Informatica® Multidomain MDM
10.4 HotFix 2

Guía de seguridad

Informatica Multidomain MDM Guía de seguridad
10.4 HotFix 2
Diciembre 2020

Fecha de publicación: 2021-01-14

Tabla de contenido

Prefacio

Utilice la *Guía de seguridad de Multidomain MDM* de Informatica® para saber cómo habilitar la seguridad en Multidomain MDM. Aprenda a utilizar el Administrador de acceso de seguridad para proteger los recursos de MDM Hub y use Dynamic Data Masking para impedir el acceso a los datos confidenciales. Aprenda también a administrar usuarios y grupos y a usar permisos, privilegios y funciones para administrar la seguridad de los usuarios.

Esta guía asume que posee conocimientos de los sistemas operativos, los entornos de base de datos y el servidor de aplicaciones.

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 a la seguridad de MDM Hub

Este capítulo incluye los siguientes temas:

Resumen de la seguridad de MDM Hub

MDM Hub protege los datos frente al acceso y la manipulación no autorizados para preservar la confidencialidad de la información y la integridad de los datos.

Puede utilizar el Administrador de acceso de seguridad en la Consola del concentrador para proteger los recursos de MDM Hub y aplicar directivas de seguridad operativa, incluidas la autenticación y la autorización de los usuarios.

Puede utilizar Dynamic Data Masking para impedir el acceso a los datos confidenciales. Por ejemplo, puede utilizar Dynamic Data Masking para ocultar los números de tarjetas de crédito a todos los usuarios que carezcan de derechos administrativos.

La seguridad en las implementaciones de MDM Hub se puede configurar de varias maneras. Puede utilizar proveedores de seguridad de otros fabricantes para controlar elementos de seguridad específicos de su organización, o puede configurar MDM Hub para que administre todos los aspectos de la seguridad. Para obtener más información sobre el uso de Marco de servicios de integración (SIF) para configurar la seguridad, consulte la *Guía del marco de servicios de integración de Multidomain MDM*.

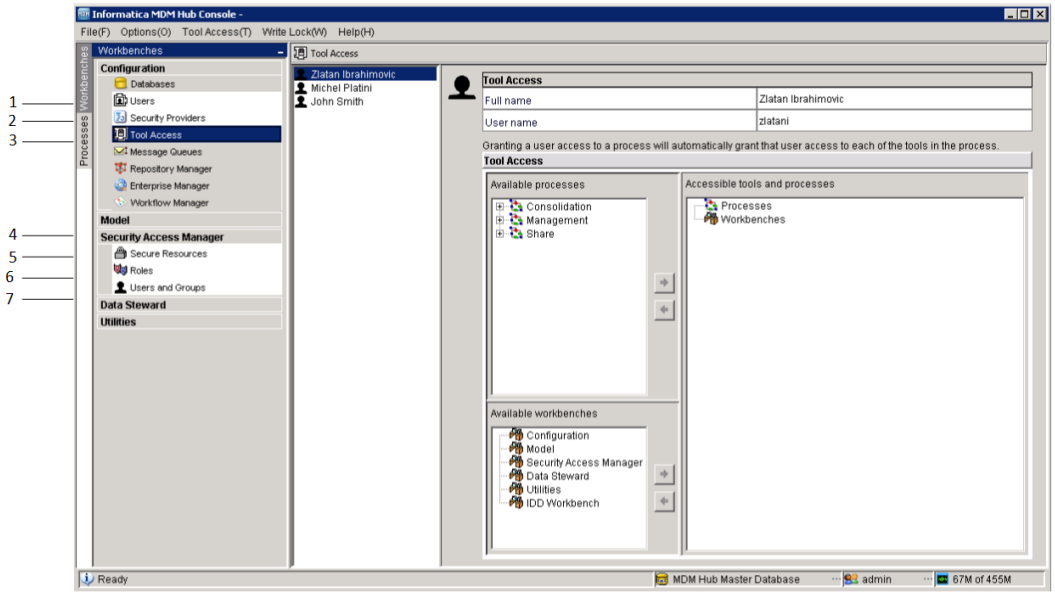
Importante: Antes de comenzar a proteger Multidomain MDM, asegúrese de que el servidor de aplicaciones y los dispositivos de almacenamiento en memoria caché estén protegidos.

Consola de MDM Hub

Utilice la Consola del concentrador para configurar la seguridad en MDM Hub.

Para controlar los privilegios de acceso a las herramientas de la Consola del concentrador, puede utilizar la herramienta Acceso a herramientas en el entorno de trabajo de configuración. Por ejemplo, puede utilizar la herramienta Acceso a herramientas para denegar a los gestores de datos el acceso a todas las herramientas de la Consola del concentrador, excepto a las herramientas Administrador de datos y Administrador de fusión.

La siguiente imagen muestra la interfaz de la Consola del concentrador:



1. herramienta Usuarios
2. herramienta Proveedores de seguridad
3. herramienta Acceso a herramientas
4. Administrador de acceso de seguridad
5. herramienta Recursos seguros
6. herramienta Funciones
7. herramienta Usuarios y grupos

Dynamic Data Masking

Informatica Dynamic Data Masking es un producto de seguridad de datos que opera entre un cliente y una base de datos para impedir el acceso no autorizado a la información confidencial. Dynamic Data Masking intercepta las solicitudes enviadas a la base de datos y aplica las reglas de enmascaramiento de datos a la solicitud para enmascarar los datos antes de devolverlos al cliente.

Puede utilizar Dynamic Data Masking para enmascarar o impedir el acceso a los datos confidenciales almacenados tanto en bases de datos de producción como en bases de datos que no son de producción administradas por MDM Hub. Configure las reglas de conexión para identificar las solicitudes entrantes y las

reglas de seguridad para definir cómo desea enmascarar los datos. Dynamic Data Masking supervisa las solicitudes entrantes para bases de datos de MDM Hub y modifica la solicitud de base de datos antes de enviarla a la base de datos. La base de datos procesa la solicitud modificada y devuelve los resultados enmascarados a Dynamic Data Masking. A continuación, Dynamic Data Masking envía los resultados a MDM Hub.

Puede utilizar Dynamic Data Masking para enmascarar datos de tipos específicos de solicitudes para bases de datos, o puede restringir el acceso a los datos de determinados grupos dentro de una organización. Por ejemplo, puede crear una regla para aplicar una función de enmascaramiento a los números de tarjetas de crédito cuando la solicitud para la base de datos proceda de un miembro del equipo de asistencia. Cuando Dynamic Data Masking reenvía los datos a MDM Hub, el miembro del equipo de asistencia ve los números enmascarados en vez de ver los números reales de las tarjetas de crédito.

Nota: Para utilizar Dynamic Data Masking en MDM Hub, debe tener instalados Dynamic Data Masking 9.6.0 y la revisión de error de emergencia 14590. Las versiones anteriores de Dynamic Data Masking no son compatibles con MDM Hub.

Para obtener más información sobre Dynamic Data Masking, consulte la documentación de Dynamic Data Masking.

Administrador de acceso de seguridad

El Administrador de acceso de seguridad es el módulo de seguridad para MDM Hub. El Administrador de acceso de seguridad protege los recursos de MDM Hub frente al acceso no autorizado.

El Administrador de acceso de seguridad aplica las directivas de seguridad de su organización en su implementación de MDM Hub. El Administrador de acceso de seguridad administra la autenticación y la autorización de los usuarios según su configuración de seguridad.

Nota: Puede utilizar el Administrador de acceso de seguridad para configurar el acceso de los usuarios a los recursos de MDM Hub desde aplicaciones de terceros. Sin embargo, no es posible configurar la seguridad para las herramientas de la Consola del concentrador mediante el Administrador de acceso de seguridad. La Consola del concentrador autentica a los usuarios y autoriza el acceso de los usuarios a los recursos y las herramientas de la Consola del concentrador mediante un mecanismo de seguridad independiente.

Autenticación

La autenticación es el proceso de comprobar la identidad de un usuario.

MDM Hub autentica a los usuarios según las credenciales que hayan proporcionado, como un nombre de usuario y una contraseña, o datos binarios sin procesar en una carga de seguridad.

MDM Hub utiliza los siguientes tipos de autenticación:

Interno

Autentica a los usuarios en MDM Hub, donde el usuario inicia sesión con un nombre de usuario y una contraseña.

Directorio externo

Autentica a los usuarios a través de un directorio de usuarios externo, compatible de forma nativa con los servidores de directorios preparados para LDAP, con Microsoft Active Directory y con Kerberos.

Proveedores de autenticación externos

Autentica a los usuarios a través de proveedores de autenticación de otros fabricantes.

Las implementaciones de MDM Hub pueden usar un tipo de autenticación de forma exclusiva o bien una combinación de tipos de autenticación. El tipo de autenticación que se usará depende de cómo configure la seguridad.

Autorización

La autorización es el proceso de determinar si un usuario tiene privilegios suficientes para acceder al recurso de MDM Hub solicitado.

En MDM Hub, se puede utilizar la autorización interna y externa:

Interno

Autoriza mediante MDM Hub. MDM Hub examina los privilegios de las funciones asignadas a la cuenta del usuario para determinar si puede acceder a los recursos seguros.

Externa

Autoriza a través de proveedores de autorización de otros fabricantes.

Puede configurar MDM Hub para que utilice uno de los dos tipos de autorización, o bien para que utilice ambos tipos de autorización.

Recursos seguros y privilegios

Puede configurar varios recursos de MDM Hub como recursos seguros.

Los siguientes recursos son configurables:

- Objetos base
- Asignaciones
- Paquetes
- Funciones de limpieza
- Conjuntos de reglas de coincidencia
- Metadatos
- Perfiles
- Tabla de usuarios

Puede conceder acceso a los recursos de MDM Hub según los privilegios. MDM Hub puede asignar los siguientes privilegios:

- Lectura
- Crear
- Actualizar
- Fusión
- Ejecución

- Eliminar

Los recursos pueden ser privados o seguros. De forma predeterminada, los recursos son seguros. MDM Hub solo puede conceder privilegios para recursos seguros.

Cuando se configura la seguridad en MDM Hub, tenga en cuenta lo siguiente:

- Un recurso específico está configurado para ser seguro.
- Una función específica está configurada para tener acceso a uno o más recursos seguros.
- Cada recurso seguro puede configurarse con privilegios específicos, como lectura o escritura, que definen el acceso al recurso seguro para esa función.

Para ejecutar una solicitud del Marco de servicios de integración, el usuario que ha iniciado sesión debe tener una función con los privilegios necesarios para acceder al recurso implicado en la solicitud.

Funciones

Una función representa un conjunto de privilegios para acceder a recursos seguros de MDM Hub. Puede asignar una función a un usuario para que este obtenga los privilegios.

Puede utilizar la herramienta Funciones en el entorno de trabajo Administrador de acceso de seguridad para asignar funciones a usuarios y grupos de usuarios. Las funciones asignadas a un usuario o grupo de usuarios determinan los privilegios de recurso de un usuario o grupo de usuarios. Los privilegios no se pueden asignar a los usuarios directamente.

Administrador de acceso de seguridad aplica la autorización de recursos de las solicitudes de usuarios de aplicaciones externas. Los administradores y los gestores de datos que utilizan la Consola del concentrador para acceder a los recursos de MDM Hub no se ven afectados en la misma medida por los privilegios de recursos.

Escenarios de implementación de seguridad

La seguridad en las implementaciones de MDM Hub se puede configurar de varias maneras.

Un punto de decisión de directiva es un punto de comprobación de seguridad específico que determina la identidad de los usuarios en tiempo de ejecución. Esto se denomina autenticación. Un punto de decisión de directiva también confirma a qué recursos de MDM Hub pueden acceder los usuarios. Esto se denomina autorización. El grado con que los puntos de decisión de directiva son gestionados internamente por MDM Hub, o externamente por proveedores de seguridad de terceros u otros servicios de seguridad, depende de la implementación de MDM Hub.

Los siguientes escenarios son ejemplos a grandes rasgos de cómo configurar la seguridad en implementaciones de MDM Hub:

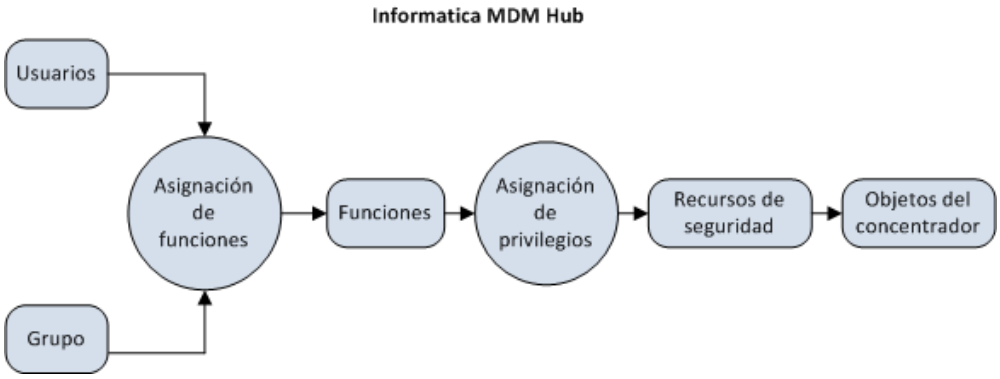
- Puntos de decisión de directiva solamente internos
- Directorio de usuarios externo
- Puntos de decisión de directiva centralizados basados en funciones
- Puntos de decisión de directiva centralizados exhaustivos

Nota: MDM Hub no refleja los cambios en los privilegios de recursos realizados en un proveedor de seguridad externo. Si realiza cambios en los privilegios de recursos mediante un proveedor de seguridad externo, utilice otro medio para sincronizar los cambios con MDM Hub.

Punto de decisión de directiva interno

MDM Hub puede administrar todas las decisiones de directiva de forma interna.

La siguiente imagen muestra una implementación de seguridad en la que MDM Hub administra todas las decisiones de directiva de forma interna:



En este escenario, MDM Hub realiza todas las decisiones de directiva en función de cómo están configurados los usuarios, grupos, funciones, privilegios y funciones mediante la Consola del concentrador.

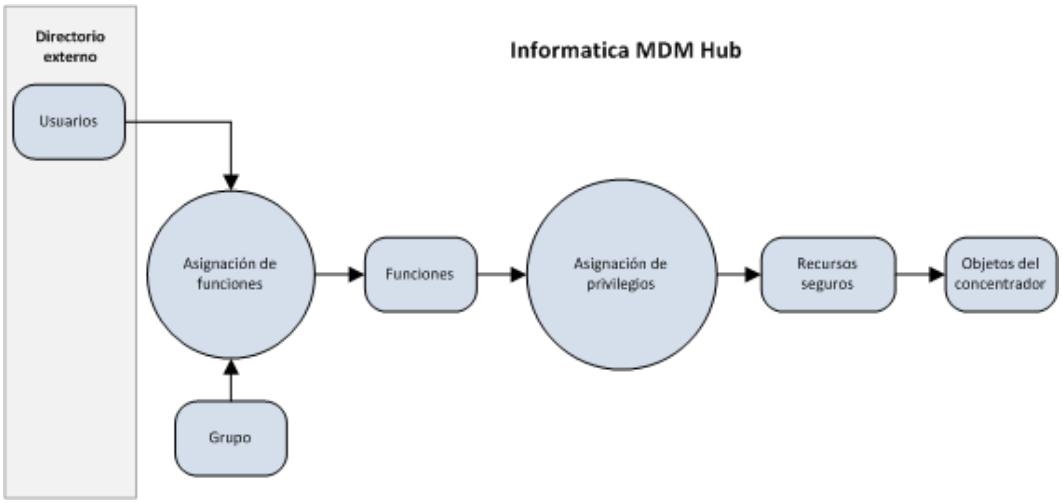
Directorio de usuarios externo

MDM Hub puede integrarse con un directorio de usuarios externo.

