change and approve, reject or escalate it.</
description>
            <action name="Approve"/>
            <action name="Reject">
                <targetTask>UpdateRejectedRecord</targetTask>
            </action>
            <action name="Escalate">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="Reassign">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
```

Tipos de acción

Esta sección del archivo de configuración de IDD especifica los tipos de acciones que puede usar cada tarea en una aplicación IDD.

Cada tipo de tarea define un conjunto de posibles acciones que pueden realizarse en el contexto de la tarea. Como es posible que varios tipos de tarea tengan las mismas acciones o similares, los tipos de acciones se definen fuera del contexto de una tarea y se referencian desde la definición del tipo de tarea, como se ha descrito anteriormente.

Al editar una tarea en el Administrador de configuración de IDD, en la ventana **Configuración de tarea**, puede configurar los tipos de acciones y el siguiente paso de cada tarea. Al trabajar con una tarea en la aplicación IDD, solo los tipos de acciones seleccionados se mostrarán al usuario como un botón y el tipo de tarea seleccionado en la sección **Siguiente paso** ejecutará el siguiente paso del flujo de trabajo para ese tipo de acción determinado.

Nota: Para un tipo de acción seleccionado, si el valor de la sección **Siguiente paso** es **<Empty>**, la acción finalizará el proceso de flujo de trabajo cuando se ejecute.

La siguiente tabla ofrece la lista de tipos de acciones y su descripción:

Tipos de acción	Descripción
SubmitForApproval	Envíe un cambio para su aprobación.
Augment	Asigne la tarea a otro usuario para obtener ayuda.
CompleteUpdate	Confirme los cambios realizados en un registro de área de asunto.
Approve	Apruebe y confirme los cambios realizados en un registro de área de asunto.
Reject	Rechace cambios y vuelva a asignarlos al usuario que los realizó.
Escalate	Asigne la tarea a otro revisor para obtener ayuda. Esto puede provocar que se cree una nueva tarea.
Reassign	Asigne la tarea a otro usuario o función.
Anular fusión	Realice la operación de anular la fusión definida por la tarea.
CancelTask	Elimine la tarea para cancelarla.

Tipos de acción: ejemplo de XML

El siguiente fragmento del archivo de configuración de IDD pertenece a tipos de tareas (más adelante en esta subsección se hará referencia a este fragmento).

```
<!-- Action Definitions - MUST come before the task types definitions. -->
        <actionType name="SubmitForApproval" displayName="Submit For Approval">
            <description>Submit a change for approval.</description>
            <class>com.siperian.dsapp.domain.task.action.SubmitForApproval</class>
        </actionType>
        <actionType name="Augment" displayName="Augment" manualReassign="true">
            <description>Reassign the task to another user for assistance.</description>
```

```
            <class>com.siperian.dsapp.domain.task.action.Reassign</class>
        </actionType>
        <actionType name="CompleteUpdate" displayName="Complete Update">
            <description>Commit changes made to a subject area record.</description>
            <class>com.siperian.dsapp.domain.task.action.CompleteUpdate</class>
        </actionType>
        <actionType name="Approve" displayName="Approve">
            <description>Approve and commit changes made to a subject area record.</
description>
            <class>com.siperian.dsapp.domain.task.action.Approve</class>
        </actionType>
        <actionType name="Reject" displayName="Reject">
            <description>Reject changes and reassign to the user
                         who made the changes.</description>
            <class>com.siperian.dsapp.domain.task.action.Reject</class>
        </actionType>
        <actionType name="Escalate" displayName="Escalate">
            <description>Reassign the task to another reviewer for assistance.
                         This could result in a new task being created.</description>
            <class>com.siperian.dsapp.domain.task.action.Reassign</class>
        </actionType>
        <actionType name="Reassign" displayName="Reassign" manualReassign="true">
            <description>Reassign the task to another user/role.</description>
            <class>com.siperian.dsapp.domain.task.action.Reassign</class>
        </actionType>
        <actionType name="Unmerge" displayName="Unmerge">
            <description>Perform the unmerge operation defined by the task.</description>
            <class>com.siperian.dsapp.domain.task.action.Unmerge</class>
        </actionType>
        <actionType name="CancelTask" displayName="Cancel Task" cancelTask="true">
            <description>Cancel the task by deleting it.</description>
            <class>com.siperian.dsapp.domain.task.action.CancelTask</class>
</actionType>
```

Atributos y etiquetas ActionType

nombre

El atributo name de un tipo de acción no se debe cambiar nunca.

Este atributo es para uso interno de la aplicación IDD y de Informatica MDM Hub, por lo que no es necesario que modifique estos valores. Si introduce un nuevo tipo de acción, asígnele cualquier nombre, puesto que no será relevante.

displayName

Este es el nombre de la acción tal y como se muestra en una aplicación IDD.

Sin embargo, el nombre que se muestra en una aplicación IDD se obtiene de un paquete de recursos, por lo que es posible que los cambios en este valor no generen los correspondientes cambios visibles en la aplicación IDD.

Etiqueta de descripción

Este elemento proporciona una breve descripción del objetivo del tipo de acción.

manualReassign

Cuando este atributo se define en true, se solicita al usuario de la aplicación IDD que seleccione a un usuario determinado para asignarle la tarea antes de que se realice la acción.

Esto se utiliza, por ejemplo, al volver a asignar manualmente una tarea a otro usuario. Si se establece en false, la asignación de la tarea para este tipo de acción es automática.

closeTaskView

Cuando este atributo se define en true, la ficha en la que trabajaba el usuario de la aplicación IDD al realizar esta acción se cerrará y el usuario volverá a la página del Espacio de trabajo Inicio.

El siguiente fragmento de código es un ejemplo de un tipo de acción.

```
<actionType cancelTask="true" closeTaskView="true"
            displayName="Cancel Task" manualReassign="false" name="CancelTask">
            <description>Cancel the task by deleting it.</description>
            <class>com.siperian.dsapp.domain.task.action.CancelTask</class>
        </actionType>
```

Nota: Puede configurar este atributo para cada tipo de acción mediante el archivo de configuración de IDD (IDDConfig.xml). El valor predeterminado de este atributo es true.

cancelTask

Cuando este atributo está definido en true, la tarea se cancela cuando se realiza la acción.

En consecuencia, la tarea se elimina completamente y no se puede recuperar, y todos los cambios pendientes asociados a la tarea se eliminarán permanentemente.

Etiqueta de clase

Este atributo NO debe modificarse en esta versión porque especifica la clase Java que se utiliza para ejecutar la acción.

No es posible añadir controladores de acción personalizados en esta versión, pero se planea incluir esta función en una versión futura.

Configuración de seguridad de tareas

Cuando una instancia de la aplicación IDD se implementa, o cuando el servidor de aplicaciones se reinicia, la aplicación IDD sincroniza un conjunto de recursos personalizados con Informatica MDM Hub.

Este conjunto de recursos personalizados incluye un recurso personalizado para cada área de asunto y cada tipo de tarea por área de asunto (como se define en el archivo de configuración de IDD).

Utilice la herramienta Funciones de la Consola del concentrador para configurar la seguridad para las tareas especificando privilegios para los recursos personalizados de los tipos de tarea.

En una aplicación IDD, se aplican los siguientes privilegios para los tipos de tarea:

Privilegio	Descripción
Lectura	Sin usar.
Crear	Este privilegio es obligatorio para que un usuario de la aplicación IDD pueda crear nuevas tareas. Cuando el usuario selecciona el comando Crear tarea desde la vista de datos, la aplicación IDD muestra un cuadro de diálogo que contiene una lista de posibles tipos de tarea que crear. Esta lista contiene solo los tipos de tarea para los que el usuario tiene el privilegio de creación. Además, las tareas que se muestran en esta lista también deben configurarse correctamente en el archivo de configuración de IDD al definir el atributo creationType en "create".
Actualizar	Sin usar.
Eliminar	Sin usar.
Fusionar	Sin usar.
Ejecutar	Este privilegio es obligatorio para que un usuario de la aplicación IDD vea detalles sobre una tarea y realice modificaciones en esos detalles (como añadir comentarios, modificar la fecha de vencimiento e incluso volver a asignar la tarea). Los usuarios de la aplicación IDD que tienen privilegios de ejecución en un tipo de tarea pueden ejecutar todas las acciones para ese tipo de tarea. Esto es así independientemente de lo que haga la acción cuando se ejecute. Por ejemplo, si hay una acción que crea una nueva tarea, el usuario puede ejecutar la acción incluso si no tiene privilegios de creación en el tipo de tarea que crea la acción.