No obstante, los usuarios o grupos de usuarios que se mantienen en el directorio de usuarios externo han de estar registrados en MDM Hub. El registro es obligatorio para que MDM Hub pueda asignar funciones, y sus privilegios asociados, a estos usuarios y grupos.

Asigne usuarios del directorio externo a grupos en MDM Hub. Es necesario conservar las relaciones entre los usuarios y los grupos en MDM Hub, incluso cuando también se mantienen mediante el Protocolo ligero de acceso a directorios (LDAP).

La siguiente imagen muestra una implementación de seguridad donde se administran usuarios en un directorio externo, pero se administran los grupos, la asignación de funciones y la asignación de privilegios en MDM Hub.

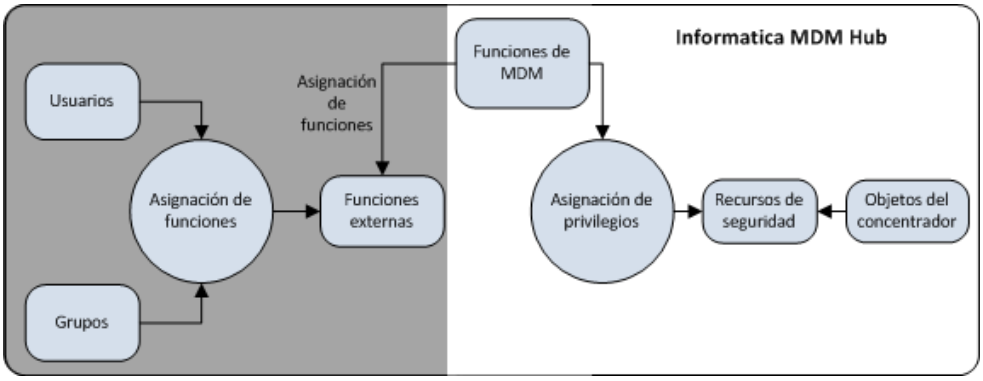


En este escenario, el directorio de usuarios externo administra las cuentas de usuario, los grupos y los perfiles de usuario. El directorio de usuarios externo puede autenticar a los usuarios y proporcionar información a MDM Hub sobre la pertenencia a grupos y los perfiles de usuario.

Decisión de directiva centralizada basada en funciones

MDM Hub puede administrar algunas decisiones de directiva internamente y recibir asignaciones de funciones externas.

La siguiente imagen muestra una implementación de seguridad donde la asignación de funciones, además de las cuentas de usuario, grupos y perfiles de usuario, se realizan de forma externa a MDM Hub:



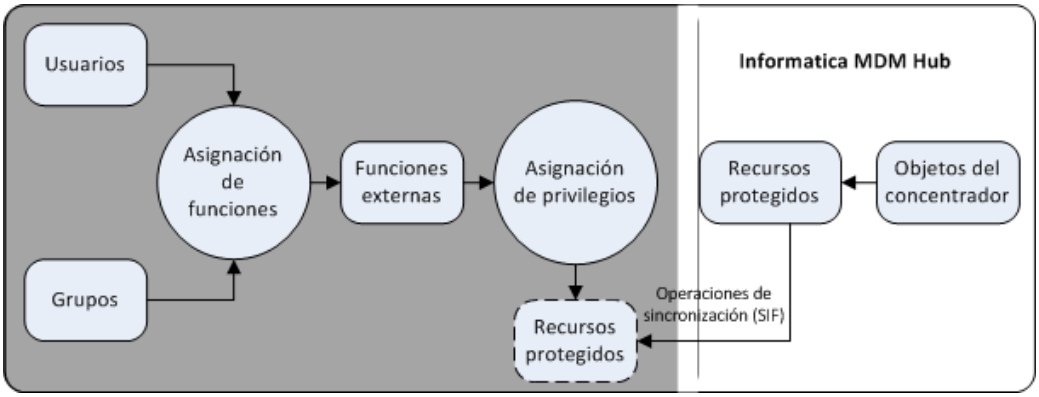
En este escenario, las funciones externas se asignan de forma explícita a las funciones de MDM Hub.

Decisión de directiva centralizada exhaustiva

MDM Hub puede controlar recursos protegidos internamente, pero aceptar funciones y privilegios asignados desde un directorio externo.

La siguiente imagen muestra una implementación de seguridad en la que la definición de las funciones y la asignación de los privilegios se producen de forma externa a MDM Hub. La figura muestra también que las

cuentas de usuario, grupos, perfiles de usuario y asignación de funciones se realizan de forma externa a MDM Hub:



En este escenario, MDM Hub simplemente expone los recursos protegidos mediante proxies externos, que se sincronizan con los recursos protegidos internamente mediante solicitudes de Marco de servicios de integración. Todas las decisiones de directiva son externas a MDM Hub.

Tareas de configuración de escenarios de seguridad

En la siguiente tabla se muestran las tareas de configuración de seguridad que corresponden a cada uno de los escenarios de implementación de seguridad. Si una celda indica "Sí", la tarea asociada se produce dentro de MDM Hub. Si una celda indica "No", la tarea asociada se produce de forma externa a MDM Hub.

Servicio / Tarea	Puntos de decisión de directiva internos	Directorio de usuarios externo	Puntos de decisión de directiva centralizados RoleNobased	Puntos de decisión de directiva centralizados exhaustivos
Configurar usuarios de MDM Hub	Sí	Sí	No	No
Utilizar autenticación externa	No	Sí	No	No
Asignar usuarios a la base de datos actual del Almacén de referencias operativas	Sí	Sí	No	No
Administrar la directiva de contraseñas global	Sí	No	No	No
Configurar grupos de usuarios	Sí	Sí	No	No
Proteger recursos de MDM Hub	Sí	Sí	Sí	Sí
Establecer el estado de un recurso de MDM Hub	Sí	Sí	Sí	Sí
Configurar funciones	Sí	Sí	Sí	No
Asignar funciones internas a funciones externas	No	No	Sí	No

Servicio / Tarea	Puntos de decisión de directiva internos	Directorio de usuarios externo	Puntos de decisión de directiva centralizados RoleNobased	Puntos de decisión de directiva centralizados exhaustivos
Asignar privilegios de recurso a funciones	Sí	Sí	Sí	No
Administrar proveedores de seguridad	No	Sí	Sí	Sí
Asignar funciones a usuarios y a grupos de usuarios	Sí	Sí	No	No

Nota: Si utiliza proveedores de seguridad de otros fabricantes para gestionar cualquier parte de la seguridad de su implementación de MDM Hub, consulte las instrucciones de configuración de dicho proveedor.

Deshabilitar el usuario administrativo predeterminado

Puede deshabilitar la cuenta de usuario administrativo predeterminado para evitar cualquier autenticación externa para fines de seguridad. Como resultado, los usuarios externos no pueden usar esta cuenta para acceder al sistema de MDM. Debe crear y configurar un usuario administrativo no predeterminado en MDM Hub.

1. Cree un usuario administrativo en MDM Hub. Vaya a **Usuarios > Agregar usuario > Nuevo**, cree esta nueva cuenta de usuario y active la casilla de verificación **Habilitar administrador**.
2. Asigne el usuario al ORS registrado. Use la pestaña **Base de datos de destino** si quiere asignarla a varios ORS.
3. Para deshabilitar la cuenta de usuario administrativo predeterminada, conecte la base de datos principal de MDM Hub y ejecute el siguiente comando:

   ```
   update c_repos_user set user_enabled_ind = 0 where rowid_user = 'INST.0 ' ;
   commit;
   ```

4. Asigne este usuario para que sea utilizado por el **servicio de identidad** en la consola de ActiveVOS.
   a. Vaya a la carpeta `<directorio de instalación de MDM Hub>/hub/server/bin`.
   b. Abra el archivo `build.properties`.
   c. Agregue la siguiente propiedad para el nombre de usuario que creó: `mdm.identity.user=<nombre de usuario>`.
   d. Guarde el archivo.
5. Abra una línea de comandos y ejecute el siguiente script:
   - En Windows. `<directorio de instalación de MDM Hub>\hub\server\postInstallSetup.bat`
   - En UNIX. `<directorio de instalación de MDM Hub>/hub/server/postInstallSetup.sh`
6. Reinicie el servidor de aplicaciones.
7. Inicie sesión en la consola de ActiveVOS y actualice la contraseña para este nuevo usuario, agregado al **servicio de identidad**.
   a. En la pestaña **Administración**, vaya a **Configurar servicios > Servicio de identidad**.

b. En la pestaña **Conexión**, en la sección **Configuración de conexión**, especifique y confirme la nueva contraseña.

c. Haga clic en **Actualizar**.

Cuando instale un HotFix, la configuración `mdm.identity.user=<nombre de usuario>` se eliminará del campo `build.properties` automáticamente. Debe agregar esta propiedad manualmente. Abra el campo `build.properties`, agregue la propiedad y guarde el archivo. Ejecute el script `postInstallSetup`. Reinicie el servidor de aplicaciones.

CAPÍTULO 2

Recursos

Este capítulo incluye los siguientes temas:

Resumen de los recursos

La Consola del concentrador permite exponer u ocultar recursos de MDM Hub a las aplicaciones externas.

Un recurso seguro es un recurso de MDM Hub protegido que se muestra a la herramienta Funciones, que permite añadir el recurso a funciones con privilegios específicos. Un grupo de recursos es un conjunto de recursos seguros que simplifica la asignación de privilegios. Con la herramienta Recursos seguros puede definir grupos de recursos y crear una jerarquía de recursos.

Puede configurar los siguientes recursos de MDM Hub como recursos seguros:

Objeto base

El usuario tiene acceso a todos los objetos base, las columnas y los metadatos de contenido seguros.

Función de limpieza

El usuario puede ejecutar todas las funciones de limpieza de seguridad.

Perfil de Administrador de jerarquía

El usuario tiene acceso a todos los perfiles del Administrador de jerarquía seguros.

Servicios de entidad de negocio

El usuario tiene acceso a todos los servicios de entidad de negocio seguros.

Asignación

El usuario tiene acceso a todas las asignaciones seguras y sus columnas.

Paquete

El usuario tiene acceso a todos los paquetes seguros y sus columnas.

Paquete remoto

El usuario tiene acceso a todos los paquetes remotos seguros.

Los grupos por lotes son seguros de forma predeterminada. No puede cambiar el estado de los grupos por lotes a privado. El grupo por lotes tiene privilegios de lectura y ejecución.

Además, puede utilizar la Consola del concentrador para proteger otros recursos a los que tengan acceso las solicitudes de SIF, incluidos los metadatos, los conjuntos de reglas de coincidencia, la tabla de auditoría y la tabla de usuarios.

Nota: Si utiliza Informatica Data Director, puede utilizar los métodos HTTP GET o POST para acceder al servidor del concentrador. Otros métodos HTTP, tales como DELETE o PUT, devuelven un error HTTP.

Recursos seguros y privados

Puede configurar un recurso de MDM Hub protegido como seguro o privado.

Seguro

Muestra el recurso de MDM Hub a la herramienta Funciones, lo que permite añadir el recurso a funciones con privilegios específicos. Cuando asigna una función específica a un usuario, el usuario puede usar solicitudes de SIF para acceder a los recursos seguros según los privilegios asociados con la función. De forma predeterminada, MDM Hub designa los recursos nuevos, como un objeto base, como seguros.

Privado

Oculta el recurso de MDM Hub a la herramienta Funciones. Impide que las solicitudes de SIF tengan acceso al recurso.

Un recurso debe ser seguro antes de que las aplicaciones externas puedan utilizar solicitudes de SIF para acceder a un recurso de MDM Hub.

Es posible que no desee exponer ciertos recursos de MDM Hub a aplicaciones externas. Por ejemplo, si su implementación de MDM Hub tiene asignaciones o paquetes que solo se utilizan en tareas por lotes (no en solicitudes de SIF), podría desear que fueran privados.

Nota: MDM Hub no considera las columnas de un paquete como recursos seguros. Las columnas de un paquete heredan el estado seguro y los privilegios de las columnas del objeto base principal. Si las columnas del paquete se basan en columnas de la tabla del sistema, no es necesario configurar la seguridad para ellas, ya que de forma predeterminada se puede acceder a ellas.

Grupos de recursos

Un grupo de recursos es una recopilación lógica de recursos seguros.

Puede utilizar la herramienta Recursos seguros para definir grupos de recursos y, a continuación, asignarles recursos relacionados. Los grupos de recursos simplifican la asignación de privilegios, y permiten asignar privilegios a varios recursos y asignar grupos de recursos a una función.

Para simplificar la administración, considere la posibilidad de crear los siguientes tipos de grupos de recursos:

- Defina un grupo de recursos ALL_RESOURCES que contenga todos los recursos seguros para poder establecer los privilegios mínimos a nivel global.
- Defina grupos de recursos por tipo de recurso de modo que pueda establecer privilegios mínimos para esos tipos de recursos.
- Defina grupos de recursos por área funcional, como TRAINING_RESOURCES, por ejemplo.
- Defina un grupo de recursos comodín que luego pueda asignar a muchas funciones diferentes que tengan privilegios similares.

Jerarquías de grupos de recursos

Un grupo de recursos también puede contener otros grupos de recursos, excepto un grupo de recursos al que pertenezca. Esto significa que puede crear una jerarquía de grupos de recursos y simplificar la administración de una gran recopilación de recursos.

Recursos seguros

Solo los recursos seguros pueden pertenecer a grupos de recursos. Los recursos privados no pueden pertenecer a grupos de recursos.

Si cambia el estado de un recurso a privado, entonces MDM Hub quita el recurso de todos los grupos de recursos a los que pertenezca. Cuando establece el estado de un recurso a seguro, MDM Hub añade el recurso al grupo de recursos correspondiente.

Herramienta Recursos seguros

Utilice la herramienta Recursos seguros en la Consola del concentrador para administrar la seguridad de los recursos de MDM Hub en detalle, incluido establecer el estado de un recurso de MDM Hub como seguro o privado. También puede usar los grupos de recursos para configurar una jerarquía de recursos.

La herramienta Recursos seguros contiene las siguientes fichas:

Recursos

Se usa para establecer el estado de recursos de MDM Hub individuales como seguro o privado. MDM Hub presenta los recursos como una jerarquía que muestra las relaciones entre los recursos. Los recursos globales aparecen en la parte superior de la jerarquía.

Grupos de recursos

Se utiliza para configurar los grupos de recursos.

Puede utilizar la herramienta Recursos seguros para exponer u ocultar los recursos en la herramienta Funciones y en las solicitudes de SIF. Debe conectarse a un Almacén de referencias operativas antes de usar la herramienta.

Configuración de recursos seguros

Para buscar y configurar recursos de MDM Hub, utilice la ficha Recursos de la herramienta Recursos seguros.

Configurar el estado de un recurso de MDM Hub

Puede configurar el estado de un recurso como seguro o privado para cualquier recurso de MDM Hub.

Nota: Esta configuración de estado no se aplica a los grupos de recursos, que solo contienen recursos seguros, ni a los recursos globales.