Importante: Los privilegios para tareas, áreas de asunto y objetos base funcionan conjuntamente en SAM. Una configuración incorrecta de SAM puede provocar un comportamiento inesperado en una aplicación IDD. Una función o un usuario realizan la asignación de tareas (descrita más abajo y administrada en el Administrador de configuración de IDD). IDD no comprueba que la función o el usuario tengan la configuración de seguridad para permitir operaciones en esa tarea. El implementador de la aplicación de IDD será el responsable de configurar esto correctamente. Asimismo, para que un usuario de la aplicación IDD pueda cancelar una tarea, el usuario debe tener el privilegio de eliminación (DELETE) en la XREF para cada objeto base de un área de asunto.

Asignación de tarea

Configuración de asignación de tareas

Cada área de asunto de la aplicación IDD puede configurarse para que use un conjunto determinado de tipos de tarea.

A su vez, cada tipo de tarea puede estar vinculado con una o varias funciones de seguridad o con un solo nombre de usuario. De esta manera, la tarea de un tipo de tarea concreto solo se puede asignar a usuarios con las funciones de seguridad determinadas o al usuario especificado en la definición de la asignación de tarea.

En el archivo de configuración XML, la asignación de tareas se puede definir mediante la etiqueta `taskAssignmentConfig`.

Ejemplo:

```
<taskAssignmentConfig task="UpdateWithApproval">
                    <securityRole roleUid="DataSteward"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="UpdateWithOptionalApproval" >
                    <securityRole roleUid="DataSteward"/>
                    <securityRole roleUid="Customer-NY"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="UpdateRejectedRecord" user=”user1”/>
                <taskAssignmentConfig task="ReviewNoApprove">
                    <securityRole roleUid="Manager"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="FinalReview" >
                    <securityRole roleUid="SrManager"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="Merge">
                    <securityRole roleUid="DataSteward"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="Unmerge">
                    <securityRole  roleUid="DataSteward"/>
                </taskAssignmentConfig>
```

En el ejemplo anterior, las tareas `UpdateWithOptionalApproval` se pueden asignar a usuarios con una función de Gestor de datos o de Cliente-NY. Las tareas del tipo UpdateRejectedRecord solo se pueden asignar a un usuario (user1).

El elemento de asignación de tareas debe contener la tarea de `atributo` requerida, con el nombre de los tipos de tarea definidos en la configuración de IDD. Asimismo, debe contener una o más funciones de seguridad del elemento secundario o un atributo de usuario con el nombre de un usuario, al que se le puede asignar la tarea del tipo particular.

IU de configuración de asignación de tareas

Puede especificar la asignación de tareas mediante la ficha Asignación de tareas del cuadro de diálogo Área de asunto de IDD.

Al hacer clic en la ficha **Asignación de tareas**, se muestran los tipos de tarea que se pueden utilizar con el área de asunto. Puede seleccionar un tipo de tarea y hacer clic en **Agregar** para añadirla al área de asunto.

Si todos los tipos de tarea definidos en la instancia de la aplicación IDD ya se han añadido al área de asunto, el botón Agregar estará deshabilitado.

Puede modificar un tipo de tarea seleccionado con el botón **Editar**. El botón **Eliminar** permite quitar un tipo de tarea del área de asunto.

Debe seleccionar la opción **Asignar a función** para modificar o añadir funciones. Las funciones de seguridad definidas en Informatica MDM Hub (mediante Informatica MDM Hub) se pueden mover a la lista de funciones seleccionadas y vincular con el tipo de tarea para un área de asunto.

Asignación automática de tareas

La asignación de tareas automática se controla mediante un demonio del servidor que se ejecuta como parte de Informatica MDM Hub.

La frecuencia con la se ejecuta se controla mediante el valor de la propiedad sip.task.assignment.interval en cmxserver.properties. De forma predeterminada, este valor se establece en cero, lo que significa que el demonio está deshabilitado. Solo se debe habilitar si se ejecutan aplicaciones IDD y necesita asignar tareas. Para habilitar el demonio, defina un valor en minutos para sip.task.assignment.interval. Un valor de 1 provocará que el demonio se ejecute una vez por minuto. Este demonio tiene dos tareas:

Asignará cualquier tarea sin propietario (rowid_user nulo) como se define en la configuración de asignación de tareas de la aplicación IDD.

Examinará todas las entradas de tablas de coincidencia asociadas con una tabla principal del área de asunto configurada y creará tareas para asignarlas a los usuarios de la aplicación IDD disponibles.

Un *usuario disponible* (a) tiene menos tareas asignadas actualmente que la cantidad máxima configurada y (b) tiene asignada la función especificada en la configuración de asignación de tareas. Puede configurar el número máximo de tareas que se pueden asignar automáticamente a un usuario de una aplicación IDD especificando la propiedad sip.task.maximum.assignment en el archivo cmxserver.properties. El número máximo de tareas predeterminado que asignar por usuario es 25.

Cuando se asignan tareas automáticamente, se seleccionan los usuarios de la aplicación IDD de la función configurada para la asignación de tareas de modo Round-Robin hasta que no haya más usuarios con menos del número máximo de tareas permitidas asignadas. Cada vez que el demonio de asignación se ejecuta, asignará todas las tareas no asignadas que pueda. Si no hay suficientes usuarios para recibir todas las tareas sin asignar, es posible que queden tareas sin asignar después de que se ejecute el demonio (que se asignarán cuando haya espacio disponible en la cola de tareas de un usuario de la aplicación IDD de destino). Cuando se realice la asignación de tareas automática, no se puede predecir con certeza qué usuario de la aplicación IDD recibirá una tarea determinada. Si es necesario asignar una tarea a un usuario concreto, se debe emplear la asignación manual.

Personalización de asignación automática de tareas

La asignación de tarea automática se puede personalizar mediante la salida de usuario AssignTasks.

La salida de usuario AssignTasks funciona con el adaptador del flujo de trabajo de Siperian BPM.

Asignación manual de tareas

El usuario de la aplicación IDD controla la asignación de tareas manual en la aplicación IDD.

Al crear tareas, los usuarios tienen la opción de seleccionar un usuario de destino para la tarea. Si se especifica, el usuario seleccionado se convierte en el propietario de la tarea recientemente creada. Si se deja en blanco, el demonio de asignación automática asigna la tarea al siguiente usuario disponible.

Personalización de asignación de tareas

La asignación de tarea manual se puede personalizar mediante la salida de usuario GetAssignableUsersForTasks.

La salida de usuario GetAssignableUsersForTasks funciona con el adaptador del flujo de trabajo de Siperian BPM.

Cambiar tareas asignadas

Las aplicaciones IDD pueden administrar asignaciones de tareas en la ficha de administración de tareas.

Si por ejemplo se asigna una tarea a un usuario que no está en la oficina, un administrador puede utilizar la aplicación IDD para asignar sus tareas a otro usuario.

Si un usuario no va a estar disponible durante un período de tiempo, puede impedir que se le asignen tareas automáticamente quitando a ese usuario de la función.

Notificación de tarea

La notificación de tareas es directa.

A intervalos de tiempo configurados, se puede enviar un correo electrónico de resumen a usuarios que poseen tareas. El demonio se ejecuta como parte de Informatica MDM Hub. El intervalo en el que se envían las notificaciones se puede configurar como un número determinado de horas en el archivo cmxserver.properties con la propiedad sip.task.digest.interval. El intervalo de notificación predeterminado es de 0 horas, por lo que los resúmenes están deshabilitados. Para habilitarlos, modifique este valor para reflejar una cantidad de horas.

A continuación, se incluye un ejemplo de un correo electrónico de resumen:

```
Desde: siperian_task_notification@siperian.com Para: null Asunto: Resumen de tareas del
gestor de datos para versión Mime de administración: 1.0 Tipo de contenido: text/plain;
charset=us-ascii Contenido-Transferencia-Codificación: 7bit Tareas completadas desde la
última notificación: 0 tareas asignadas totales: Este mensaje ha sido enviado por el
demonio de notificaciones de tareas del servidor del concentrador de Siperian.
```

Nota: No se puede personalizar el cuerpo del correo electrónico de resumen.

Configuración del correo electrónico de notificaciones de tareas

Para configurar el correo electrónico de notificaciones de tareas, edite las propiedades en el archivo cmxserver.properties. Debe configurar una ubicación del servidor SMTP saliente.

La siguiente lista describe las propiedades del correo electrónico de notificaciones de tareas que puede configurar en el archivo cmxserver.properties:

mail.smtp.sender

La dirección de correo electrónico del remitente. El valor predeterminado es siperian_task_notification@siperian.com.