1. Inicie la herramienta Recursos seguros.
2. Adquiera un bloqueo de escritura.
3. En la ficha Recursos, desplácese por el árbol Recursos para encontrar los recursos que desee configurar.
4. Haga doble clic en el nombre del recurso para alternar entre seguro y privado. Para cambiar el estado de varios recursos al mismo tiempo, realice los pasos 5 y 6.
5. Seleccione los recursos que requieren un cambio de estado. Puede seleccionar varios recursos si lo desea.
6. Actualice el estado de los recursos seleccionados.
   - Haga clic en el botón **Seguro** para cambiar el estado de los recursos seleccionados a seguro.
   - Haga clic en el botón **Privado** para cambiar el estado de los recursos seleccionados a privado.
7. Haga clic en el botón **Guardar** para guardar los cambios.

Filtrar recursos

Para simplificar el cambio de estado de un conjunto de recursos de MDM Hub, puede especificar un filtro que solamente muestre los recursos que desee cambiar.

1. Inicie la herramienta Recursos seguros.
2. Adquiera un bloqueo de escritura.
3. Haga clic en el botón **Filtrar recursos**.

   La herramienta Recursos seguros muestra el cuadro de diálogo Filtro de recursos.
4. Seleccione los tipos de recursos.
   - Seleccione los tipos de recursos que desee incluir en el filtro.
   - Borre los tipos de recursos que desee excluir en el filtro.
5. Haga clic en **Aceptar**.

   La herramienta Recursos seguros muestra el árbol Recursos filtrado.

Configuración de los grupos de recursos

Con la herramienta Recursos seguros puede definir grupos de recursos y crear una jerarquía de recursos. Después, puede utilizar la herramienta Funciones para asignar privilegios a varios recursos en una sola operación.

La herramienta Recursos seguros diferencia visualmente los recursos que pertenecen al grupo de recursos actual directamente de los recursos que lo hacen indirectamente. Los recursos que se añaden de forma explícita a un grupo de recursos son miembros directos. Los recursos que pertenecen a un grupo de recursos que se ha añadido a otro grupo de recursos son miembros indirectos.

Por ejemplo, supongamos que desea tener dos grupos de recursos:

- El Grupo de recursos A contiene el objeto base Cliente, lo que significa que el objeto base Cliente es un miembro directo del Grupo de recursos A.
- El Grupo de recursos B contiene el objeto base Dirección.
- El Grupo de recursos A contiene el Grupo de recursos B, lo que significa que el objeto base Dirección es un miembro indirecto del Grupo de recursos A.

En este ejemplo, el objeto base Dirección no está disponible cuando edita el Grupo de recursos A. Debe editar el Grupo de recursos B para modificar el objeto base Dirección.

Añadir grupos de recursos

Utilice la herramienta Recursos seguros para añadir un grupo de recursos a la lista de recursos.

1. Inicie la herramienta Recursos seguros.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Grupos de recursos**.

   La herramienta Recursos seguros mostrará la pestaña Grupo de recursos.
4. Haga clic en el botón **Añadir**.

   La herramienta Recursos seguros muestra el cuadro de diálogo Añadir recursos a grupo de recursos.
5. Escriba un nombre único y descriptivo para este grupo de recursos.
6. Haga clic en el signo más (+) si desea expandir la jerarquía de recursos.

   Cada recurso tiene una casilla que indica su pertenencia al grupo de recursos. Si selecciona un elemento primario, también se seleccionan todos los elementos secundarios. Por ejemplo, si selecciona el elemento Objetos base en el árbol, se seleccionan todos los objetos base y sus recursos secundarios.
7. Seleccione los recursos que desee asignar a este grupo de recursos.
8. Haga clic en **Aceptar**.

   La herramienta Recursos seguros añadirá el nuevo recurso al nodo Grupos de recursos.

Editar y eliminar grupos de recursos

Puede utilizar la herramienta Recursos seguros para editar o eliminar grupos de recursos.

1. Inicie la herramienta Recursos seguros.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Grupos de recursos**.

4. Seleccione el grupo de recursos cuyas propiedades desee editar o eliminar.
   - Haga clic en el botón **Editar** para editar un grupo de recursos.
   - Haga clic en el botón **Quitar** para eliminar un grupo de recursos.

   La herramienta Recursos seguros muestra el cuadro de diálogo Asignar recursos a grupo de recursos. O la herramienta Recursos seguros quita el recurso eliminado del nodo Grupos de recursos.
5. Edite el nombre del grupo de recursos.
6. Haga clic en el signo más (+) para expandir la jerarquía de recursos.
7. Seleccione la casilla de verificación **Mostrar solo los recursos seleccionados para este grupo de recursos**.
8. Seleccione los recursos que desee asignar a este grupo de recursos.
9. Borre los recursos que desee quitar de este grupo de recursos.
10. Haga clic en **Aceptar**.

Actualizar la lista de recursos

Después de añadir un recurso, puede actualizar la lista de recursos para que refleje los cambios.

Para actualizar la lista Recursos, elija **Actualizar** en el menú Recursos seguros.

La herramienta Recursos seguros actualizará la lista de recursos.

Actualizar otros cambios de seguridad

También puede cambiar el intervalo de actualización de todos los cambios de seguridad.

Para establecer el intervalo de actualización para los cambios de seguridad, establezca el siguiente parámetro en el archivo `cmxserver.properties`:

```
cmx.server.sam.cache.resources.refresh_interval
```

Nota: El intervalo de actualización predeterminado es 5 tics de reloj, a una velocidad de 60.000 milisegundos por tic de reloj, lo que equivale a 5 minutos.

Configuración de seguridad para servicios de entidad de negocio de Data Director

Los servicios de entidad de negocio son recursos seguros y solo las funciones de usuario con privilegios pueden acceder a ellos en Data Director.

Puede configurar los siguientes recursos de servicios de entidad de negocio en la consola de MDM Hub:

- Buscar-Reemplazar
- Importación de archivos
- Coincidencia ad hoc

Debe utilizar la herramienta Recurso seguro para configurar los servicios de entidad de negocio como recursos seguros. A continuación, puede utilizar la herramienta Funciones para asignar privilegios a funciones de usuario.

Configurar servicios de entidad de negocio como un recurso seguro

Utilice la herramienta Recursos seguros en el entorno de trabajo del Administrador de acceso de seguridad para configurar los recursos necesarios como un recurso seguro.

1. Inicie la herramienta Recursos seguros.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Recursos**.
4. Desplácese al árbol de recursos y expanda **Servicios de entidad de negocio**.
5. Haga doble clic en el nombre del recurso para alternar entre seguro y privado.
    a. Haga clic en el botón **Seguro** para cambiar el estado de los recursos seleccionados a seguro.
    b. Haga clic en el botón **Privado** para cambiar el estado de los recursos seleccionados a privado.
6. Haga clic en **Guardar**.

Asignar privilegios de función a servicios de entidad de negocio

Utilice la herramienta Funciones en el entorno de trabajo del Administrador de acceso de seguridad para asignar a servicios de entidad de negocio privilegios sobre funciones de usuario.

1. Inicie la herramienta Funciones.
2. Adquiera un bloqueo de escritura.
3. Desplácese por la lista de funciones y seleccione la función necesaria.
4. Haga clic en la ficha **Privilegios del recurso**.
5. Desplácese al árbol de recursos y expanda **Servicios de entidad de negocio**.
6. Seleccione el privilegio **Ejecutar** para cada recurso del servicio de entidad de negocio.
7. Haga clic en **Guardar**.

CAPÍTULO 3

Funciones

Este capítulo incluye los siguientes temas:

Resumen de las funciones

Una función es una recopilación de privilegios que se asignan a un usuario o grupo. Una función representa un conjunto de privilegios para acceder a recursos seguros de MDM Hub.

Para ver o manipular un recurso seguro de MDM Hub, los usuarios deben tener asignadas las funciones que les concedan los privilegios suficientes para acceder a dicho recurso. Las funciones determinan dónde puede acceder un usuario y qué tareas puede realizar en MDM Hub.

Las funciones de MDM Hub son altamente granulares y flexibles, lo que permite a los administradores implementar medidas de seguridad complejas en las directivas de seguridad de sus organizaciones. Algunos usuarios, como los administradores, pueden tener asignada una sola función con acceso a todo. Otros usuarios, como los gestores de datos, pueden tener asignada una función con privilegios restringidos de forma explícita.

Una función también puede tener asignadas otras funciones, heredando los privilegios de acceso configurados para esas funciones. Los privilegios son acumulativos; es decir, cuando se combinan funciones, sus privilegios también se combinan. Por ejemplo: imagínese que la Función A tiene privilegios de lectura para un objeto base Dirección, y que la Función B tiene los privilegios de creación y actualización para el mismo objeto. Si una cuenta de usuario tiene asignadas las funciones A y B, tendrá los privilegios de lectura, creación y actualización para el objeto base Dirección. Una cuenta de usuario hereda los privilegios configurados para todas las funciones que se le asignen.

Configuración de las funciones

Puede crear, editar y eliminar funciones en MDM Hub.

Nota: Si utiliza una implementación de seguridad centralizada exhaustiva, en la que los usuarios son autorizados de forma externa, no necesita configurar funciones.

Los privilegios de recursos varían según el nivel de acceso que necesiten los usuarios para realizar sus tareas. El procedimiento recomendado para los administradores es seguir el principio del menor privilegio. Asigne a los usuarios el nivel de privilegio más bajo con el que puedan realizar su trabajo.

Añadir funciones

Para configurar las funciones y asignar los privilegios de acceso a los recursos de MDM Hub, utilice la herramienta Funciones en el entorno de trabajo Administrador de acceso de seguridad.

Sugerencia: Evite los espacios en los nombres de las funciones. Los espacios pueden causar errores cuando MDM Hub se comunica con ActiveVOS.

1. Inicie la herramienta Funciones.
2. Adquiera un bloqueo de escritura.
3. Señale cualquier punto del panel de navegación, haga clic con el botón derecho y elija **Añadir función**.

   La herramienta Funciones abrirá el cuadro de diálogo Añadir función.
4. Escriba el nombre de la función.
5. Escriba una descripción opcional de la función.
6. Especifique un nombre externo, o alias, de la función.
7. Haga clic en **Aceptar**.

   La nueva función aparece en la lista de funciones.

Editar y eliminar funciones

Para editar o eliminar una función existente, utilice la herramienta Funciones en el entorno de trabajo Administrador de acceso de seguridad.

1. Inicie la herramienta Funciones.
2. Adquiera un bloqueo de escritura.
3. Desplácese por la lista de funciones y seleccione la función que desee editar.
   - Para cada propiedad que desee editar, haga clic en el botón **Editar** que aparece junto a ella y especifique el nuevo valor.
   - Señale cualquier punto del panel de navegación, haga clic con el botón derecho y elija **Eliminar función**. Haga clic en **Sí** cuando se le solicite confirmación.
4. Haga clic en el botón **Guardar** para guardar los cambios.

Privilegios

Con la autorización interna de MDM Hub, puede asignar privilegios a las funciones.

Puede asignar los siguientes privilegios a las funciones:

Lectura

El usuario puede ver, pero no modificar datos.

Crear

El usuario puede crear registros de datos en el Almacén del concentrador

Actualizar

El usuario puede actualizar registros de datos en el Almacén del concentrador.

Eliminar

El usuario puede eliminar registros de datos en el Almacén del concentrador.

Fusión

El usuario puede fusionar y anular la fusión de datos.

Ejecución

El usuario puede ejecutar funciones de limpieza y grupos por lotes.

Los privilegios determinan el acceso que tienen los usuarios de aplicaciones externas a los recursos de MDM Hub. Por ejemplo, puede configurar una función para que tenga privilegios de lectura, creación, actualización y fusión en determinados paquetes.

Nota: Cada privilegio es distinto y se debe asignar de forma explícita. Los privilegios no agregan otros privilegios. Por ejemplo, un usuario que tenga acceso para actualizar un recurso no tiene por qué tener acceso de lectura al recurso. Ambos privilegios deben asignarse de forma individual.

Cuando utilice la Consola del concentrador, los privilegios no se aplicarán, aunque la configuración continuará afectando al uso de la Consola del concentrador. Por ejemplo, los gestores de datos no pueden ver ningún paquete en el Administrador de fusión ni en el Administrador de datos, excepto aquellos para los que tienen privilegios de lectura. Para editar y guardar los cambios en los datos de un paquete específico, los gestores de datos deben tener privilegios de actualización y creación en ese paquete.

Si los gestores de datos no tienen privilegios de actualización o creación, no podrán modificar ningún dato en el Administrador de datos. De igual modo, un gestor de datos debe tener privilegios de fusión a fin de utilizar el Administrador de fusión para fusionar o anular la fusión de registros. Para obtener más información sobre las herramientas Administrador de fusión y Administrador de datos, consulte la *Guía del gestor de datos de Multidomain MDM*.

Funciones internas y funciones externas

En una implementación de seguridad centralizada basada en funciones, debe crear una asignación entre la función interna de MDM Hub y la función externa gestionada independientemente de MDM Hub.

El nombre de la función externa podría ser distinto del nombre de la función interna utilizada en un entorno de MDM Hub.

Los detalles de configuración dependen de la implementación de las asignaciones de funciones del proveedor de seguridad. Las funciones se asignan en un archivo de configuración. Puede asignar una función externa a más de una función interna.

Nota: Aunque las asignaciones suelen crearse en XML, no existe un formato predefinido para los archivos de configuración. No tienen por qué ser un archivo XML o siquiera un archivo. La asignación forma parte de la implementación personalizada del proveedor de autenticación o perfil de usuario. El objetivo de la asignación es llenar una lista de funciones de objeto de perfil de usuario con los ID de funciones internas.

Asignar privilegios de recurso a funciones

Puede utilizar la herramienta Funciones en el entorno de trabajo Administrador de acceso de seguridad para asignar y editar privilegios de recurso a funciones.

1. Inicie la herramienta Funciones.
2. Adquiera un bloqueo de escritura.
3. Examine la lista de funciones y seleccione la función a la que desee asignar privilegios de recurso.
4. Haga clic en la ficha **Privilegios del recurso**.
5. Expanda la jerarquía Recursos para mostrar los recursos seguros que quiera configurar para esta función.
6. Para cada recurso que desee configurar:
   - Seleccione todos los privilegios que desee conceder a esta función.
   - Anule la selección de los privilegios que desee quitar a esta función.
7. Haga clic en el botón **Guardar** para guardar los cambios.

Asignar funciones a otras funciones

Una función también pueden heredar otras funciones, excepto una función a la que ya pertenece. Por ejemplo, si asigna la función B a la función A, la función A hereda los privilegios de acceso de la función B.

1. Inicie la herramienta Funciones.
2. Adquiera un bloqueo de escritura.
3. Examine la lista de funciones y seleccione la función a la que desee asignar otras funciones.
4. Haga clic en la ficha **Funciones**.

   La herramienta Funciones muestra todas las funciones que pueden asignarse a la función seleccionada.
5. Seleccione todas las funciones que desee asignar a la función seleccionada.
6. Anule la selección de las funciones que desee quitar de esta función.
7. Haga clic en el botón **Guardar** para guardar los cambios.

Generar un informe de privilegios de recurso para funciones

Puede generar un informe que describa los privilegios de recurso concedidos a una función en concreto.

1. Inicie la herramienta Funciones.
2. Adquiera un bloqueo de escritura.
3. Desplácese por la lista de funciones y seleccione aquella para la que desee generar un informe.
4. Haga clic en la ficha **Informe**.
5. Haga clic en **Generar**.

   La herramienta Funciones genera el informe y lo muestra en la ficha Informes.

Guardar el informe generado como un archivo HTML

1. Haga clic en **Guardar**.

   La herramienta Funciones le pedirá que especifique la ubicación de destino del informe guardado.
2. Desplácese hasta la ubicación de destino.

3. Haga clic en **Guardar**.

   El Administrador de acceso de seguridad guarda el informe utilizando la siguiente convención de nomenclatura:

   <*ORS_Name*>-<*Role_Name*>-RolePrivilegeReport.html

   Donde:

   - *ORS_Name* es el nombre de la base de datos de destino.
   - *Role_Name* es la función asociada al informe generado.

   La herramienta Funciones guardará el informe actual como un archivo HTML en la ubicación de destino. En el futuro, podrá visualizar este informe en un navegador.

CAPÍTULO 4

Usuarios y grupos de usuarios

Este capítulo incluye los siguientes temas:

Resumen de los usuarios y los grupos de usuarios

Un usuario de MDM Hub es una persona que puede acceder a recursos de MDM Hub.

Las cuentas de usuario se definen en la Base de datos principal del Almacén del concentrador. Para ver una introducción a los usuarios de MDM Hub, consulte el *Guía de introducción a Multidomain MDM*.

Una cuenta de usuario obtiene acceso a los recursos de MDM Hub mediante las funciones que tiene asignadas, heredando los privilegios configurados para cada función.

Puede utilizar la herramienta Usuarios en el entorno de trabajo de configuración para configurar las cuentas de usuario para los usuarios de MDM Hub, así como para cambiar las contraseñas y habilitar la autenticación externa. Las aplicaciones externas con autorización suficiente también pueden registrar cuentas de usuario mediante solicitudes SIF, tal como se describe en la *Guía del marco de servicios de integración de Multidomain MDM*.

Configuración de los usuarios

Puede crear, editar y eliminar usuarios en MDM Hub.

En función de cómo se haya implementado la seguridad, su implementación de MDM Hub podría requerir la adición de usuarios a la Base de datos principal.

Debe configurar los usuarios en la Base de datos principal en los siguientes escenarios:

- Utiliza la autorización interna en MDM Hub.
- Utiliza la autorización externa con MDM Hub.

- Varios usuarios acceden a la Consola del concentrador utilizando cuentas distintas.

Aunque el mismo usuario vaya a acceder a más de un Almacén de referencias operativas asociado con la Base de datos principal, solo es necesario definirlo una vez.

Acceso de los usuarios a los recursos de MDM Hub

Los usuarios, incluidos los administradores y los gestores de datos, pueden acceder a recursos de MDM Hub de las siguientes maneras:

Aplicaciones de MDM

Los usuarios pueden interactuar con MDM Hub iniciando sesión en la Consola del concentrador y utilizando las herramientas a las que tienen acceso. También pueden utilizar IDD o la herramienta de aprovisionamiento para acceder a datos en objetos base y entidades empresariales.

Aplicaciones de terceros

Los usuarios pueden interactuar de forma indirecta con los datos de MDM Hub mediante aplicaciones de terceros que utilicen clases SIF. Estos usuarios nunca inician sesión en la Consola del concentrador. Inician sesión en MDM Hub utilizando aplicaciones que pueden invocar clases SIF. Estos usuarios se conocen como usuarios de aplicaciones externas. Para obtener más información acerca de los tipos de solicitudes SIF que pueden invocar los desarrolladores, consulte la *Guía del marco de servicios de integración de Multidomain MDM*.

Añadir cuentas de usuario

Utilice la herramienta Usuarios del entorno de trabajo del Administrador de acceso de seguridad para añadir una cuenta de usuario a MDM Hub.

1. Inicie la herramienta Usuarios.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Usuarios**.
4. Haga clic en el botón **Añadir usuario**.

   La herramienta Usuarios abrirá el cuadro de diálogo **Añadir usuario**.
5. Especifique un nombre de pila, un segundo nombre y un apellido para el usuario.
6. Escriba un nombre de usuario para el usuario.

   Nota: Los nombres de usuario no distinguen entre mayúsculas y minúsculas, y se almacenan como caracteres en minúscula.
7. Introduzca una dirección de correo electrónico válida para el usuario. MDM Hub envía la contraseña para esta cuenta de usuario a dicha dirección de correo electrónico.
8. Escriba la base de datos predeterminada para el usuario. Esta es la base de datos que se selecciona de forma predeterminada cuando el usuario inicia sesión en la Consola del concentrador.
9. Si la cuenta de usuario es para una aplicación, seleccione la casilla de verificación **Usuario de aplicación**.

   Nota: Los usuarios de aplicación se utilizan para la autenticación basada en certificados de solicitudes generadas por una aplicación de confianza en nombre del usuario.
10. Introduzca y compruebe una contraseña para el usuario.
11. Elija el tipo de autenticación.

- Seleccione la casilla de verificación **Utilizar autenticación externa** si su implementación de MDM Hub utiliza la autenticación a través de un proveedor de seguridad de otros fabricantes.
- Anule la selección de la casilla de verificación **Utilizar autenticación externa** si desea utilizar la autenticación interna de MDM Hub.

12. Busque un certificado público para el usuario. MDM Hub puede utilizar este certificado para la autenticación de solicitudes de usuario.

    Nota: Si la cuenta de usuario es para un usuario de aplicación, debe seleccionar un certificado.

13. Haga clic en **Aceptar**.

    La herramienta Usuarios añade al nuevo usuario a la lista de usuarios de la pestaña **Usuarios**.

Editar y eliminar cuentas de usuario

Puede utilizar la herramienta Usuarios en el entorno de trabajo del Administrador de acceso de seguridad para editar o quitar cuentas de usuario.

1. Inicie la herramienta Usuarios.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Usuarios**.
4. Si desea eliminar un usuario, seleccione la cuenta de usuario que desea quitar.
5. Haga clic en el botón **Eliminar**.

   La herramienta Usuarios le pedirá que confirme la eliminación.

6. Haga clic en **Sí** para confirmar la eliminación.

   La herramienta Usuarios quita la cuenta de usuario eliminada de la lista de usuarios.

7. Si desea editar un usuario, seleccione la cuenta de usuario que desea configurar.
8. Para cambiar un nombre, haga doble clic en la celda y escriba otro nombre.
9. Seleccione una base de datos de inicio de sesión y un servidor diferentes, si lo desea.
10. Seleccione la casilla de verificación **Administrador** para conceder al usuario acceso de administrador, lo que le permite tener acceso a todas las herramientas de la Consola del concentrador y a todas las bases de datos.
11. Seleccione la casilla de verificación **Habilitar** para activar esta cuenta de usuario y permitir que este usuario inicie sesión.

    Nota: Si utiliza la autenticación externa para un usuario, su cuenta de usuario no se puede deshabilitar mediante la Consola del concentrador.

12. Haga clic en el botón **Guardar**.

    La herramienta Usuarios guarda los cambios realizados en la cuenta de usuario.

Editar información de usuario complementaria

Puede utilizar MDM Hub para administrar la información complementaria de cada usuario, como una dirección de correo electrónico o números de teléfono. MDM Hub no requiere que especifique esta información. MDM Hub tampoco utiliza esta información de forma especial.

Nota: No puede cambiar la dirección de correo electrónico del usuario `administrador` en la consola del concentrador. Para cambiar la dirección de correo electrónico del usuario administrador, actualice la entrada de usuario administrador directamente en la tabla C_REPOS_USER en el esquema CMX_SYSTEM.

1. Inicie la herramienta Usuarios.

2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Usuarios**.
4. Seleccione el usuario cuyas propiedades desee editar.
5. Haga clic en el botón **Editar**.

   La herramienta Usuarios abre el cuadro de diálogo **Editar usuario**.
6. Especifique cualquiera de las propiedades del usuario, como el tratamiento, la dirección de correo electrónico o el mensaje de inicio de sesión. El mensaje de inicio de sesión es el mensaje que la Consola del concentrador muestra después de que este usuario inicie sesión.
7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Guardar** para guardar los cambios.

Cambiar la configuración de contraseñas para las cuentas de usuario

Puede cambiar la configuración de la contraseña de un usuario. Se mantiene la información más reciente acerca de la última contraseña y quién la cambió. El historial de contraseñas no está disponible.

1. Inicie la herramienta Usuarios.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Usuarios**.
4. Seleccione al usuario cuya contraseña desee cambiar.
5. Haga clic en el botón **Cambiar contraseña**.

   La herramienta Usuarios mostrará el cuadro de diálogo **Cambiar contraseña** para el usuario seleccionado.
6. Especifique y compruebe la nueva contraseña.
7. Elija el tipo de autenticación.
   - Seleccione la casilla de verificación **Utilizar autenticación externa** si su implementación de MDM Hub utiliza la autenticación a través de un proveedor de seguridad de otros fabricantes.
   - Anule la selección de la casilla de verificación **Utilizar autenticación externa** si desea utilizar la autenticación interna de MDM Hub.
8. Haga clic en **Aceptar**.

Configurar el acceso de los usuarios al Almacén de referencias operativas

Puede configurar el acceso de los usuarios a las bases de datos del Almacén de referencias operativas.

1. Inicie la herramienta Usuarios.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la ficha **Base de datos de destino**.

   La herramienta Usuarios abrirá la ficha Base de datos de destino.
4. Expanda los nodos de la base de datos para ver qué usuarios pueden acceder a esa base de datos.
5. Para cambiar las asignaciones de usuarios a una base de datos, haga clic con el botón derecho en el nombre de la base de datos y elija **Asignar usuario**.

La herramienta Usuarios abrirá el cuadro de diálogo **Asignar usuarios a base de datos**.

6. Seleccione los nombres de los usuarios que desee asignar a la base de datos seleccionada.
7. Borre los nombres de los usuarios que no desee asignar a la base de datos seleccionada.
8. Haga clic en **Aceptar**.

Configuración de la directiva de contraseña

Puede definir directivas globales de contraseñas para todos los usuarios. Para los usuarios individuales, configure directivas privadas de contraseñas que tengan prioridad sobre las directivas globales. Todas las contraseñas distinguen entre mayúsculas y minúsculas.

Nota: Si implementa MDM Hub en el servidor de aplicaciones JBoss con seguridad habilitada, asegúrese de que la contraseña que establece sea compatible con la directiva de contraseña de JBoss. La contraseña también debe respetar la directiva de contraseña global de MDM Hub. Esto es importante porque las contraseñas para la Consola del concentrador y para JBoss deben coincidir.

Valores de la directiva de contraseña

Puede especificar la configuración de la contraseña de los usuarios de MDM Hub.

MDM Hub le permite establecer las siguientes directivas de contraseña privada para los usuarios:

Longitud de contraseña

Longitud mínima y máxima de una contraseña en caracteres.

Caducidad de la contraseña

Especifica si una contraseña caduca o no, y el número de días durante el cual una contraseña es válida.

Seleccione la casilla de verificación **La contraseña caduca** para establecer un período de vencimiento para las contraseñas. Anule la selección de la casilla de verificación **La contraseña caduca** para establecer contraseñas que no caduquen.

Si selecciona la casilla de verificación **La contraseña caduca**, especifique el número de días tras el cual caducará la contraseña. El período de caducidad de contraseña mínimo que puede definir es `10`.

Configuración de inicio de sesión

Número de inicios de sesión de gracia y número máximo de inicios de sesión incorrectos.

Historial de contraseña

Número de veces que puede reutilizarse una contraseña.

Requisitos de contraseña

Seleccione la casilla de verificación **Validación de patrones de contraseña habilitada** para aplicar un patrón de contraseña. Puede especificar los siguientes criterios para el patrón de contraseña:

- Número mínimo de caracteres únicos
- La contraseña debe empezar por
- La contraseña debe contener
- La contraseña debe terminar con

Administrar la directiva de contraseña global

La directiva de contraseña global se aplica a aquellos usuarios que no tengan directivas de contraseña privadas especificadas.

1. Inicie la herramienta **Usuarios**.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la ficha **Directiva de contraseña global**.

   Aparece la ventana Directiva de contraseña global.
4. Especifique la configuración de la directiva de contraseña.
5. Haga clic en **Aceptar**.
6. Haga clic en el botón **Guardar** para guardar la configuración global.

Administrar directivas de contraseña privadas

Puede especificar una directiva de contraseña privada que reemplace la directiva de contraseña global de cualquier usuario.

Nota: El procedimiento recomendado para gestionar directivas de contraseña es asegurarse de que la mayoría de las contraseñas de usuario estén gestionadas por una directiva global en vez de muchas directivas privadas.

1. Inicie la herramienta Usuarios.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Usuarios**.
4. Seleccione el usuario para el que desea establecer la directiva de contraseña privada.
5. Haga clic en el botón **Administrar directiva de contraseña**.

   Aparecerá la ventana de **Directiva de contraseña privada** del usuario seleccionado.
6. Habilite la opción **Directiva de contraseña privada activada**.
7. Especifique la configuración de directiva de contraseña del usuario.
8. Haga clic en **Aceptar**.
9. Haga clic en el botón **Guardar** para guardar los cambios.

Configuración de seguridad de los orígenes de datos JDBC

En las implementaciones de MDM Hub, si un origen de datos JDBC utiliza la seguridad de servidor de aplicaciones, debe configurar los ajustes en el archivo cmxserver.properties.

Debe almacenar el nombre de usuario y la contraseña del servidor de aplicaciones para el origen de datos JDBC en el archivo cmxserver.properties. Las contraseñas no pueden aparecer como texto sin cifrar. Es necesario cifrar las contraseñas antes de guardarlas en el archivo cmxserver.properties.

Si desea más información sobre los orígenes de datos JDBC seguros, consulte la documentación del servidor de aplicaciones.

Nombres de usuario y contraseñas para un origen de datos JDBC seguro

Si desea configurar los nombres de usuario y las contraseñas para un origen de datos JDBC seguro en el archivo cmxserver.properties, utilice los siguientes parámetros:

```
databaseId.username=username
databaseId.password=encryptedPassword
```

siendo databaseId el identificador único del origen de datos JDBC.