mail.smtp.host

El nombre de host del servidor de correo.

mail.smtp.port

El número de puerto del servidor de correo.

mail.smtp.auth

Determina si el servidor de correo especificado requiere la autenticación para mensajes salientes. Debe establecer mail.smtp.auth en true si está usando el servidor de correo de Informatica MDM Hub.

mail.smtp.user

El nombre de usuario para el servidor de correo saliente. Debe especificar un valor para mail.smtp.user si mail.smtp.auth es true.

mail.smtp.password

La contraseña para el mail.smtp.user especificado. Debe especificar un valor para mail.smtp.password si mail.smtp.auth es true.

Configuración del administrador de usuarios en la Consola del concentrador

Además, para que los usuarios de la aplicación IDD reciban correo electrónico, la cuenta de correo electrónico entrante se debe definir en Informatica MDM Hub.

En la herramienta Usuarios de la Consola del concentrador, especifique la dirección de correo electrónico a la que se deben enviar las notificaciones para el usuario de IDD. Solo se enviará un correo electrónico si hay tareas asignadas a un usuario de la aplicación IDD.

Mediciones de administración de tareas e informes

Las mediciones de administración de tareas muestran la distribución de las tareas de Data Director.

Los administradores pueden utilizar mediciones de administración de tareas para mostrar la distribución de tareas de Informatica Data Director. Puede generar informes basados en las siguientes mediciones de administración de tareas:

Área de asunto de tarea por fecha de creación

Los usuarios pueden ver tendencias de fecha de creación para un área de asunto. Use `task_sa_by_create_date` como nombre de informe para configurar y rellenar el data mart para este informe.

Área de asunto de tarea por fecha de vencimiento

Los usuarios pueden ver informes basados en el número de registros con intervalos de fechas de vencimiento que el administrador especifica cuando se configura el informe. Use `task_sa_by_due_date` como nombre de informe para configurar y rellenar el data mart para este informe.

Área de asunto de tarea por prioridad

Los usuarios pueden ver informes basados en el número de registros con prioridades como "Baja", "Media" y "Alta". Use `task_sa_by_priority` como nombre de informe para configurar y rellenar el data mart para este informe.

Área de asunto de tarea por estado

Los usuarios pueden ver informes basados en el número de registros con estados de fecha de vencimiento como "A tiempo" y "Retrasado". Use `task_sa_by_status` como nombre de informe para configurar y rellenar el data mart para este informe.

Área de asunto de tarea por tipo de tarea

Los usuarios pueden ver informes basados en el número de registros con tipos de tarea como "Actualizar con aprobación", "Fusionar" y "Anular fusión". Use `task_sa_by_task_type` como nombre de informe para configurar y rellenar el data mart para este informe.

Tarea por área de asunto

Los usuarios pueden ver informes basados en el número de registros con áreas de asunto como "Persona", "Organización" y "Producto". Use `task_by_subject_area` como nombre de informe para configurar y rellenar el data mart para este informe.

Destinatario de la asignación de tarea por prioridad

Los usuarios pueden ver informes basados en el número de registros para un destinatario de la asignación con prioridades como "Baja", "Media" y "Alta". Use `task_assignee_by_priority` como nombre de informe para configurar y rellenar el data mart para este informe.

Destinatario de la asignación de tarea por estado

Los usuarios pueden ver informes basados en el número de registros para un destinatario de la asignación con estados de fecha de vencimiento como "A tiempo" y "Retrasado". Use `task_assignee_by_status` como nombre de informe para configurar y rellenar el data mart para este informe.

Seguridad de datos en datos de tarea

IDD permite a los usuarios autorizados participar en flujos de trabajo, que son modelos informáticos de trabajo real que implican una serie de operaciones o actividades. La seguridad de datos de IDD afecta a las siguientes áreas de tareas:

- Comprobar si existen permisos de visualización (si un usuario puede abrir una tarea o no). Si el usuario no tiene permiso para abrir una tarea, verá un mensaje de advertencia.
- Filtrar datos secundarios (qué registros secundarios ve el usuario en la vista de datos).

Nota:

- Los filtros de seguridad de datos no se aplican en datos de XREF. Por ejemplo, si un usuario tiene acceso a los datos del objeto principal y sus datos secundarios, de conformidad con la seguridad de datos, el usuario podrá ver todas las XREF contributivas.
- La lógica de la aplicación de filtros de seguridad de datos depende del tipo de tarea.

Tarea de revisión

La principal diferencia entre abrir los objetos principales regulares y revisar las tareas en la vista de datos es que los filtros de seguridad no se aplican en un estado activo del objeto principal y sus elementos secundarios. La seguridad de datos se aplica después de que la función de BVT de vista previa se haya ejecutado en los registros pendientes generales asociados a la tarea.

Abrir tareas de revisión con una sola función

Un usuario con una sola función únicamente puede abrir una tarea si se cumplen las siguientes condiciones:

- Todos los registros pendientes asociados a la tarea deben cumplir los filtros de seguridad de datos.
- Si hay varios filtros en una sola columna para una única función, el usuario tendrá acceso a una unión de todos los datos que cumplen cada filtro.
- Si hay filtros en varias columna para una única función, el usuario tendrá acceso a una intersección de todos los datos que cumplen cada filtro.
- Si existen filtros de seguridad configurados en los registros secundarios o secundarios de segundo nivel, debe cumplirse una de las siguientes condiciones:
  - El objeto principal tiene al menos un registro que supera las restricciones de seguridad en cada ficha secundaria con la seguridad de datos habilitada.
  - Hay un registro pendiente asociado a la tarea, que pertenece a una ficha secundaria, con la seguridad de datos habilitada y que reúne los valores de seguridad de datos de conformidad con la condición anterior.

Por ejemplo, piense en un modelo de seguridad de datos en el que el usuario tenga la función SalesManager-NY y tenga configurados los siguientes filtros de seguridad:

- Filtro 1: El código de estado es NY.
- Filtro 2: El tipo de teléfono es Trabajo y Casa.
- Filtro 3: El código de tratamiento personal es Sr.

Con el modelo de seguridad de datos indicado anteriormente, imagine una situación en la que la base de datos tenga un registro del objeto principal para el Sr. Florian Amadeu, con la dirección de facturación en el estado de Nueva York (NY) y el tipo de teléfono definido en Fax. Un usuario sin restricciones de seguridad de datos añade un nuevo teléfono de trabajo y crea una tarea de **Enviar para aprobar**. El usuario con la función SalesManager-NY podrá abrir el registro del Sr. Florian Amadeu en la vista de datos puesto que cumple las tres condiciones anteriores. El propio objeto principal satisface la seguridad de datos (Filtro 3) y tiene al menos un registro en cada elemento secundario con la seguridad de datos habilitada (dirección de Nueva York (registro activo) y teléfono de trabajo (registro pendiente)).

Con el mismo modelo de seguridad de datos indicado anteriormente, imagine una situación en la que la base de datos tenga un registro del objeto principal para el Sr. Dominic Wilkins, con la dirección de facturación en el estado de Nueva York (NY) y sin ningún tipo de teléfono. Un usuario sin restricciones de seguridad de datos añade un nuevo teléfono de trabajo y crea una tarea de **Enviar para aprobar**. El usuario con la función SalesManager-NY no podrá abrir la tarea, ya que el usuario no tiene teléfono que cumpla el Filtro 2.

Abrir tareas de revisión con varias funciones

Un usuario con varias funciones únicamente puede abrir la tarea si se cumplen las siguientes condiciones:

- Todos los registros pendientes asociados a la tarea deben cumplir los filtros de seguridad de datos para al menos una función de usuario.
- Un usuario con varias funciones puede tener aplicadas combinaciones de filtros. Como resultado, el usuario tendrá acceso a todos los datos disponibles en cada función asignada (una unión de las asignaciones de filtro).
- Si existen filtros de seguridad configurados en los elementos secundarios o secundarios de segundo nivel, debe cumplirse una de las siguientes condiciones:
  - El objeto principal tiene al menos un registro que supera las restricciones de seguridad en cada ficha secundaria con la seguridad de datos habilitada.
  - El registro pendiente asociado a la tarea tiene una ficha secundaria con la seguridad de datos habilitada y reúne los valores de seguridad de datos, como se indica en la condición anterior.

Por ejemplo, imagine un modelo de seguridad de datos en el que el usuario tenga la función SalesManager-NY con los filtros de seguridad de datos indicados en la sección "Abrir tareas de revisión con una sola función" en la página 162, además de la función CarSalesManager-NJ, que tiene configurados los siguientes filtros de seguridad:

- Filtro 1: El código de estado es NJ.