ID de base de datos para tipos de conexión SID de Oracle

Para un tipo de conexión SID de Oracle, el tipo de databaseId consta de las siguientes cadenas:

```
<nombre de host de base de datos>-<Oracle SID>-<nombre de esquema>
```

Por ejemplo, para la siguiente configuración:

- `<nombre de host de base de datos>` = `localhost`
- `<Oracle SID>` = `MDMHUB`
- `<nombre de esquema>` = `Test_ORS`

las propiedades del nombre de usuario y de la contraseña serían:

```
localhost-MDMHUB-Test_ORS.username=weblogic
localhost-MDMHUB-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

ID de base de datos para tipos de conexión de servicio de Oracle

Para un tipo de conexión de servicio de Oracle, el tipo de databaseId consta de las siguientes cadenas:

```
<nombre de servicio>-<nombre de esquema>
```

Por ejemplo, para la siguiente configuración:

- `<nombre de servicio>` = `MDM_Service`
- `<nombre de esquema>` = `Test_ORS`

las propiedades del nombre de usuario y de la contraseña serían:

```
MDM_Service-Test_ORS.username=weblogic
MDM_Service-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

ID de base de datos para tipos de conexión IBM Db2

Para un tipo de conexión IBM Db2, el databaseId consta de las siguientes cadenas:

```
<nombre de host de base de datos>-<nombre de la base de datos>-<nombre de esquema>
```

Por ejemplo, para la siguiente configuración:

- `<nombre de host de base de datos>` = `localhost`
- `<nombre de la base de datos>` = `dsui2`
- `<nombre de esquema>` = `DS_UI2`

las propiedades del nombre de usuario y de la contraseña serían:

```
localhost-dsui2-DS_UI2.username=weblogic
localhost-dsui2-DS_UI2.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

ID de base de datos para tipos de conexión de Microsoft SQL Server

Para un tipo de conexión Microsoft SQL Server, el databaseId consta de las siguientes cadenas:

```
<nombre de host de base de datos>-<nombre de la base de datos>
```

Por ejemplo, para la siguiente configuración:

- `<nombre de host de base de datos>` = `localhost`
- `<nombre de la base de datos>` = `ds_ui1`

las propiedades del nombre de usuario y de la contraseña serían:

```
localhost-ds_ui1.username=weblogic
localhost-ds_ui1.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

ID de base de datos para la base de datos principal

Si desea asegurar el origen de datos JDBC que accede a la Base de datos principal, el `databaseId` es CMX_SYSTEM. En este caso, las propiedades serían:

```
CMX_SYSTEM.username=weblogic
CMX_SYSTEM.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Cifrado de contraseñas

Para generar una contraseña cifrada para un esquema de base de datos, utilice los siguientes comandos:

```
C:\>java -cp siperian-common.jar com.siperian.common.security.Blowfish password
Plaintext Password: password
Encrypted Password: 9C03B113CD8E4BBFD236C56D5FEA56EB
```

Configuración de grupos de usuarios

Un grupo de usuarios es un conjunto lógico de cuentas de usuario.

Los grupos de usuarios simplifican la administración de la seguridad. Por ejemplo, puede combinar usuarios de aplicaciones externas en un único grupo de usuarios, y luego conceder funciones de seguridad a todo el grupo en vez de a los usuarios de forma individual. Además de usuarios, los grupos de usuarios también pueden contener otros grupos de usuarios.

Utilice la ficha Grupos de la herramienta Usuarios y grupos en el entorno de trabajo Administrador de acceso de seguridad para configurar los grupos de usuarios.

Iniciar la herramienta Usuarios y grupos

Inicie la herramienta Usuarios y grupos en la Consola del concentrador.

1. En la Consola del concentrador, conéctese a un Almacén de referencias operativas, si todavía no lo ha hecho.

2. Expanda el entorno de trabajo de Administrador de acceso de seguridad y haga clic en **Usuarios y grupos**.

   La Consola del concentrador muestra la herramienta Usuarios y grupos.

   La herramienta Usuarios y grupos contiene las siguientes fichas:

   Grupos

   Se utiliza para definir grupos de usuarios y asignar usuarios a grupos de usuarios.

   Usuarios asignados a la base de datos

   Se utiliza para asociar cuentas de usuario a una base de datos.

   Asignar usuarios/grupos a una función

   Se utiliza para asociar usuarios y grupos de usuarios a funciones.

   Asignar funciones a usuario/grupo

   Se utiliza para asociar funciones a usuarios y grupos de usuarios.

Añadir grupos de usuarios

Puede utilizar la herramienta Usuarios y grupos en el entorno de trabajo del Administrador de acceso de seguridad para añadir grupos de usuarios.

1. Inicie la herramienta Usuarios y grupos.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la ficha **Grupos**.
4. Haga clic en el botón **Añadir**.

   La herramienta Usuarios y grupos abrirá el cuadro de diálogo **Añadir grupo de usuarios**.
5. Escriba un nombre descriptivo para el grupo de usuarios.
6. Si lo desea, puede escribir una descripción del grupo de usuarios.
7. Haga clic en **Aceptar**.

   La herramienta Usuarios y grupos añadirá el nuevo grupo de usuarios a la lista.

Editar y eliminar grupos de usuarios

También puede utilizar la herramienta Usuarios y grupos para editar o eliminar grupos de usuarios.

1. Inicie la herramienta Usuarios y grupos.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la ficha **Grupos**.
4. Desplácese por la lista de grupos de usuarios y seleccione el grupo de usuarios que desee editar.
5. Si desea quitar un grupo de usuarios, haga clic en el botón **Eliminar**.

   La herramienta de usuarios y grupos le pedirá que confirme la eliminación.
6. Haga clic en **Sí**.

   La herramienta de usuarios y grupos quita el grupo de usuarios que se ha eliminado de la lista.
7. Si desea editar un grupo de usuarios, haga clic en el botón **Editar** junto a cada propiedad que desee editar y especifique el nuevo valor.
8. Haga clic en el botón **Guardar** para guardar los cambios.

Asignar usuarios y grupos de usuarios a grupos de usuarios

Para asignar miembros a un grupo de usuarios:

1. Inicie la herramienta Usuarios y grupos.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la ficha **Grupo**.
4. Desplácese por la lista de grupos de usuarios y seleccione el grupo de usuarios que desee editar.
5. Haga clic con el botón derecho en el grupo de usuarios que acaba de crear y elija **Asignar usuarios y grupos**.

   La herramienta Usuarios y grupos abrirá el cuadro de diálogo **Asignar a grupo de usuarios**.
6. Seleccione los nombres de usuarios y grupos de usuarios que desee asignar al grupo de usuarios seleccionado.
7. Borre los nombres de los usuarios y grupos de usuarios que no desee asignar al grupo de usuarios seleccionado.
8. Haga clic en **Aceptar**.

Asignar usuarios a la base de datos de ORS actual

Para asignar usuarios a la base de datos actual de Almacén de referencias operativas:

1. Inicie la herramienta Usuarios y grupos.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Usuarios asignados a la base de datos**.
4. Haga clic en el botón **Asignar usuarios a la base de datos** para asignar usuarios a una base de datos de Almacén de referencias operativas.

   La herramienta Usuarios y grupos abrirá el cuadro de diálogo **Asignar usuarios a base de datos**.
5. Seleccione los nombres de los usuarios que desee asignar a la base de datos seleccionada del Almacén de referencias operativas.
6. Borre los nombres de los usuarios que no desee asignar a la base de datos seleccionada del Almacén de referencias operativas.
7. Haga clic en **Aceptar**.

Asociaciones entre funciones y usuarios y grupos de usuarios

Puede asociar funciones a usuarios y a grupos de usuarios. Con la herramienta **Usuarios y grupos** puede asociar funciones a usuarios de las siguientes maneras:

- Asignar usuarios y grupos de usuarios a funciones.
- Asignar funciones a usuarios y a grupos de usuarios.

Elija el modo más adecuado para su implementación.

Asignar usuarios y grupos de usuarios a funciones

Para asignar usuarios y grupos de usuarios a una función:

1. Inicie la herramienta Usuarios y grupos.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la pestaña **Asignar usuarios/grupos a función** .
4. Seleccione la función a la que desee asignar usuarios y grupos de usuarios.
5. Haga clic en el botón **Editar**.

   La herramienta Usuarios y grupos abrirá el cuadro de diálogo **Asignar usuarios a función**.
6. Seleccione los nombres de usuarios y grupos de usuarios que desee asignar a la función seleccionada.
7. Borre los nombres de los usuarios y grupos de usuarios que no desee asignar a la función seleccionada.
8. Haga clic en **Aceptar**.

Asignar funciones a usuarios y grupos de usuarios

Para asignar funciones a usuarios y a grupos de usuarios:

1. Inicie la herramienta Usuarios y grupos.
2. Adquiera un bloqueo de escritura.
3. Haga clic en la ficha **Asignar funciones a usuario/grupo**.
4. Seleccione el usuario o el grupo de usuarios al que desee asignar funciones.
5. Haga clic en el botón **Editar**.

   La herramienta Usuarios y grupos abrirá el cuadro de diálogo **Asignar funciones a usuario**.
6. Seleccione las funciones que desee asignar al usuario o al grupo de usuarios seleccionado.
7. Borre las funciones que no desee asignar al usuario o grupo de usuarios seleccionado.
8. Haga clic en **Aceptar**.

CAPÍTULO 5

Proveedores de seguridad

Este capítulo incluye los siguientes temas:

Resumen de los proveedores de seguridad

Un proveedor de seguridad es una aplicación de terceros que proporciona servicios de seguridad, como autenticación y autorización, a los usuarios que acceden a MDM Hub. Los proveedores de seguridad forman parte de algunos escenarios de implementación de seguridad de MDM Hub.

Un archivo de proveedor contiene información del perfil de un proveedor de seguridad. Si desea utilizar proveedores de seguridad de otros fabricantes, utilice la herramienta Proveedores de seguridad para cargar los archivos de proveedor en MDM Hub. También puede utilizar la herramienta Proveedores de seguridad para modificar, eliminar, habilitar o deshabilitar proveedores de seguridad en la lista Proveedores.

MDM Hub se proporciona con un conjunto de proveedores de seguridad internos predeterminados. También puede añadir proveedores de seguridad de otros fabricantes. Los proveedores de seguridad internos no se pueden eliminar.

Administración de los proveedores de seguridad

Los proveedores de seguridad se pueden administrar en la implementación de MDM Hub mediante la herramienta Proveedores de seguridad en el entorno de trabajo de configuración de la Consola del concentrador.

Puede añadir proveedores de seguridad del conjunto interno predeterminado de MDM Hub o de la selección de proveedores que haya añadido. Los proveedores de seguridad internos no se pueden eliminar.

MDM Hub admite los siguientes tipos de proveedores de seguridad:

Proveedor de autenticación

Autentica un usuario mediante la validación de su identidad. Informa a MDM Hub de que los usuarios son quienes dicen ser. Este tipo de proveedor de seguridad no valida si los usuarios tienen los privilegios necesarios para acceder a recursos específicos de MDM Hub.

Proveedor de autorización

Informa a MDM Hub de si los usuarios tienen los privilegios necesarios para acceder a recursos específicos de MDM Hub.

Proveedor de perfiles de usuario

Informa a MDM Hub sobre cada usuario, facilitando datos como sus atributos específicos y las funciones a las que pertenece.

Los proveedores internos representan las implementaciones internas de MDM Hub para los servicios de autenticación, autorización y perfil de usuario.

Algunos de los proveedores predeterminados de MDM Hub son superproveedores. Los superproveedores siempre devuelven una respuesta positiva a las solicitudes de autenticación y autorización. Utilice un superproveedor en un entorno de desarrollo cuando no desee configurar usuarios, funciones ni privilegios. Los superproveedores también se pueden utilizar en un entorno de producción en el que la seguridad se proporciona como una capa superior a las solicitudes de SIF para mejorar el rendimiento.

Administración de los archivos de proveedor

Un archivo de proveedor contiene información del perfil de un proveedor de seguridad.

Si desea utilizar sus propios proveedores de seguridad de otros fabricantes, debe registrarlos explícitamente mediante la herramienta Proveedores de seguridad. Para registrar un proveedor de seguridad, cargue un archivo de proveedor que contenga la información de perfil necesaria para el registro.

Un archivo de proveedor es un archivo JAR que contiene los siguientes datos:

- Un archivo manifest que describe uno o más proveedores de seguridad externos. Cada proveedor de seguridad tiene la siguiente configuración:
  - Nombre de proveedor
  - Descripción del proveedor
  - Tipo de proveedor
  - Nombre de clase de fábrica del proveedor
  - Propiedades que especifican detalles de configuración del proveedor. Puede ser una lista de pares nombre-valor: nombres de propiedad con valores predeterminados.
- La implementación del proveedor y las bibliotecas de otros fabricantes necesarias.

El InformaticaKit de recursos copia una implementación de ejemplo de un archivo de proveedor en el Servidor del concentrador. Para obtener más información sobre el archivo de proveedor de ejemplo, consulte la *Guía del kit de recursos de Multidomain MDM*.

Cargar un archivo de proveedor

Cargue un archivo de proveedor para añadir o actualizar información de un proveedor.

1. Inicie la herramienta Proveedores de seguridad.

2. Adquiera un bloqueo de escritura.
3. En el panel de navegación de la izquierda, haga clic con el botón derecho en Archivos de proveedores y elija **Cargar archivo de proveedores**.

   La herramienta Proveedor de seguridad solicita que seleccione el archivo JAR del proveedor.
4. Especifique el archivo JAR, puede desplazarse por el sistema de archivos si es necesario, y seleccione el archivo JAR que desea cargar.
5. Haga clic en **Abrir**.

   La herramienta Proveedor de seguridad comprueba el archivo seleccionado para determinar si es un archivo de proveedor válido.
6. Si el archivo de proveedor que carga tiene el mismo nombre que un archivo de proveedor existente, la herramienta Proveedor de seguridad le preguntará si desea sobrescribir el archivo de proveedor existente. Haga clic en **Sí** para confirmar.

   La herramienta Proveedor de seguridad rellena la lista Proveedores con la información adicional del proveedor. Una vez cargado el archivo de proveedor, puede eliminar el archivo original del sistema de archivos.

Eliminar un archivo de proveedores

Puede eliminar un archivo de proveedor si deja de utilizar el proveedor de seguridad.

1. Inicie la herramienta Proveedores de seguridad.
2. Adquiera un bloqueo de escritura.
3. En el panel de navegación izquierdo, haga clic con el botón derecho en el archivo de proveedores que desee eliminar y, después, elija **Eliminar archivo de proveedores**.

   La herramienta del proveedor de seguridad le pedirá que confirme la eliminación.
4. Haga clic en **Sí**.

   La herramienta del proveedor de seguridad quita de la lista el archivo de proveedores eliminado.

   Nota: No se pueden eliminar los archivos de proveedor internos que se proporcionan con MDM Hub.

Configuración de un proveedor de seguridad

La herramienta Proveedores de seguridad muestra una lista de los proveedores registrados.

La lista de proveedores registrados está ordenada por el tipo de proveedor. La secuencia de proveedores en la lista Proveedores también representa el orden en el que se invocan. Un usuario debe autenticarse en al menos un proveedor de la lista Proveedores.

Por ejemplo, cuando intenta iniciar sesión y facilita su nombre de usuario y contraseña, MDM Hub envía sus credenciales de inicio de sesión a todos los proveedores de autenticación en la lista de autenticación. MDM Hub procede de forma secuencial por la lista. Si la autenticación se realiza correctamente con uno de los proveedores de la lista, MDM Hub le autentica. Si la autenticación no se produce con ninguno de los proveedores de autenticación disponibles, no se le autentica.

Cambiar la configuración del proveedor de seguridad

Para cambiar la configuración de un proveedor de seguridad, realice los pasos siguientes:

1. Inicie la herramienta Proveedores de seguridad.
2. Adquiera un bloqueo de escritura.
3. Seleccione el proveedor de seguridad que desea modificar.
4. En el panel Propiedades, haga clic en el botón **Editar** junto a la configuración que desee modificar.
5. Haga clic en el botón **Guardar** para guardar los cambios.

Habilitar y deshabilitar proveedores de seguridad

1. Adquiera un bloqueo de escritura.
2. Seleccione el proveedor de seguridad que desee habilitar o deshabilitar.
   - Marque la casilla de verificación **Habilitado** para habilitar un proveedor de seguridad que esté deshabilitado.
   - Anule la selección de la casilla **Habilitado** para deshabilitar un proveedor de seguridad.

   Una vez deshabilitado, el nombre del proveedor no está disponible y se coloca al final de la lista Proveedores. No es posible reorganizar los proveedores deshabilitados en la lista Proveedores.
3. Haga clic en el botón **Guardar** para guardar los cambios.

Cambiar el orden de procesamiento de un proveedor de seguridad

MDM Hub procesa los proveedores de seguridad en el orden en el que aparecen en la lista Proveedores. Puede reorganizar el orden en el que aparecen los proveedores de seguridad.

1. Inicie la herramienta Proveedores de seguridad.
2. Adquiera un bloqueo de escritura.
3. Para mover un proveedor hacia arriba, haga clic con el botón derecho en el proveedor que desee mover y seleccione **Subir proveedor**.

   La herramienta Proveedor de seguridad coloca al proveedor delante del proveedor anterior en la lista Proveedores y, a continuación, actualiza el panel de navegación.
4. Para mover un proveedor hacia abajo, haga clic con el botón derecho en el proveedor que desee mover y seleccione **Bajar proveedor**.

   La herramienta Proveedor de seguridad coloca al proveedor debajo del proveedor anterior en la lista Proveedores y, a continuación, actualiza el panel de navegación.

Propiedades del proveedor

El panel del proveedor contiene los siguientes campos:

Nombre

El nombre del proveedor de seguridad.

Descripción

La descripción del proveedor de seguridad.

Tipo de proveedor

El tipo del proveedor de seguridad. El tipo puede ser uno de los siguientes valores:

- Autenticación
- Autorización
- Perfil de usuario

Archivo de proveedores

El nombre del archivo de proveedor asociado con el proveedor de seguridad, o el **proveedor interno** de proveedores internos.

Habilitado

Indica si el proveedor de seguridad está habilitado o no. Un proveedor de seguridad habilitado está seleccionado. Un proveedor de seguridad deshabilitado no está seleccionado. Tenga en cuenta que los proveedores internos no pueden estar deshabilitados.

Propiedades

Las propiedades adicionales de este proveedor de seguridad, si el proveedor de seguridad las ha definido. Cada propiedad es una pareja de valores de nombre. Un proveedor de seguridad puede necesitar o permitir propiedades únicas que puede especificar aquí.

Añadir propiedades del proveedor

Para añadir propiedades de proveedor, realice los siguientes pasos.

1. Inicie la herramienta Proveedores de seguridad.
2. Adquiera un bloqueo de escritura.
3. En el panel de navegación, seleccione el proveedor de autenticación al que desee añadir propiedades.
4. Haga clic en el botón **Añadir**.

   La herramienta Proveedores de seguridad abre el cuadro de diálogo Añadir propiedad del proveedor.
5. Especifique el nombre de la propiedad.
6. Especifique el valor que quiera asignar a esta propiedad.
7. Haga clic en **Aceptar**.

Editar propiedades de proveedores

Para editar una propiedad del proveedor existente, realice los siguientes pasos.

1. Inicie la herramienta Proveedores de seguridad.
2. Adquiera un bloqueo de escritura.
3. En el panel de navegación, seleccione el proveedor de autenticación cuyas propiedades desee editar.
4. Para cada propiedad que desee editar, haga clic en el botón **Editar** que aparece junto a ella y especifique el nuevo valor.
5. Haga clic en el botón **Guardar** para guardar los cambios.

Proveedores personalizados

Puede empaquetar clases de proveedores personalizados en el archivo JAR o ZIP que incluye el archivo de proveedor.

Especifique la configuración para los proveedores personalizados en el archivo `providers.properties`. A continuación, coloque el archivo dentro del archivo JAR del directorio META-INF. Luego, el cargador traduce la configuración a lo que aparece en la consola del concentrador.

Un archivo provider.properties tiene los siguientes elementos:

ProviderList

Lista de los nombres de los proveedores que contiene, separados por comas.

File-Description

Descripción del paquete.

XXX-Provider-Name

Nombre para mostrar del proveedor *XXX*.

XXX-Provider-Description

Descripción del proveedor *XXX*.

XXX-Provider-Type

Tipo del proveedor *XXX*. Los valores posibles son `USER_PROFILE_PROVIDER`, `JAAS_LOGIN_MODULE` y `AUTHORIZATION_PROVIDER`.

XXX-Provider-Factory-Class-Name

Clase de implementación del proveedor, que también se encuentra en el mismo archivo JAR o ZIP.

XXX-Provider-Properties

Lista separada por comas de pares de nombre/valor que definen las propiedades del proveedor.

Nota: El archivo de almacenamiento del proveedor debe contener todas las clases necesarias para que el proveedor personalizado funcione, además de los recursos necesarios. Estos recursos son específicos de su implementación.

Archivo providers.properties de ejemplo

Nota: Todos los valores son obligatorios excepto *XXX*-Provider-Properties.