- Filtro 2: El año del vehículo es el 2009.

Asimismo, el usuario tiene otra función CarSalesManager-CA, que tiene el siguiente filtro de seguridad configurado.

- Filtro 1: El código de estado de dirección es CA.
- Filtro 2: El año del vehículo es el 2008.

Con el modelo de seguridad de datos indicado anteriormente, imagine una situación en la que la base de datos tenga un registro del objeto principal para el Sr. Derrick Rose, con la dirección de facturación en el estado de California (CA) y el tipo de teléfono definido en Casa. Un usuario sin restricciones de seguridad de

datos añade una nueva dirección de facturación en el estado de Nueva York (NY) y crea una tarea de **Enviar para aprobar**. El usuario con la función SalesManager-NY podrá abrir el registro del Sr. Derrick Rose en la vista de datos, puesto que cumple los filtros de seguridad de la función SalesManager-NY.

Con el mismo modelo de seguridad de datos indicado anteriormente, imagine una situación en la que la base de datos tenga un registro del objeto principal para el Sr. Tyros Thomas, con la dirección de facturación en el estado de California (CA) y un coche fabricado en 2008. Un usuario sin restricciones de seguridad de datos cambia la dirección de facturación a Nueva Jersey (NJ) y crea una tarea de **Enviar para aprobar**. El usuario con las funciones CarSalesManager-CA y CarSalesManager-NJ no puede abrir la tarea, ya que el Sr. Tyros Thomas no cumple los filtros para CarSalesManager-CA y CarSalesManager-NJ con el registro pendiente para la nueva dirección.

Filtrar registro secundario en la vista de tarea

IDD aplica filtros de seguridad al obtener datos para fichas secundarias en la vista de datos. Por ejemplo, piense en un modelo de seguridad de datos en el que el usuario tenga la función SalesManager-CA y tenga el código de estado de dirección de facturación del filtro de seguridad CA.

Con el modelo de seguridad de datos indicado anteriormente, imagine una situación en la que la base de datos tenga un registro del objeto principal para el Sr. Blake Griffin, con dos direcciones de facturación, una en la ciudad de Nueva York y otra en Bloomfield Hills, ambas en el estado de Nueva York (NY). El usuario sin restricciones de seguridad de datos cambia el valor de estado de Bloomfied Hills a California (CA), crea una dirección de facturación adicional en Los Ángeles (California, CA) y, a continuación, crea una tarea de **Enviar para aprobar**. El usuario con la función SalesManager-NY podrá abrir el registro del Sr. Blake Griffin en la vista de datos y puede ver dos direcciones de CA en la ficha **Dirección de facturación**. Una de ellas es la anterior dirección de Nueva York que ha cambiado, mientras que la segunda es la nueva dirección añadida. El filtro no muestra la dirección de Nueva York que no ha cambiado cuando se aplican filtros de seguridad en la BVT de vista previa.

Abrir tareas de fusión/anular fusión

IDD aplica las siguientes reglas para determinar si el usuario puede abrir la tarea de fusión o anular fusión.

- La tarea de fusión solo se puede abrir si todos los objetos principales que se van a fusionar cumplen los ajustes de seguridad de datos.
- La tarea de anular fusión se puede abrir si el objeto principal puede abrirse de conformidad con los ajustes de seguridad de datos.

Por ejemplo, piense en un modelo de seguridad de datos en el que el usuario tenga la función SalesManager-CA y tenga el código de estado de dirección de facturación del filtro de seguridad CA.

Con el modelo de seguridad de datos mencionado anteriormente, imagine una situación en la que haya dos personas en la base de datos que se llamen Kevin Durant. Una de estas personas tiene una dirección de facturación en Los Ángeles (CA) y la otra tiene una dirección de facturación en Nueva York (NY). El usuario sin restricciones de seguridad de datos crea una tarea de **fusión** para registros de dos personas. Los usuarios con la función SalesManager- CA no podrán abrir la tarea, ya que no tienen el permiso necesario para abrir el registro de una persona con dirección de facturación en el estado de Nueva York (NY) y, por lo tanto, no pueden realizar una tarea de **fusión** completa.

Asignación de tareas con reconocimiento de datos

Al asignar una tarea en el cuadro de diálogo **Asignar tarea**, IDD filtra a los revisores de tareas que no tienen el privilegio para abrir la tarea. Asimismo, para la asignación de tareas automática, el demonio asigna la tarea solo a los usuarios que tienen el privilegio para abrir la tarea.

APÉNDICE H

Códigos de configuración regional

Este apéndice incluye los siguientes temas:

Códigos de idioma

Código ISO	Idioma
aa	Afar
ab	Abjasio
af	Afrikáans
am	Amárico
ar	Árabe
as	Asamés
ay	Aimara
az	Azerí
ba	Baskir
be	Bielorruso
bg	Búlgaro
bh	Bihari
bi	Bislama

Código ISO	Idioma
bn	Bengalí
bo	Tibetano
br	Bretón
ca	Catalán
co	Corso
cs	Checo
cy	Galés
da	Danés
de	Alemán
dz	Butaní
el	Griego
en	Inglés
eo	Esperanto
es	Español
et	Estonio
eu	Euskera
fa	Persa
fi	Finés
fj	Fiyi
fo	Feroés
fr	Francés
fy	Frisio
ga	Irlandés
gd	Gaélico escocés
gl	Gallego
gn	Guaraní
gu	Guyaratí

Código ISO	Idioma
ha	Hausa
he	Hebreo (anteriormente iw)
hi	Hindi
hr	Croata
hu	Húngaro
hy	Armenio
ia	Interlingua
id	Indonesio (anteriormente in)
ie	Interlingue
ik	Iñupiaq
is	Islandés
it	Italiano
iu	Inuit
ja	Japonés
jw	Javanés
ka	Georgiano
kk	Kazajo
kl	Groenlandés
km	Camboyano
kn	Canarés
ko	Coreano
ks	Cachemir
ku	Kurdo
ky	Kirguis
la	Latin
ln	Lingala
lo	Laosiano

Código ISO	Idioma
lt	Lituano
lv	Letón
mg	Malgache
mi	Maorí
mk	Macedonio
ml	Malabar
mn	Mongol
mo	Moldavo
mr	Maratí
ms	Malayo
mt	Maltés
my	Birmano
na	Nauru
ne	Nepalí
nl	Neerlandés
no	Noruego
oc	Occitano
om	(Afan) Oromo
o	Oriya
pa	Punyabí
pl	Polaco
ps	Pastún
pt	Portugués
qu	Quechua
rm	Retorromance
rn	Kirundi
ro	Rumano

Código ISO	Idioma
ru	Ruso
rw	Kiñaruanda