```
ProviderList=ProviderOne,ProviderTwo,ProviderThree,ProviderFour
ProviderOne-Provider-Name: Sample Role Based User Profile Provider
ProviderOne-Provider-Description: Sample User Profile Provider for roled-based management
ProviderOne-Provider-Type: USER_PROFILE_PROVIDER
ProviderOne-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleRoleBasedUserProfileProviderFactory
ProviderOne-Provider-Properties: name1=value1,name2=value2
ProviderTwo-Provider-Name: Sample Login Module
ProviderTwo-Provider-Description: Sample Login Module
ProviderTwo-Provider-Type: JAAS_LOGIN_MODULE
ProviderTwo-Provider-Factory-Class-Name: com.siperian.sam.sample.authn.SampleLoginModule
ProviderTwo-Provider-Properties:
ProviderThree-Provider-Name: Sample Role Based Authorization Provider
ProviderThree-Provider-Description: Sample Role Based Authorization Provider
ProviderThree-Provider-Type: AUTHORIZATION_PROVIDER
ProviderThree-Provider-Factory-Class-Name:
com.siperian.sam.sample.authz.SampleAuthorizationProviderFactory
ProviderThree-Provider-Properties:
ProviderFour-Provider-Name: Sample Comprehensive User Profile Provider
```

```
ProviderFour-Provider-Description: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Type: USER_PROFILE_PROVIDER
ProviderFour-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleComprehensiveUserProfileProviderFactory
ProviderFour-Provider-Properties:
File-Description=The sample provider files
```

Autenticación externa

Puede utilizar la autenticación externa con MDM Hub para los usuarios a través del Servicio de autenticación y autorización de Java (JAAS).

MDM Hub proporciona plantillas para los siguientes tipos de estándares de autenticación:

- Protocolo ligero de acceso a directorios (LDAP)
- Microsoft Active Directory
- La autenticación de redes mediante el protocolo de Kerberos

Estas plantillas proporcionan la configuración (como protocolos, nombres de servidor y puertos) necesaria para estos estándares de autenticación. Puede utilizar estas plantillas para añadir un nuevo módulo de inicio de sesión con la configuración que necesite. Para obtener más información sobre estos estándares de autenticación, consulte la documentación del proveedor aplicable.

Añadir un módulo de inicio de sesión

Para configurar la autenticación externa en MDM Hub, debe crear un módulo de inicio de sesión.

1. Inicie la herramienta Proveedores de seguridad.
2. Adquiera un bloqueo de escritura.
3. Haga clic con el botón derecho en Proveedores de autenticación (módulos de inicio de sesión) y seleccione **Añadir módulo de inicio de sesión**.

   La herramienta Proveedores de seguridad abrirá el cuadro de diálogo Añadir módulo de inicio de sesión.
4. Haga clic en la flecha hacia abajo y seleccione una plantilla para el módulo de inicio de sesión.

   OpenLDAP-template

   Basada en las propiedades de la autenticación de LDAP.

   MicrosoftActiveDirectory-template

   Basada en las propiedades de la autenticación de Active Directory.

   Kerberos-template

   Basada en las propiedades de la autenticación de Kerberos.
5. Haga clic en **Aceptar**.

   La herramienta Proveedores de seguridad añadirá el módulo del inicio de sesión nuevo a la lista.
6. En el panel de propiedades, haga clic en el botón **Editar** junto a la propiedad que desee modificar. Especifique la configuración para el tipo de módulo de inicio de sesión que desee crear.
7. Haga clic en el botón **Guardar** para guardar los cambios.

Eliminar un módulo de inicio de sesión

Puede eliminar un módulo de inicio de sesión si lo desea.

1. Inicie la herramienta Proveedores de seguridad.
2. Adquiera un bloqueo de escritura.
3. En el panel de navegación, haga clic con el botón derecho en un módulo de inicio de sesión en Proveedores de autenticación (módulos de inicio de sesión) y elija **Eliminar módulo de inicio de sesión**.

   La herramienta del proveedor de seguridad le pedirá que confirme la eliminación.
4. Haga clic en **Sí**.

   La herramienta Proveedor de seguridad quita el módulo de inicio de sesión eliminado de la lista y actualiza el panel de navegación izquierdo.

CAPÍTULO 6

Seguridad a nivel de aplicación

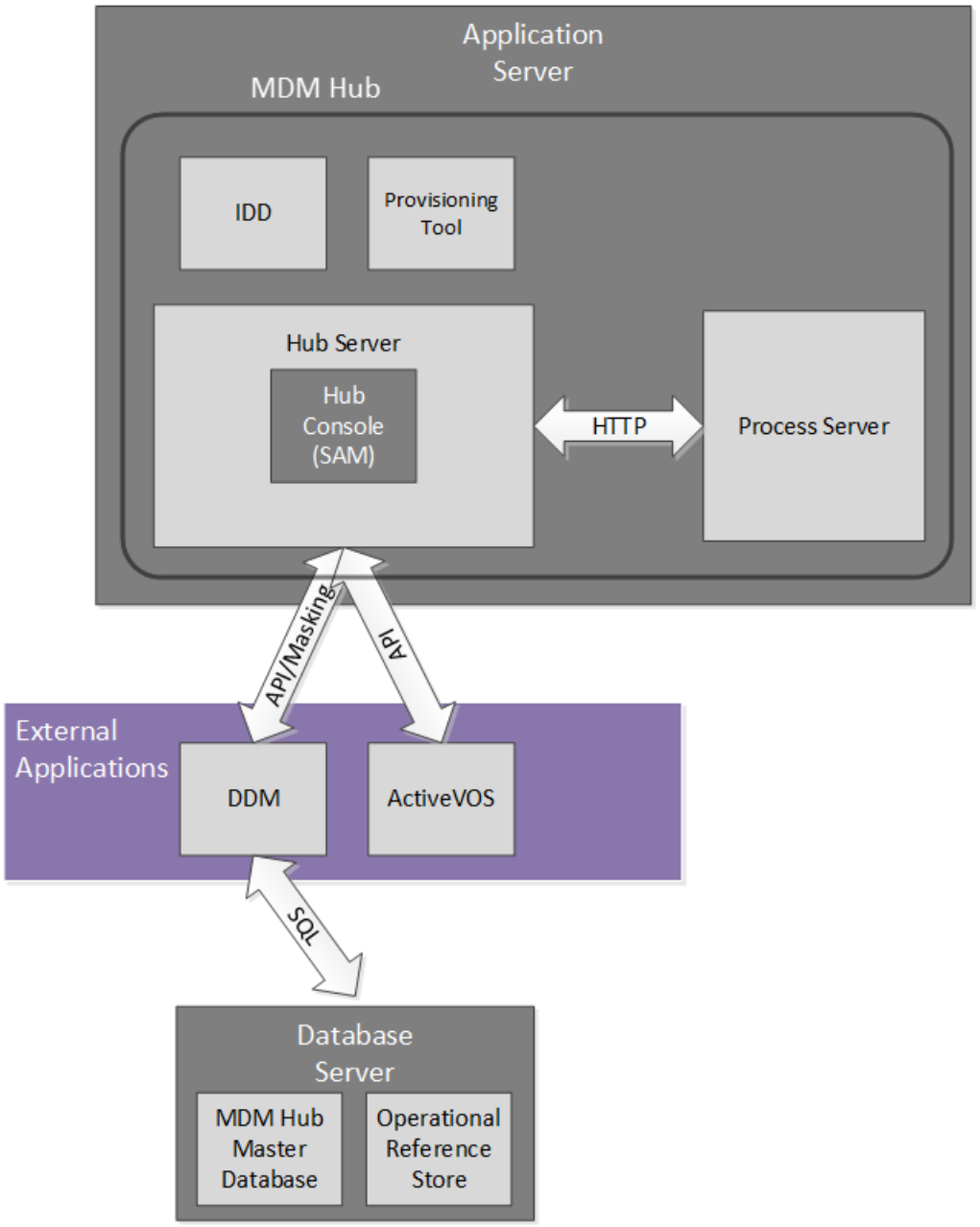
Este capítulo incluye los siguientes temas:

Resumen de seguridad a nivel de aplicación

El Administrador de acceso de seguridad (SAM) es el módulo de seguridad de MDM Hub, que controla las credenciales y las funciones de usuario. Las demás aplicaciones y los demás componentes de una implementación de MDM Hub también tienen configuración de seguridad para garantizar que la comunicación con MDM Hub se realiza de forma segura. Por ejemplo, puede configurar la seguridad a nivel de datos para Informatica Data Director.

Informatica realiza pruebas de seguridad internas en sus productos. Por ejemplo, Informatica utiliza aplicaciones de análisis estándares del sector para buscar vulnerabilidades de seguridad en los productos, como ataques de inyección de SQL. Otras aplicaciones de seguridad de Informatica, que se usan junto con el SAM, aportan una capa extra de seguridad a la implementación de MDM Hub. Informatica Dynamic Data Masking (DDM) aplica una máscara a los datos para evitar el acceso no autorizado a la información confidencial. La herramienta de aprovisionamiento de Informatica MDM e Informatica ActiveVOS no son aplicaciones de seguridad, pero se comunican de forma segura con MDM Hub.

La siguiente imagen muestra una implementación de MDM Hub de ejemplo y el modo en que los componentes están conectados entre sí:



Informatica Data Director

Informatica Data Director es una aplicación de control de datos basada en la web de MDM Hub. Cuando se configura una aplicación Data Director, los usuarios de negocio pueden crear, administrar, consumir y supervisar datos principales.

Informatica Data Director aplica las diez principales recomendaciones de seguridad de Open Web Application Security Project (Proyecto abierto de seguridad en aplicaciones Web, OWASP por sus siglas en inglés). Informatica usa IBM Security AppScan para buscar vulnerabilidades de seguridad, como ataques de

inyección de SQL. Los métodos de HTTP GET o POST pueden obtener información de IDD, pero otros métodos de HTTP, como DELETE o PUT, devuelven un error de HTTP.

Cuando configura una aplicación Data Director, puede organizar las tablas en el Almacén de referencias operativas en entidades de negocio o en áreas de asunto. Ambos métodos permiten agrupar los datos relacionados que desea tratar como una unidad, como por ejemplo todos los datos de un cliente. Las entidades de negocio son el método de organización recomendado, ya que las entidades de negocio de la versión 10.1 de Multidomain MDM forman la base del marco de Entidad 360, que incluye servicios de entidad de negocio y vistas de entidades modernas.

Para la seguridad de los datos, una aplicación Data Director utiliza las funciones de usuario y los privilegios de recursos que se establecen en el Almacén de referencias operativas. Recuerde que un administrador de MDM utiliza el entorno de trabajo del Administrador de acceso de seguridad en la Consola del concentrador para definir los privilegios de recursos de cada función de usuario. En una aplicación Data Director, los usuarios pueden realizar las operaciones que les permite su función de usuario.

Los privilegios de función para las entidades de negocio y las áreas de asunto se derivan de los privilegios de recursos de distintas formas, por lo que la seguridad puede ser ligeramente diferente. Sin embargo, ambos métodos son igualmente seguros. Para obtener más información sobre la seguridad en las entidades de negocio, consulte la *Guía de la herramienta de aprovisionamiento de Multidomain MDM*. Para obtener más información sobre la configuración de seguridad y la seguridad de los datos en las áreas de asunto, consulte la *Guía de implementación de Multidomain MDM Data Director*.

Herramienta de aprovisionamiento

Utilice la herramienta de aprovisionamiento para crear modelos de entidad de negocio basados en la información de esquema que ha definido en un almacén de referencias operativas (ORS, Operational Reference Store). El modelo de entidad de negocio es un componente fundacional del marco de Entidad 360 en Data Director.

Debe iniciar sesión en la herramienta de aprovisionamiento antes de configurar entidades de negocio.

A medida que se trabaja en los archivos de configuración, los cambios se guardan en un espacio de trabajo temporal. La herramienta de aprovisionamiento no aplicará los cambios hasta que se publiquen. Si varios usuarios modifican al mismo tiempo la configuración de las entidades de negocio de un ORS, MDM Hub se actualizará con la configuración que se haya publicado en último lugar.

La herramienta de aprovisionamiento se debe ejecutar en el mismo servidor de aplicaciones que el servidor del concentrador.

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

ActiveVOS

Informatica ActiveVOS® es una herramienta de administración de procesos de negocio (BPM) que le permite automatizar procesos de negocio. Puede crear modelos de proceso que integren personas, procesos y sistemas, lo que incrementa la eficiencia de su negocio.

Puede usar ActiveVOS para asegurarse de que los datos de la entidad actualizados pasen por un flujo de trabajo de aprobación de cambios antes de que los registros actualizados contribuyan a los registros de mejor versión de confianza (BVT, Best Version of the Truth). Por ejemplo, puede que un proceso de negocio

requiera que un administrador sénior revise y apruebe las actualizaciones en datos de clientes antes de que se conviertan en datos principales.

Para admitir un flujo de trabajo de aprobación de cambios, MDM Hub e Data Director se integran con el servidor de ActiveVOS. Los flujos de trabajo de MDM predefinidos, los tipos de tareas y las funciones permiten que los componentes se sincronicen entre sí. Puede configurar la implementación de MDM para que funcione con el servidor de ActiveVOS integrado. Por otro lado, puede ejecutar una instancia independiente de ActiveVOS en su entorno.

El ActiveVOS integrado autentica las solicitudes de Data Director y MDM Hub mediante un principal específico de confianza para MDM y ActiveVOS. A este principal se lo conoce como usuario de confianza. El administrador del sistema crea las credenciales y las funciones del usuario de confianza en el servidor de aplicaciones.

El servidor de ActiveVOS debe ejecutarse en el mismo servidor de aplicaciones que MDM Hub. Para obtener más información, consulte la *Guía de configuración de Multidomain MDM*.

Dynamic Data Masking

Informatica Dynamic Data Masking es un producto de seguridad de datos que opera entre un cliente y una base de datos para impedir el acceso no autorizado a la información confidencial. Dynamic Data Masking intercepta las solicitudes enviadas a la base de datos y aplica una máscara a los datos antes de enviar los resultados de la solicitud al cliente.

Dynamic Data Masking proporciona un nivel de seguridad de datos adicional a las bases de datos que administra MDM Hub. Utilice la consola de administración de Dynamic Data Masking para configurar la conexión de Dynamic Data Masking con el Almacén de referencias operativas y configure las reglas de enmascaramiento para los datos. Configure la conexión de MDM Hub con Dynamic Data Masking al registrar un Almacén de referencias operativas.

El programa de instalación de MDM no instala Dynamic Data Masking con MDM Hub. Debe instalar Dynamic Data Masking por separado. Para obtener más información sobre la instalación de Dynamic Data Masking, consulte la documentación de Dynamic Data Masking.

Nota: Para utilizar Dynamic Data Masking en MDM Hub, debe tener instalados Dynamic Data Masking 9.6.0 y la revisión de error de emergencia 14590. Las versiones anteriores de Dynamic Data Masking no son compatibles con MDM Hub.

Integración entre Dynamic Data Masking y MDM Hub

Una vez que se haya instalado y configurado Dynamic Data Masking correctamente, puede integrar Dynamic Data Masking con MDM Hub.

Los pasos siguientes describen el proceso de integración:

1. En la consola de administración de Dynamic Data Masking, cree un servicio de Dynamic Data Masking. Configure el número del puerto de escucha para que coincida con el número de puerto al que el cliente envía las solicitudes a la base de datos.
2. Defina las propiedades de conexión de la base de datos que precisa el enmascaramiento de datos.
3. Cree una regla de conexión. Configure la regla para identificar las solicitudes a la base de datos que deben enmascararse. Asigne una base de datos y un conjunto de reglas de seguridad al conjunto de reglas de conexión.

4. Cree un conjunto de reglas de seguridad. Defina las reglas para enmascarar los datos que se devolverán a MDM Hub.
5. En la Consola del concentrador, configure la conexión a Dynamic Data Masking.

Cuando se ejecutan procesos para el Almacén de referencias operativas, Dynamic Data Masking aplica las reglas en la base de datos antes de devolver datos a MDM Hub.

Nota: Si no añade la conexión de Dynamic Data Masking al Almacén de referencias operativas, MDM Hub omite cualquier regla de Dynamic Data Masking que haya definido.

Para obtener más información sobre cómo configurar Dynamic Data Masking, consulte la *Guía del administrador de Informatica Dynamic Data Masking*.

Procedimientos recomendados de Dynamic Data Masking para MDM Hub

Puede utilizar Dynamic Data Masking de forma eficaz en MDM Hub con ayuda de los procedimientos recomendados.

Procedimientos recomendados para crear reglas de Dynamic Data Masking en el Editor de reglas

Dynamic Data Masking evalúa las reglas del Editor de reglas de arriba a abajo. Por tanto, si crea reglas que no son de enmascaramiento, debe colocarlas por encima de las reglas de enmascaramiento que cree para que se apliquen.

Procedimiento recomendado para permitir que los usuarios vean datos sin enmascarar

Dynamic Data Masking no enmascara los datos en la base de datos. Cuando visualiza datos en MDM Hub, los datos aparecen enmascarados. Utilice declaraciones CREATE VIEW en Dynamic Data Masking para conceder a los usuarios privilegios para ver los datos sin enmascarar.

Procedimiento recomendado para bloquear usuarios

Para impedir que los usuarios añadan un registro al que se le aplica enmascaramiento, debe crear una regla independiente para cada objeto base afectado. Defina una coincidencia de texto como `%INSERT %<BO_NAME>%<ROLE NAME>%` y la acción de procesamiento de instrucciones de bloqueo.

Procedimiento recomendado para permitir que los usuarios actualicen datos enmascarados

De forma predeterminada, el motor de Dynamic Data Masking impide que los usuarios editen tablas con datos enmascarados. Si desea actualizar datos enmascarados en MDM Hub, puede crear una regla en el Editor de reglas de Dynamic Data Masking para permitir que un usuario actualice columnas enmascaradas.

Práctica recomendada para crear reglas con el indicador MDM_SYSTEM

En MDM Hub, el usuario MDM_SYSTEM es un indicador interno para las llamadas de sistema. MDM_SYSTEM no aparece en la lista de funciones de la Consola del concentrador. Dynamic Data Masking aplica enmascaramiento según las funciones de MDM Hub que tenga el usuario. Cuando cree reglas de Dynamic Data Masking en el Editor de reglas, no cree reglas solo para el indicador MDM_SYSTEM. La guía de instalación y configuración de Youchart of Accounts debe combinar MDM_SYSTEM con un nombre de usuario o funciones que pertenezcan a un usuario. Puede combinar el indicador MDM_SYSTEM con cualquier otra regla para crear reglas avanzadas en Dynamic Data Masking.

Configurar Dynamic Data Masking para un Almacén de referencias operativas

Configure la conexión de Dynamic Data Masking con MDM Hub al registrar un Almacén de referencias operativas mediante la Consola del concentrador.

1. Inicie la Consola del concentrador.

   Aparecerá el cuadro de diálogo **Cambiar base de datos**.
2. Seleccione la Base de datos principal de MDM Hub y haga clic en **Conectar**.
3. En el entorno de trabajo de configuración, inicie la herramienta **Bases de datos**.
4. Adquiera un bloqueo de escritura.
5. Haga clic en el botón **Registrar base de datos**.

   Aparece el **Asistente de conexión de Informatica MDM Hub**, que le pide que seleccione el tipo de base de datos.
6. Seleccione el tipo de base de datos y haga clic en **Siguiente**.
7. Configure las propiedades de conexión de la base de datos.
8. En el campo **Puerto**, el puerto que especifique debe coincidir con el puerto de escucha de Dynamic Data Masking para la base de datos.
9. En el campo **URL de conexión de DDM**, escriba la URL para el servidor de Dynamic Data Masking.
10. Haga clic en **Finalizar**.

    Aparece el cuadro de diálogo **Registrar base de datos**.
11. Haga clic en **Aceptar**.

    MDM Hub registra el Almacén de referencias operativas.
12. Seleccione el Almacén de referencias operativas que ha registrado y haga clic en el botón **Probar conexión de base de datos** para probar la configuración de la base de datos.

    Si utiliza WebSphere, reinicie WebSphere antes de probar la conexión de base de datos.

    El cuadro de diálogo Probar base de datos muestra el resultado de la prueba de conexión de la base de datos.
13. Haga clic en **Aceptar**.

    Dynamic Data Masking se conecta al Almacén de referencias operativas que ha registrado.

Configurar un canal T3S de WebLogic en Linux

El protocolo T3S de WebLogic se basa en SSL, y puede configurarlo para MDM Hub.

Los siguientes pasos asumen que está familiarizado con los procedimientos para crear y usar un almacén de claves, configurar una instancia de servidor para SSL y crear un canal. Para obtener más información, consulte la documentación de WebLogic.

1. Antes de comenzar, debe tener un almacén de claves que desea usar con fines de identificación.
2. En la consola de administración de WebLogic, desplácese hasta la instancia de servidor que utiliza con MDM y configure SSL con las siguientes propiedades:
   - **Identity and Trust Location** = **Keystore**

- **Private Key Location** = **from Custom Identity Keystore**
- **Private Key Alias** = <Alias definido en el almacén de claves>
- **Private Key Passphrase** = <Frase de contraseña definida en el almacén de claves>
- **Certificate Location** = **from Custom Identity Keystore**
- **Trusted Certificate Authorities** = **from Java Standard Trust Keystore**

3. Abra una ventana de símbolo del sistema del administrador (cmd) y utilice el comando `keytool` para importar el almacén de claves en los directorios JDK y JRE en `lib/security/cacerts`.
   El siguiente código de muestra es un ejemplo de la sintaxis:

```
keytool -import -alias <SSL Private Key Alias> -keystore "<JDK installation
directory>/jre/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/
Oracle_Home/user_projects/domains/base_domain/servers/<WebLogic server instance>/
keystores/wls12c_server.cer" -v

keytool -import -alias <SSL Private Key Alias> -keystore "<JRE installation
directory>/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/
user_projects/domains/base_domain/servers/<WebLogic server instance>/keystores/
wls12c_server.cer" -v
```

   Nota: Si necesita ayuda con el comando `keytool`, consulte la documentación de Java.

4. Desplácese hasta el archivo `<dominio de WebLogic>/bin/startWebLogic.sh` y establezca la siguiente opción de Java:

```
-Doracle.jdbc.J2EE13Compliant=true
```

5. En la consola de administración de WebLogic, cree un canal T3S que coincida con la configuración de SSL. Establezca las siguientes propiedades:
   - **Name** = <Nombre del canal>
   - **Protocol** = t3s
   - **Listen Address** = <Nombre de host definido en el almacén de claves>
   - **Listen Port** = <Puerto definido en el almacén de claves>
   - Seleccione **Tunneling Enabled**
   - Seleccione **Two Way SSL**
   - Compruebe que **Server Private Key Alias** muestra el alias que especificó cuando configuró SSL.
6. Guarde el canal y compruebe que este aparece en la lista de canales de red.
7. Si utiliza Informatica Data Director con las vistas de Entidad 360, desplácese hasta el archivo `<dominio de WebLogic>/bin/setDomainEnv.sh` y establezca las siguientes opciones de MDM:
   - `e360.mdm.protocol=t3s`
   - `e360.mdm.host=<Dirección de escucha del canal T3S>`
   - `e360.mdm.port=<Puerto de escucha del canal T3S>`
8. Reinicie WebLogic.
9. Compruebe que el canal funciona haciendo ping en él.

```
java weblogic.Admin -url t3s://<T3S Channel Listen Address>:<T3S Channel Listen
Port> -username <WebLogic username> -password <WebLogic password> PING
```

10. Ahora puede iniciar la consola del concentrador mediante HTTPS y el puerto seguro.

```
https://<T3S Channel Listen Address>:<T3S Channel Listen Port>/cmx/
```

Habilitar Secure Siperian Bus en el servidor de aplicaciones WebSphere

Para habilitar la comunicación de mensaje seguro a través de Siperian Bus, debe configurar la consola de WebSphere y después las `cmxserver.properties` relevantes.

1. Abra la consola de WebSphere.
2. Configure un usuario nuevo en la pestaña **Usuarios y grupos**.
   a. Haga clic en **Administrar usuarios** y después en **Crear**.
   b. En la página **Crear un usuario nuevo**, introduzca la información necesaria para crear un usuario nuevo. No asigne ningún privilegio a este usuario.
   c. Haga clic en **Crear** para completar la acción.
3. Establezca la configuración en la pestaña **Integración de servicio**.
   a. Vaya a **Buses** y haga clic en el vínculo **SiperianBus**. Aparece la página **Configuración**.
   b. En la sección **Propiedades adicionales**, haga clic en **Seguridad**. Aparece la página **Buses > SiperianBus > Buses > Seguridad para bus SiperianBus**.
   c. En la sección **Propiedades generales**, active la casilla de verificación **Habilitar seguridad de bus**.
   d. En la sección **Directiva de autorización**, haga clic en **Usuarios y grupos en el rol de conector de bus**.
   e. Haga clic en **Nuevo**, seleccione el botón de radio **Usuarios** y haga clic en **Siguiente**.
   f. Seleccione el usuario, y haga clic nuevamente en **Siguiente**. Se abrirá la página **Resumen**.
   g. Haga clic en **Finalizar**.
   h. Regrese a la página **Buses > SiperianBus > Buses > Seguridad para bus SiperianBus**.
   i. En **Artículos relacionados**, haga clic en el vínculo **Datos auténticos de JAAS -J2C** y haga clic en **Nuevo**.
   j. En la sección **Propiedades generales**, especifique **Alias**, **ID de usuario** y **Contraseña**. Haga clic en **Aceptar**.
   k. Regrese a la página **Buses > SiperianBus > Seguridad para bus SiperianBus**.
   l. En la sección **Propiedades generales**, seleccione este alias de JAAS desde la lista de **alias de autenticación entre motores**. Haga clic en **Aceptar**.
4. Establezca la configuración en la pestaña **Recursos**.
   a. Vaya a **JMS > Fábrica de conexiones de cola** y después haga clic en el vínculo de la fábrica de conexión para abrirla. Aparece la página **Configuración**.
   b. En la sección **Configuración de seguridad**, en la lista de **alias de autenticación administrados por el contenedor** seleccione el alias de JAAS que definió anteriormente. Haga clic en **Aceptar**.
   c. Vaya a **JMS > Especificaciones de activación** y haga clic en el vínculo **SiperianActivation**. Aparece la página **Configuración**.
   d. En la sección **Configuración de seguridad**, en la lista de **alias de autenticación** seleccione el alias de JAAS que definió anteriormente. Haga clic en **Aceptar**.

Pase a la configuración de las propiedades relevantes en el archivo `cmxserver.properties`.

Configure cmxserver.properties para Secure Siperian Bus

Debe configurar las `cmxserver.properties` relevantes para completar la configuración de Secure Siperian Bus. A continuación, genere la contraseña cifrada. Antes de comenzar, habilite la seguridad para Siperian Bus en el servidor de aplicaciones WebSphere.

1. En MDM Hub, abra el archivo `cmxserver.properties`.
   - En UNIX. `<directorio de instalación de infamdm>/hub/server/resources`
   - En Windows. `<directorio de instalación de infamdm>\hub\server\resources`
2. Establezca el nombre de usuario por almacenar:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.username=<nombre de usuario>
   ```
3. Establezca la contraseña por almacenar:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.password=<contraseña>
   ```

   Por ejemplo:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.password=UlRJz88k4O2EL5yDw2jypuCLAkEYHCwVg8F
   iNJavdfVvKnC8RFGIGE45IeKyQm5C2WJe2pX+ajXj1QeC/j
   +o7jQmItiaYoyrEMsIRWTvZiHg14ZKjYbFNJcwGSC3rpURvPqH+WMjaEWdXxcD8p7uZ1pphc7WXkE
   +VouCR6kRwy0=
   ```
4. Ejecute el siguiente comando para generar la contraseña cifrada en el entorno:

   ```
   java -classpath siperian-api.jar;siperian-common.jar;siperian-server.jar
   com.delos.util.PublicKeyBasedEncryptionHelper <plain text password> <infa home
   server>
   ```

   Por ejemplo:

   ```
   java -classpath siperian-api.jar;siperian-common.jar;siperian-server.jar
   com.delos.util.PublicKeyBasedEncryptionHelper admin \<infamdm installation directory>
   \hub\
   ```

CAPÍTULO 7

Autenticación basada en certificados

Este capítulo incluye los siguientes temas:

Autenticación basada en certificados Resumen

MDM Hub utiliza un mecanismo de autenticación basada en certificados para proteger la comunicación entre los componentes de MDM Hub y las aplicaciones de confianza. El mecanismo de autenticación también es compatible con el Marco de servicios de integración (SIF) y las API de servicios de entidad de negocio.