sa	Sánscrito
sd	Sindhi
sg	Sango
sh	Serbocroata
si	Cingalés
sk	Eslovaco
sl	Esloveno
sm	Samoano
sn	Shona
so	Somalí
sq	Albanés
sr	Serbio
ss	Suazi
st	Sesotho
su	Sudanés
sv	Sueco
sw	Suajili
ta	Tamil
te	Telugu
tg	Tayiko
th	Tailandés
ti	Tigriña
tk	Turcomano
tl	Tagalo
tn	Setsuana

Código ISO	Idioma
to	Tonga
tr	Turco
ts	Xitsonga
tt	Tártaro
tw	Twi
ug	Uigur
uk	Ucraniano
ur	Urdú
uz	Uzbeko
vi	Vietnamita
vo	Volapük
wo	Wólof
xh	Xhosa
yi	Yidis (anteriormente ji)
yo	Yoruba
za	Chuang
zh	Chino
zu	Zulú

Temas relacionados

- "Tablas de búsqueda con columna de subtipo" en la página 66

Códigos de país

País	Código de dos letras	N.º de ISO
ISLAS ÅLAND	AX	248
AFGANISTÁN	AF	4

País	Código de dos letras	N.º de ISO
ALBANIA	AL	8
ARGELIA	DZ	12
SAMOA AMERICANA	AS	16
ANDORRA	AD	20
ANGOLA	AO	24
ANGUILA	AI	660
ANTÁRTIDA	AQ	10
ANTIGUA Y BARBUDA	AG	28
ARGENTINA	AR	32
ARMENIA	AM	51
ARUBA	AW	533
AUSTRALIA	AU	36
AUSTRIA	AT	40
AZERBAIYÁN	AZ	31
BAHAMAS	BS	44
BARÉIN	BH	48
BANGLADÉS	BD	50
BARBADOS	BB	52
BIELORRUSIA	BY	112
BÉLGICA	BE	56
BELICE	BZ	84
BENÍN	BJ	204
BERMUDAS	BM	60
BUTÁN	BT	64
BOLIVIA	BO	68
BOSNIA-HERZEGOVINA	BA	70
BOTSUANA	BW	72

País	Código de dos letras	N.º de ISO
ISLA BOUVET	BV	74
BRASIL	BR	76
TERRITORIO BRITÁNICO DEL OCÉANO ÍNDICO	IO	86
BRUNÉI DARUSSALAM	BN	96
BULGARIA	BG	100
BURKINA FASO	BF	854
BURUNDI	BI	108
CAMBOYA	KH	116
CAMERÚN	CM	120
CANADÁ	CA	124
CABO VERDE	CV	132
ISLAS CAIMÁN	KY	136
REPÚBLICA CENTROAFRICANA	CF	140
CHAD	TD	148
CHILE	CL	152
CHINA	CN	156
ISLA NAVIDAD	CX	162
ISLAS COCOS (KEELING)	CC	166
COLOMBIA	CO	170
COMORAS	KM	174
CONGO, República Democrática del (antes Zaire)	CD	180
CONGO, República del	CG	178
ISLAS COOK	CK	184
COSTA RICA	CR	188
COSTA DE MARFIL	CI	384
CROACIA (nombre local: Hrvatska)	HR	191
CUBA	CU	192

País	Código de dos letras	N.º de ISO
CHIPRE	CY	196
REPÚBLICA CHECA	CZ	203
DINAMARCA	DK	208
YIBUTI	DJ	262
DOMINICA	DM	212
REPÚBLICA DOMINICANA	DO	214
ECUADOR	EC	218
EGIPTO	EG	818
EL SALVADOR	SV	222
GUINEA ECUATORIAL	GQ	226
ERITREA	ER	232
ESTONIA	EE	233
ETIOPÍA	ET	231
ISLAS MALVINAS	FK	238
ISLAS FEROE	FO	234
FIYI	FJ	242
FINLANDIA	FI	246
FRANCIA	VI	250
GUYANA FRANCESA	GF	254
POLINESIA FRANCESA	PF	258
TIERRAS AUSTRALES FRANCESAS	TF	260
GABÓN	GA	266
GAMBIA	GM	270
GEORGIA	GE	268
ALEMANIA	DE	276
GHANA	GH	288
GIBRALTAR	GI	292

País	Código de dos letras	N.º de ISO
GRECIA	GR	300
GROENLANDIA	GL	304
GRANADA	GD	308
GUADALUPE	GP	312
GUAM	GU	316
GUATEMALA	GT	320
GUINEA	GN	324
GUINEA-BISSAU	GW	624
GUYANA	GY	328
HAITÍ	HT	332
ISLAS HEARD Y MC DONALD	HM	334
HONDURAS	HN	340
HONG KONG	HK	344
HUNGRÍA	HU	348
ISLANDIA	IS	352
INDIA	IN	356
INDONESIA	ID	360
IRÁN (REPÚBLICA ISLÁMICA DE)	IR	364
IRAK	IQ	368
IRLANDA	IE	372
ISRAEL	IL	376
ITALIA	IT	380
JAMAICA	JM	388
JAPÓN	JP	392
JORDANIA	JO	400
KAZAJISTÁN	KZ	398
KENIA	KE	404

País	Código de dos letras	N.º de ISO
KIRIBATI	KI	296
COREA, REPÚBLICA POPULAR DEMOCRÁTICA DE	KP	408
COREA, REPÚBLICA DE	KR	410
KUWAIT	KW	414
KIRGUIZISTÁN	KG	417
LAOS, REPÚBLICA DEMOCRÁTICA POPULAR DE	LA	418
LETONIA	LV	428
LÍBANO	LB	422
LESOTO	LS	426
LIBERIA	LR	430
JAMAHIRIYA ÁRABE LIBIA	LY	434
LIECHTENSTEIN	LI	438
LITUANIA	LT	440
LUXEMBURGO	LU	442
MACAO	LU	446
MACEDONIA, ANTIGUA REPÚBLICA YUGOSLAVA DE	MK	807
MADAGASCAR	MG	450
MALAUI	MW	454
MALASIA	MY	458
MALDIVAS	MV	462
MALÍ	ML	466
MALTA	MT	470
ISLAS MARSHALL	MH	584
MARTINICA	MQ	474
MAURITANIA	MR	478
MAURICIO	MU	480
MAYOTTE	YT	175

País	Código de dos letras	N.º de ISO
MÉXICO	MX	484
MICRONESIA, ESTADOS FEDERADOS DE	FM	583
MOLDAVIA, REPÚBLICA DE	MD	498
MÓNACO	MC	492
MONGOLIA	MN	496
MONTSERRAT	MS	500
MARRUECOS	MA	504
MOZAMBIQUE	MZ	508
MYANMAR	MM	104
NAMIBIA	NA	516
NAURU	NR	520
NEPAL	NP	524
PAÍSES BAJOS	NL	528
ANTILLAS NEERLANDESAS	AN	530
NUEVA CALEDONIA	NC	540
NUEVA ZELANDA	NZ	554
NICARAGUA	NI	558
NÍGER	NE	562
NIGERIA	NG	566
NIUE	NU	570
ISLA NORFOLK	NF	574
ISLAS MARIANAS DEL NORTE	MP	580
NORUEGA	NO	578
OMÁN	OM	512
PAKISTÁN	Clave principal	586
PALAU	PW	585
PALESTINA, TERRITORIO OCUPADO DE	PS	275

País	Código de dos letras	N.º de ISO
PANAMÁ	PA	591
PAPÚA NUEVA GUINEA	PG	598
PARAGUAY	PY	600
PERÚ	PE	604
FILIPINAS	PH	608
PITCAIRN	PN	612
POLONIA	PL	616
PORTUGAL	PT	620
PUERTO RICO	PR	630
QATAR	QA	634
REUNIÓN	RE	638
RUMANIA	RO	642
FEDERACIÓN RUSA	RU	643
RUANDA	RW	646
SANTA ELENA	SH	654
SAN CRISTÓBAL Y NIEVES	KN	659
SANTA LUCÍA	LC	662
SAN PEDRO Y MIQUELÓN	PM	666
SAN VICENTE Y LAS GRANADINAS	VC	670
SAMOA	WS	882
SAN MARINO	SM	674
SANTO TOMÉ Y PRÍNCIPE	ST	678
ARABIA SAUDÍ	SÁ	682
SENEGAL	SN	686
SERBIA Y MONTENEGRO	CS	891
SEYCHELLES	SC	690
SIERRA LEONA	SL	694

País	Código de dos letras	N.º de ISO
SINGAPUR	SG	702
ESLOVAQUIA	SK	703
ESLOVENIA	SI	705
ISLAS SALOMÓN	SB	90
SOMALIA	SO	706
SUDÁFRICA	ZA	710
ISLAS GEORGIA DEL SUR Y SANDWICH DEL SUR	GS	239
ESPAÑA	ES	724
SRI LANKA	LK	144
SUDÁN	SD	736
SURINAM	SR	740
ISLAS SVALBARD Y JAN MAYEN	SJ	744
SUAZILANDIA	SZ	748
SUECIA	SE	752
SUIZA	CH	756
SIRIA, REPÚBLICA ÁRABE	SY	760
TAIWÁN	TW	158
TAYIKISTÁN	TJ	762
TANZANIA, REPÚBLICA UNIDA DE	TZ	834
TAILANDIA	JU	764
TIMOR ORIENTAL	TL	626
TOGO	TG	768
TOKELAU	TK	772
TONGA	TO	776
TRINIDAD Y TOBAGO	TT	780
TÚNEZ	TN	788
TURQUÍA	TR	792

País	Código de dos letras	N.º de ISO
TURKMENISTÁN	TM	795
ISLAS TURCAS Y CAICOS	TC	796
TUVALU	TV	798
UGANDA	UG	800
UCRANIA	UA	804
EMIRATOS ÁRABES UNIDOS	AE	784
REINO UNIDO	GB	826
ESTADOS UNIDOS	ES	840
ISLAS MENORES ALEJADAS DE LOS ESTADOS UNIDOS	UM	581
URUGUAY	UY	858
UZBEKISTÁN	UZ	860
VANUATU	VU	548
SANTA SEDE (ESTADO DE CIUDAD DEL VATICANO)	VA	336
VENEZUELA	VE	862
VIET NAM	VN	704
ISLAS VÍRGENES BRITÁNICAS	VG	92
ISLAS VÍRGENES DE ESTADOS UNIDOS	VI	850
ISLAS WALLIS Y FUTUNA	WF	876
SAHARA OCCIDENTAL	EH	732
YEMEN	YE	887
ZAMBIA	ZM	894
ZIMBABUE	ZW	716

APÉNDICE I

Solución de problemas

Este apéndice incluye los siguientes temas:

Resumen de solución de problemas

Este apéndice incluye algunas sugerencias que describen qué comprobar si se detectan resultados inesperados en la configuración de la aplicación IDD.

Comprobar la configuración de SAM

Compruebe que SAM tenga los permisos adecuados asignados en todos los niveles necesarios de acuerdo con la documentación.

Áreas en las que comprobar CRUD:

- Si se requieren las referencias cruzadas y los historiales de cambios con botones habilitados en la aplicación IDD, el contenido de los metadatos adecuados (objetos XREF y HIST) son recursos SECURE y también se configura en consecuencia.
- Consultas/Paquetes: asegúrese de que los recursos son SECURE. De lo contrario, es posible que una aplicación IDD no permita el acceso a toda el área de asunto.

Comprobar la configuración de la función de limpieza

Si las funciones de limpieza están configuradas, asegúrese de que:

- Cada función de limpieza es un recurso SECURE.
- Las funciones que necesitan acceder a la función de limpieza tienen permiso de ejecución.

Los metadatos de Informatica Data Director no se han actualizado

Informatica Data Director mantiene una memoria caché de los metadatos de MDM Hub que describe los objetos base, las columnas las relaciones, etc. Para borrar la memoria caché de la aplicación IDD seleccionada y hacer que IDD vuelva a cargar los metadatos, haga clic en **Borrar memoria caché** en el Administrador de configuración de IDD.

También puede reiniciar el servidor de aplicaciones para borrar la memoria caché.

Informatica Data Director deja de responder al cambiar entidades

Informatica Data Director deja de responder al cambiar entidades para relaciones del Administrador de jerarquía para sistemas de origen que no están habilitados para el reemplazo de administración de estado.

El comportamiento se produce para entornos de JBoss en ejecución en Java 1.7. Para solucionar este problema, debe configurar el archivo `standalone-full.xml`.

1. Abra el archivo `standalone-full.xml` para editarlo. El archivo se encuentra en el siguiente directorio:
   - En UNIX. `<directorio de instalación de JBoss>/jboss-eap-6.1/standalone/configuration`
   - En Windows. `<directorio de instalación de JBoss>\jboss-eap-6.1\standalone\configuration`
2. Añada el siguiente código XML al archivo `standalone-full.xml` para configurar el control asíncrono para el registrador:

```
<async-handler name="ASYNC">
   <level name="INFO"/>
   <queue-length value="1024"/>
   <overflow-action value="BLOCK"/>
      <subhandlers>
         <handler name="FILE"/>
         <handler name="CONSOLE"/>
      </subhandlers>
</async-handler>
```

3. En <subsystem xmlns="urn:jboss:domain:logging:1.2"> en el archivo `standalone-full.xml`, añada el siguiente código XML para configurar la administración asíncrona del registrador raíz:

```
<root-logger>
   <level name="INFO"/>
```

```
        <handlers>
           <handler name="ASYNC"/>
        </handlers>
     </root-logger>
```

4. Reinicie el servidor de aplicaciones.

La configuración de Informatica Data Director no es válida

Si recibe el error de que la configuración de Informatica Data Director no es válida, valide el archivo `IDDconfig.xml` en el esquema `siperian-bdd-config-6.xsd`.

El esquema `siperian-bdd-config-6.xsd` se encuentra en el kit de recurso en el siguiente directorio:

- En UNIX. `<directorio de instalación de infamdm>/hub/resourcekit/sdk/bddXsdDoc`
- En Windows. `<directorio de instalación de infamdm>\hub\resourcekit\sdk\bddXsdDoc`

El rendimiento de las coincidencias es muy lento

Los usuarios de la aplicación de IDD informan de que el rendimiento de las coincidencias es muy lento.

Habilite la propiedad `needLoadChildOnOpen` y reinicie el servidor de aplicaciones.

Para habilitar la propiedad, ejecute las siguientes instrucciones SQL en la base de datos de ORS:

```
insert into C_REPOS_DS_PREF_DETAIL (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE) select
'BDDGP.30', rowid_ds_pref, 'needLoadChildOnOpen', 'true' from C_REPOS_DS_PREF where name =
'___SYSTEM_PREFERENCES_ROOT___';

commit;
```

APÉNDICE J

Glosario

administración de estado

El proceso para administrar el estado del sistema de los registros de objetos base y referencias cruzadas que afectan a la lógica de procesamiento en el flujo de datos. Puede asignar un estado del sistema a registros de objetos base y de referencias cruzadas en distintas etapas del flujo de datos mediante las herramientas del concentrador que funcionan con registros. Además, puede utilizar las distintas herramientas del concentrador para administrar su esquema para permitir la administración de estado de un objeto base, o para establecer los permisos de usuario para controlar quién puede cambiar el estado de un registro.

La administración de estado está limitada a los estados siguientes: ACTIVO, PENDIENTE y ELIMINADO.

administración de procesos empresariales (BPM)

La administración de procesos empresariales se centra en la adaptación de los procesos de una organización. Informatica MDM incluye un motor de administración de procesos empresariales incorporado. Mediante este motor se pueden automatizar los procesos de revisión y aprobación de los datos principales.

administrador

Usuario de la aplicación IDD que tiene la responsabilidad principal de configurar la aplicación IDD.

Administrador de acceso de seguridad (SAM)

El Administrador de acceso de seguridad (SAM) es el marco de seguridad integral de Informatica MDM Hub para proteger los recursos de Informatica MDM Hub de accesos no autorizados. En tiempo de ejecución, SAM aplica las decisiones de las políticas de seguridad de su organización para su implementación de Informatica MDM Hub, de forma que la autenticación de usuarios y la autorización de acceso se gestionen conforme a su configuración de seguridad.

Administrador de configuración de IDD

Una utilidad basada en web que se utiliza para añadir, modificar y administrar aplicaciones IDD.

Administrador de esquema

El Administrador de esquema es un componente de tiempo de diseño de la Consola del concentrador que se utiliza para definir el esquema, además de para definir las tablas de ensayo y de conexión. El Administrador de esquema también se utiliza para definir reglas de coincidencia y fusión, validación y colas de mensajes.

Administrador de jerarquía

El Administrador de jerarquía permite a los usuarios administrar los datos de jerarquía que estén asociados a los registros administrador en el MDM Hub. Para obtener más información, consulte la *Guía de configuración de Multidomain MDM* y la *Guía del gestor de datos de Multidomain MDM*.

Almacén del concentrador

En una implementación de Informatica MDM HUB, la base de datos que contiene la base de datos principal y una o más bases de datos de Almacenes de referencias operativas (ORS).

Almacén de referencias operativas (ORS)

Es un esquema de base de datos que almacena las reglas para procesar los datos principales, las reglas para administrar el conjunto de objetos de datos principales, junto con las reglas de procesamiento y la lógica auxiliar que utiliza Informatica MDM Hub al definir la mejor versión de confianza (BVT).

anular fusión

Proceso de anulación de la fusión de registros fusionados anteriormente. Solo para objetos base con estilo de fusión.

Aplicación IDD

La unidad de configuración e implementación principal de la implementación de IDD. Una aplicación IDD es lo que ven los usuarios profesionales al iniciar IDD e iniciar sesión.

archivos auxiliares

Los archivos auxiliares son archivos temporales que se crean en diferentes circunstancias, al editar o exportar un proyecto.

Área de asunto

El concepto de organización principal de una aplicación IDD. Un área de asunto representa un conjunto de datos que se debe tratar como una unidad desde una perspectiva empresarial.

asignación

Define un conjunto de transformaciones que se aplican a datos de origen. Las asignaciones se utilizan durante el proceso de transferencia a tabla provisional (o al usar la solicitud API SiperianClient CleansePut) para transferir datos desde una tabla de conexión a una tabla de ensayo. Una asignación identifica la columna de origen en la tabla de conexión y la columna de destino que se debe completar en la tabla de ensayo, junto con cualquier función de limpieza intermedia utilizada para limpiar los datos.

autenticación

Proceso de comprobación de la identidad de un usuario para asegurarse de que es quien dice ser. En la aplicación IDD, los usuarios se autentican según las credenciales que proporcionan (nombre de usuario y contraseña, carga de seguridad o ambos métodos). La aplicación IDD proporciona un mecanismo de autenticación interno y también permite que los usuarios se autentiquen mediante otros proveedores de autenticación.

base de datos

Conjunto organizado de datos en el almacén del concentrador. Informatica MDM Hub admite dos tipos de bases de datos: una base de datos principal y un Almacén de referencias operativas (ORS).

Base de datos principal

Base de datos que contiene los valores de configuración del entorno de Informatica MDM Hub (cuentas de usuario, configuración de seguridad, registro de ORS, configuración de la cola de mensajes, etc.). Un determinado entorno de Informatica MDM Hub solo puede tener una base de datos principal. El nombre predeterminado de la base de datos principal es CMX_SYSTEM.

clave de coincidencia

Cadenas codificadas que representan los datos en la columna de clave de coincidencia parcial del objeto base. Las claves de coincidencia están formadas por valores codificados, comprimidos y de longitud fija generados a partir de una combinación de las palabras y números de un nombre o una dirección, de forma que las variaciones relevantes tengan el mismo valor de clave de coincidencia. Las claves de coincidencia son una parte de los tokens de coincidencia que se generan durante el proceso de tokens, se almacenan en la tabla de claves de coincidencia y se utilizan posteriormente durante el proceso de coincidencia para identificar candidatos de coincidencia.

clave de coincidencia parcial

Columna especial en el objeto base que el Administrador de esquema añade si una columna de coincidencia utiliza la estrategia de búsqueda/coincidencia parcial. Esta columna es el campo principal utilizado durante la búsqueda y coincidencia para generar candidatos de coincidencia para este objeto base. Todos los objetos base de coincidencia parcial tienen una única clave de coincidencia parcial.

clave externa

En una base de datos relacional, una columna (o un conjunto de columnas) cuyo valor se corresponde con un valor de clave principal en otra tabla (o, excepcionalmente, en la misma tabla). La clave externa actúa como un puntero a la otra tabla. Por ejemplo, la columna Department_Number de la tabla Employee sería una clave externa que apunta a la clave principal de la tabla Department.

coincidencia

El proceso de determinar si se deben fusionar automáticamente dos registros o si deben ser candidatos para una fusión manual porque los dos registros tienen valores idénticos o similares en las columnas especificadas.

coincidencia parcial

Una estrategia de búsqueda/coincidencia que utiliza coincidencias probabilísticas, que tienen en cuenta variaciones ortográfícas, posibles errores ortográficos y otras diferencias que pueden hacer que los registros coincidentes no sean idénticos.

columna de coincidencia

Una columna que se utiliza en una regla de coincidencia para establecer comparaciones. Cada columna de coincidencia se basa en una o más columnas del objeto base.

Confianza

La confianza es un mecanismo para medir el factor de confianza asociado con cada celda según su sistema de origen, historial de cambios y otras reglas empresariales. La confianza tiene en cuenta la antigüedad de los datos, el nivel de descenso de su fiabilidad a lo largo del tiempo y la validez de los datos.

conjunto de reglas de coincidencia

Un conjunto lógico de reglas de coincidencia que permiten a los usuarios ejecutar diferentes conjuntos de reglas en distintas etapas del proceso de coincidencia. Los conjuntos de reglas de coincidencia incluyen un nivel de búsqueda que dicta la estrategia de búsqueda, cualquier número de reglas de coincidencia automáticas y manuales y, opcionalmente, un filtro que permite incluir o excluir selectivamente registros durante el proceso de coincidencia. Los conjuntos de reglas de coincidencia se utilizan para ejecutarse para reglas de columna de coincidencia, pero no reglas de coincidencia de clave principal.

Consola del concentrador

Interfaz de usuario de Informatica MDM Hub que incluye un conjunto de herramientas para administradores y gestores de datos. Cada herramienta permite a los usuarios realizar una determinada acción o un conjunto de acciones relacionadas, como generar el modelo de datos, ejecutar tareas por lotes, configurar el flujo de datos, configurar el acceso de aplicaciones externas a los recursos de Informatica MDM Hub y otras tareas de configuración y operativas del sistema.

Control de datos

El control de datos es la práctica de administrar datos como un activo corporativo en toda la empresa. Se realiza a través de procesos, políticas, estándares, tecnologías y personal de toda la organización para garantizar la disponibilidad de datos precisos, coherentes y oportunos para facilitar la toma de decisiones y mejorar los procesos empresariales.

Datos en vuelo

Los datos en vuelo son los datos empresariales que pueden pasar por distintos estados (ACTIVO, PENDIENTE o ELIMINADO) mientras progresan por un flujo de trabajo.

Datos principales

Un conjunto de entidades comunes y principales (junto con sus atributos y valores) que se consideran críticas para el negocio de una empresa y que se deben utilizar en dos o más sistemas o procesos empresariales. Varios ejemplos de datos principales podrían ser los datos de productos, empleados, proveedores y ubicaciones.

deduplicar

Es una técnica para eliminar datos redundantes.

duplicar

Uno o más registros en los que los datos de determinadas columnas (como el nombre, la dirección o los datos de organización) son idénticos o prácticamente idénticos. Las reglas de coincidencia ejecutadas durante el proceso de coincidencia determinan si dos registros son lo suficientemente similares para considerarse duplicados para fines de consolidación.

Enmascaramiento de datos

Se trata de un mecanismo para ocultar información según las funciones de seguridad.

entidad

Una entidad es un objeto, persona, lugar o cosa que tiene significado y sobre la que se puede actuar en la base de datos.

entidad de negocio

Una estructura anidada de objetos base. Utilice la vista Entidad 360 en Informatica Data Director para ver toda la información relacionada con el objeto base raíz de una entidad de negocio. Realice una búsqueda en Informatica Data Director para buscar datos en una entidad de negocio.

esquema

El modelo de datos que se utiliza en la implementación de Informatica MDM Hub de un cliente. Informatica MDM Hub no impone ni requiere ningún esquema determinado. El esquema es independiente de los sistemas de origen.

estado del sistema

Describe la compatibilidad de los registros de objeto base con Informatica MDM Hub. Los siguientes estados son compatibles: ACTIVO, PENDIENTE y ELIMINADO.

Filtro de seguridad

El filtro de seguridad especifica una condición que IDD aplica para restringir y proteger los datos del área de asunto a los que pueden acceder los usuarios individuales. Se pueden definir filtros en la columna del objeto principal, en la columna secundaria y en la columna secundaria de segundo nivel. Puede configurar cualquier número de filtros para un área de asunto.

flujo de trabajo

En Informatica Multidomain MDM, un flujo de trabajo representa un proceso empresarial de una organización. Consulte *proceso empresarial* en la página 189.

función de limpieza

IDD permite utilizar funciones de limpieza ya definidas en MDM para limpiar, estandarizar y validar datos de entrada. Puede usar esta función para la estandarización y validación de direcciones, así como para el aumento de datos de otros orígenes.

gestor de datos

Usuario de la aplicación IDD que tiene la responsabilidad principal de la calidad de datos.

Grupo de área de asunto

Un conjunto de una o más áreas de asunto que tienen el mismo objeto base en su raíz (también llamado objeto principal).

grupo de recursos

Un conjunto de recursos seguros que simplifica la asignación de privilegios, lo que permite asignar privilegios a varios recursos al mismo tiempo, como asignar fácilmente grupos de recursos a una función.

grupo de usuarios

Un conjunto lógico de cuentas de usuario.

jerarquía

En el Administrador de jerarquía, un conjunto de tipos de relaciones. Estos tipos de relación no se clasifican según la posición de las entidades en la jerarquía ni están necesariamente relacionados entre sí. Simplemente son tipos de relación que se agrupan para facilitar la clasificación y la identificación.

Kit de recurso

El kit de recurso de Informatica MDM Hub es un conjunto de utilidades, ejemplos y bibliotecas que proporcionan ejemplos de las funciones de Informatica MDM Hub que se pueden ampliar e implementar.

limpieza de datos

El proceso de estandarizar el diseño y el contenido de datos, descomponer y analizar valores de texto en elementos identificables, verificar valores identificables (como códigos postales) con bibliotecas de datos y reemplazar valores incorrectos por valores correctos de bibliotecas de datos.

linaje

Los sistemas y registros de esos sistemas que han contribuido a los registros consolidados en el almacén del concentrador.

Marco de servicios de integración (SIF)

La parte de Informatica MDM Hub que interactúa con programas cliente. Lógicamente, actúa como un segundo nivel en el modelo de cliente/servidor. Permite implementar las interacciones de solicitud/respuesta que usan cualquiera de las siguientes variaciones arquitectónicas:

- Servicios web emparejados ligeramente mediante el protocolo SOAP.
- Llamadas a procedimientos remotos de Java fuertemente acoplados basados en Enterprise JavaBeans (EJBs) o XML.
- Mensajes basados en el servicio de mensajes de Java (JMS) asincrónico.
- Documentos XML que se transfieren mediante el protocolo de transferencia de hipertexto (HTTP).

mejor versión de confianza (BVT)

Un registro que se ha consolidado con las mejores celdas de datos de los registros de origen. En ocasiones se abrevia como BVT.

metadatos

Datos que se utilizan para describir otros datos. En Informatica MDM Hub, los metadatos se utilizan para describir el esquema (modelo de datos) que se usa en la implementación de Informatica MDM Hub, junto con los valores de configuración relacionados.

metadatos de contenido

Datos que describen los datos empresariales que Informatica MDM Hub ha procesado. Los metadatos de contenido se almacenan en tablas de compatibilidad para un objeto base, como tablas de referencias cruzadas, tablas del historial y de otro tipo. Los metadatos de contenido se utilizan para ayudarle a determinar de dónde proceden los datos del objeto base y cómo han cambiado con el tiempo.

Modelo de datos

El modelo de datos es un modelo abstracto que describe cómo se estructuran y organizan los datos.

objeto base

Una tabla que contiene información sobre una entidad relevante para su negocio, como un cliente o una cuenta.

objeto base de relación

Un objeto base de relación es un objeto base utilizado para almacenar información acerca de las relaciones del Administrador de jerarquía.

objeto de diseño

Partes de los metadatos que se usan para definir el esquema y otros valores de configuración para una implementación. Entre los objetos de diseño se incluyen instancias de los siguientes tipos de objetos de Informatica MDM Hub: columnas y objetos base, tablas de conexión y de ensayo, columnas, índices, relaciones, asignaciones, funciones de limpieza, consultas y paquetes, valores de confianza, reglas de validación y de coincidencia, definiciones del Administrador de acceso de seguridad, definiciones del Administrador de jerarquía y otros valores.

objeto del concentrador

Un término genérico para diferentes tipos de objetos definidos en el concentrador que contienen información acerca de sus entidades empresariales. Estos son algunos ejemplos: objetos base, tablas de referencias cruzadas y cualquier objeto del concentrador que pueda asociar con mediciones de informes.

origen de datos

En el entorno de servidor de aplicaciones, un origen de datos es un recurso JDBC que identifica información sobre una base de datos, como la ubicación del servidor de la base de datos, el nombre de la base de datos, el ID y la contraseña del usuario de la base de datos, etc. Informatica MDM Hub necesita esta información para comunicarse con un ORS.

parentReference

Una parentReference se puede definir en el XML para la columna que es la clave externa del registro secundario. Define una etiqueta que se mostrará en el registro secundario de segundo nivel que contiene datos del elemento secundario, para ayudar a los usuarios a entender la relación del elemento de segundo nivel con el elemento secundario.

proceso

Consulte *proceso empresarial* en la página 189.

proceso almacenado

Un conjunto con nombre de sentencias de lenguaje de consulta estructurado (SQL) compiladas y almacenadas en el servidor de base de datos. Las tareas por lotes de Informatica MDM Hub se codifican en procedimientos almacenados para que se puedan ejecutar mediante scripts de ejecución de tarea en software de programación de tareas (como Tivoli o CA Unicenter).

proceso de validación

Proceso de comprobación de la integridad de los metadatos que describen un repositorio. El proceso de validación compara el modelo lógico de un repositorio con su esquema físico. Si se produce algún problema, Administrador de repositorios genera una lista de problemas que requieren atención.

proceso empresarial

Los procesos empresariales son flujos de trabajo que cumplen objetivos organizativos e implementan funciones empresariales. Los procesos empresariales contienen las actividades necesarias para cumplir los objetivos y definen las rutas de ejecución de las actividades. Multidomain MDM incluye procesos empresariales de Informatica ActiveVOS predefinidos que se administran mediante el Servidor ActiveVOS. El objetivo organizativo de estos procesos consiste en garantizar que el personal autorizado, que incluye a los administradores de negocio o los gestores de datos, revise todas las actualizaciones de los datos principales.

Proveedor de inicio de sesión externo

Un plug-in que se usa con IDD para autenticar a los usuarios en proveedores de identidad externos.

Proveedor de inicio de sesión personalizado

Se trata de un módulo que se conecta y sirve para autenticar usuarios cuando se inicia la aplicación IDD.

referencia de elemento del mismo nivel

Una referencia de elemento del mismo nivel es una relación de un registro de un área de asunto con un registro secundario de esa área de asunto. Por ejemplo, un cliente podría incluir registros secundarios de dirección y número de teléfono, y que el número de teléfono incluya una clave externa para asociarlo con una dirección específica.

regla de coincidencia

Define los criterios en los que se basa Informatica MDM Hub para determinar si los registros pueden ser duplicados. Las columnas de coincidencia se combinan en reglas de coincidencia para determinar las condiciones en las que dos registros se consideran suficientemente similares para fusionarse. Cada regla de coincidencia dice a Informatica MDM Hub la combinación de columnas de coincidencia que necesita para examinar los puntos de similitud.

Relaciones de área de asunto

Las relaciones de área de asunto definen cómo se relacionan las áreas de asunto entre sí. El área de asunto puede tener áreas de asunto secundarias, áreas de asunto secundarias de segundo nivel y referencias de elemento del mismo nivel.

ruta de coincidencia

Permite atravesar la jerarquía entre registros, tanto si esa jerarquía existe entre objetos base (rutas entre tablas) como dentro de un solo objeto base (rutas dentro de tablas). Las rutas de coincidencia se utilizan para configurar las reglas de columna de coincidencia que afectan a registros relacionados en tablas distintas o en la misma tabla.

salida de usuario

Las salidas de usuario permiten añadir lógica empresarial personalizada a operaciones de IDD estándar.

Seguridad de datos

La seguridad de datos restringe los registros que pueden ver los usuarios en función del contenido de esos registros.

servicio de entidad de negocio

Un servicio de entidad de negocio es un conjunto de operaciones que ejecutan código de MDM Hub para crear, actualizar, eliminar y buscar registros de objeto base en una entidad de negocio.

Servidor de coincidencia de limpieza

El componente de tiempo de ejecución Servidor de coincidencia de limpieza es un servlet que gestiona las solicitudes de limpieza. Este servlet está implementado en un entorno de servidor de aplicaciones. El servlet contiene dos componentes de servidor:

- un servidor de limpieza que gestiona operaciones de limpieza de datos;
- un servidor de coincidencia que gestiona operaciones de coincidencia.

El Servidor de coincidencia de limpieza es multiproceso, de modo que cada instancia puede procesar varias solicitudes de forma simultánea. Se puede implementar en diversos servidores de aplicaciones.

El Servidor de coincidencia de limpieza interactúa con todos los motores de limpieza compatibles, como el motor de limpieza Trillium Director. El Servidor de coincidencia de limpieza y el motor de limpieza estandarizan los datos. Esta función de estandarización colabora estrechamente con Informatica Consolidation Engine (antes llamado Merge Engine) para optimizar los datos para la consolidación.

Servidor del concentrador

Un componente de tiempo de ejecución en el nivel intermedio (servidor de aplicaciones) que se utiliza para servicios principales y comunes, como la administración de sesiones, seguridad y acceso.

tabla de coincidencia

Tipo de tabla del sistema, asociada con un objeto base, que es compatible con el proceso de coincidencia. Durante la ejecución de una tarea de coincidencia para un objeto base, Informatica MDM Hub rellena la tabla de coincidencia asociada con los valores ROWID_OBJECT para cada par de registros coincidentes, así como el identificador de la regla de coincidencia que generó la coincidencia y un indicador de fusión automática.

tabla de historial

Un tipo de tabla de un ORS que contiene información del historial acerca de los cambios de una tabla asociada. Las tablas de historial proporcionan opciones detalladas de control de cambios, como la fusión y la anulación de fusión del historial, el historial de datos previamente limpiados, el historial de objetos base y el historial de referencias cruzadas.

tipo de coincidencia

Cada columna de coincidencia tiene un tipo de coincidencia que determina la forma en que la columna de coincidencia se agrupará en tokens para preparar la comparación de coincidencias.

tipo de datos

Define las características de los valores permitidos en una columna de tabla (caracteres, números, fechas, datos binarios, etc.).

valor nulo

La ausencia de un valor en una columna de un registro. Nulo no es lo mismo que en blanco o cero.

INDICE

G

H

I

J

L

M

N

O

P

R

S

T

V