De forma predeterminada, el módulo de inicio de sesión de certificados considera las aplicaciones de Informatica, como Data Director, como aplicaciones de confianza. Para utilizar la autenticación basada en certificados con aplicaciones externas, debe registrar las aplicaciones como aplicaciones de confianza.

Una aplicación externa registrada como aplicación de confianza pasa a MDM Hub una concatenación del nombre de la aplicación y el nombre de usuario. Por ejemplo, `IDD/administrador`. La aplicación externa también debe pasar una carga de seguridad.

Autenticación basada en certificados y clientes externos

Los clientes externos a MDM Hub, como la API de SiperianClient, pueden enviar solicitudes que utilizan la autenticación mediante nombre de usuario y contraseña. Sin embargo, los clientes externos también pueden utilizar la autenticación basada en certificados.

Para configurar la autenticación basada en certificados para un cliente externo a MDM Hub, realice los pasos siguientes:

1. En la consola del concentrador, registre el certificado público para los usuarios asociados al cliente externo.
2. Use el cliente externo para desencadenar una solicitud.

Aplicaciones de confianza

En MDM Hub, una aplicación de confianza tiene un tipo de usuario llamado aplicación de usuario, que puede ejecutar solicitudes en nombre de cualquier usuario normal de MDM Hub, incluido el usuario administrador. Las aplicaciones de confianza pertenecen al marco de aplicaciones de confianza de MDM Hub.

Debe usar la consola del concentrador para registrar cada aplicación personalizada que quiera usar como aplicación de confianza. De forma predeterminada, MDM Hub considera las aplicaciones de Informatica, como Data Director y ActiveVOS que se usan en las implementaciones de MDM Hub, como aplicaciones de confianza.

De forma predeterminada, cada aplicación de confianza tiene configurado un conjunto de claves públicas y privadas. MDM Hub autentica la solicitud de una aplicación de confianza a través de la autenticación basada en certificados.

Para configurar una aplicación personalizada como aplicación de confianza, consulte "Añadir cuentas de usuario" en la página 32.

Añadir una aplicación externa como una aplicación de confianza

Puede agregar aplicaciones externas al marco de la aplicación de confianza de MDM HUb como aplicaciones de confianza.

1. En la consola del concentrador, añada una cuenta de usuario para el usuario de aplicación correspondiente a la aplicación externa.

   Nota: Asegúrese de seleccionar la casilla **Usuario de aplicación** en el cuadro de diálogo **Añadir usuario** y de usar solo caracteres en minúscula para el nombre de la cuenta de usuario.
2. Registre un certificado público con la cuenta de usuario de aplicación.
3. Use la aplicación externa para desencadenar una solicitud.

   Nota: Si desea usar la autenticación basada en certificados, configure el nombre de la solicitud como <nombre de aplicación>/<nombre de usuario>. El <nombre de aplicación> debe ser el mismo que se usa en el paso 1. El <nombre de usuario> es el nombre del usuario de MDM Hub que desencadena la solicitud.

Administración de certificados y claves

MDM Hub utiliza una autenticación basada en certificados. Debe conservar el certificado y los pares de claves privadas para cada usuario en una ubicación segura.

De forma predeterminada, MDM Hub mantiene los certificados y las claves privadas en la siguiente ubicación:

```
<directorio de instalación de MDM Hub>/server/resources/certificates
```

Además, puede configurar un proveedor de certificados personalizados durante la instalación de Multidomain MDM.

Para implementar un proveedor de certificados personalizados, debe implementar una interfaz `PKIUtil.java` en el archivo `siperian-server-pkiutil.jar`, que se encuentra en el siguiente directorio:

```
<directorio de instalación de MDM Hub>/hub/server/lib/pkiutils
```

Si utiliza un proveedor de certificados personalizados, debe conservar el almacén de claves y los certificados públicos que la implementación de PKIUtil utiliza.

Nota: Si necesita cambiar el proveedor de certificados, póngase en contacto con el servicio internacional de atención al cliente de Informatica para solicitar una utilidad de configuración de seguridad.

Temas relacionados

- "Utilidad de configuración de seguridad" en la página 61

Utilidad de configuración de seguridad

Puede utilizar la utilidad de configuración de seguridad para administrar algunas opciones de seguridad en la implementación de MDM Hub.

Puede utilizar la utilidad de configuración de seguridad para realizar las siguientes tareas:

- Cambiar el proveedor de certificados que se utiliza para autenticación.
- Restablecer una contraseña para un usuario de MDM Hub.
- Cambiar el algoritmo hash que se utiliza para hash de contraseña.
- Cambiar la clave hash de cliente que se utiliza para crear el algoritmo hash.

Nota: Para obtener la utilidad de configuración de seguridad, póngase en contacto con el servicio internacional de atención al cliente de Informatica.

CAPÍTULO 8

Hash de contraseña

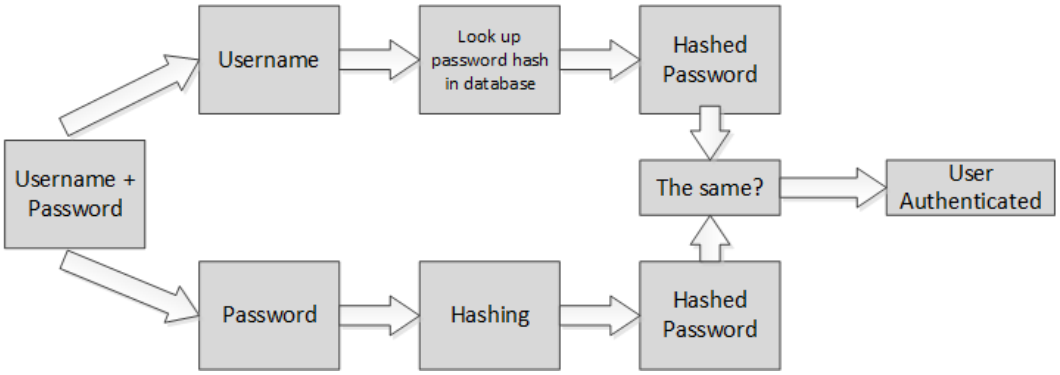
Este capítulo incluye los siguientes temas:

Resumen de hash de contraseña

El hash de contraseña es una forma de cifrar las contraseñas de forma irreversible a través de una función hash criptográfica. MDM Hub utiliza un método de hash de contraseña para proteger las contraseñas de usuario y asegurarse de que estas nunca se almacenen en formato de texto sin cifrar en una base de datos. El administrador de MDM Hub configura las opciones de hash de contraseña, tales como el algoritmo y las claves de hash del usuario, durante la instalación del Servidor del concentrador.

Informatica proporciona una utilidad de configuración de seguridad para administrar algunas opciones de configuración de seguridad en una implementación de MDM Hub, incluidos el cambio del algoritmo hash y el restablecimiento de las contraseñas de usuario de MDM Hub.

La siguiente imagen muestra cómo MDM Hub autentica la contraseña del usuario:



Temas relacionados

- "Utilidad de configuración de seguridad" en la página 61

Opciones de hash de contraseña

Durante la instalación del Servidor del concentrador, puede configurar las siguientes opciones de hash de contraseña:

- Utilizar una clave de hash personalizada como parte del algoritmo hash
- Utilizar el algoritmo hash SHA3 predeterminado o crear un algoritmo hash personalizado
- Utilizar el proveedor de certificados predeterminados o un proveedor de certificados personalizados

Tanto SHA3 como los algoritmos hash personalizados se aseguran de que las contraseñas de los usuarios de MDM Hub estén cifradas de forma irreversible y que no se almacenen nunca en formato de texto sin cifrar en una base de datos. Independientemente de qué algoritmo hash utilice, el algoritmo tendrá los siguientes componentes:

- Una función hash
- Un valor de sal
- Un valor de pimienta o clave de hash, que se establece durante la instalación de MDM Hub. El administrador de MDM Hub es responsable de generar esta clave y almacenarla de forma segura.

Si crea un valor de pimienta, Informatica recomienda usar una clave que contenga una secuencia de hasta 32 caracteres hexadecimales sin delimitadores.

Importante: Proteja la confidencialidad de la clave de hash para evitar el riesgo de vulneración de datos. Si la clave de hash es robada, deberá restablecer todas las contraseñas.

El algoritmo hash de contraseña y la implementación subyacente para el algoritmo se almacenan en las propiedades del servidor del concentrador. Para obtener más información sobre las propiedades del servidor del concentrador, consulte la *Guía de configuración de Multidomain MDM*.

Algoritmo hash personalizado

Proceso de restablecimiento de contraseña

Si se olvida la contraseña o si cree que la seguridad de los componentes secretos del algoritmo hash podrían estar en peligro, puede restablecer la contraseña. Para hacerlo, póngase en contacto con el servicio internacional de atención al cliente de Informatica.

Cuando restablece la contraseña, recibe un correo electrónico con una contraseña temporal. Utilice esta contraseña para iniciar sesión en MDM Hub y, a continuación, cambie la contraseña a algo que sea significativo para usted. Puede cambiar la contraseña en la consola del concentrador o a través de Informatica Data Director.

Utilidad de configuración de seguridad

Puede utilizar la utilidad de configuración de seguridad para administrar algunas opciones de seguridad en la implementación de MDM Hub.

Puede utilizar la utilidad de configuración de seguridad para realizar las siguientes tareas:

- Cambiar el proveedor de certificados que se utiliza para autenticación.
- Restablecer una contraseña para un usuario de MDM Hub.
- Cambiar el algoritmo hash que se utiliza para hash de contraseña.
- Cambiar la clave hash de cliente que se utiliza para crear el algoritmo hash.

Nota: Para obtener la utilidad de configuración de seguridad, póngase en contacto con el servicio internacional de atención al cliente de Informatica.

Solución de problemas

Si se producen problemas, consulte la siguiente información para encontrar una solución.

Los usuarios de MDM Hub no pueden iniciar sesión

Si MDM Hub vuelve a crear el esquema CMX_SYSTEM después de la instalación del servidor del concentrador, MDM Hub no puede reconocer las contraseñas con hash. Por consiguiente, los usuarios no pueden iniciar sesión en MDM Hub.

Para solucionar el problema, vuelva a ejecutar el script `postInstallSetup` manualmente. Este script garantiza la aplicación de hash a las contraseñas de los usuarios de MDM Hub para que puedan iniciar sesión.

Para obtener más información acerca del script postInstallSetup, consulte la *Guía de instalación de Multidomain MDM*.

APÉNDICE A

Glosario

Administrador de acceso de seguridad (SAM)

El Administrador de acceso de seguridad (SAM) es el módulo de seguridad para proteger los recursos del MDM Hub del acceso no autorizado. En tiempo de ejecución, el SAM hace cumplir las decisiones sobre política de seguridad de la organización para la implementación del MDM Hub y administra la autenticación de usuarios y la autorización de acceso según la configuración de seguridad.

Administrador de datos

Con esta herramienta se revisan los resultados de todas las fusiones —fusiones automáticas incluidas — y se corrigen los datos si es necesario. Le ofrece vista del linaje de datos para los registros de todos los objetos base. El Administrador de datos también le permite anular la fusión de registros y ver distintos tipos de historial de cada registro consolidado.

Utilice el Administrador de datos para buscar registros, ver sus referencias cruzadas, anular la fusión de registros, desvincular registros, ver el historial de registros, crear nuevos registros, editar registros y reemplazar la configuración de confianza. El Administrador de datos muestra todos los registros que cumplen los criterios de búsqueda definidos.

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)

Una base de datos que contiene datos principales y las reglas que se aplican a esos datos. Entre esas reglas están las de procesamiento de los datos principales, las de administración del conjunto de objetos de datos principales, junto con las de procesamiento y la lógica auxiliar que MDM Hub utiliza para definir la mejor versión de confianza. Una configuración de MDM Hub puede tener uno o varios almacenes de referencias operativas. El nombre predeterminado de un ORS es CMX_ORS.

autenticación

Proceso de comprobación de la identidad de un usuario para asegurarse de que es quien dice ser. En Informatica MDM Hub, los usuarios se autentican a partir de las credenciales que proporcionan: nombre de usuario/contraseña, carga de seguridad, o una combinación de ambos. Informatica MDM Hub proporciona un mecanismo de autenticación interno y también admite la autenticación de usuarios con otros proveedores de autenticación.

autorización

Proceso en el que se determina si un usuario tiene privilegios suficientes para acceder al recurso de Informatica MDM Hub que ha solicitado. En Informatica MDM Hub, los privilegios de recursos están

asignados a funciones. Los usuarios y grupos de usuarios están asignados a funciones. Los privilegios de recursos de un usuario varían según las funciones a las que esté asignado, así como de las funciones asignadas a los grupos de usuarios a los que pertenezca.

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).

bloqueo de escritura

Un bloqueo que es necesario para realizar cambios en el esquema subyacente en la Consola del concentrador. Todas las herramientas que no son de gestión de datos (excepto las herramientas de seguridad de Almacén de referencias operativas) están en modo solo lectura a menos que adquiera un bloqueo de escritura. Los bloqueos de escritura permiten que varios usuarios realicen cambios en el esquema al mismo tiempo.

carga de seguridad

Datos binarios sin formato proporcionados a una solicitud de operación de un MDM Hub que puede contener datos complementarios necesarios para obtener autenticación o autorización.

Consola del concentrador

Interfaz de usuario de Informatica MDM Hub que se compone de un conjunto de herramientas para administradores y gestores de datos. Cada herramienta permite a los usuarios llevar a cabo una determinada acción o un conjunto de acciones relacionadas, tales como generar el modelo de datos, ejecutar tareas por lotes, configurar el flujo de datos, configurar el acceso de aplicaciones externas a recursos de Informatica MDM Hub y otras tareas de operaciones y configuración del sistema.

directiva de contraseña

Especifica las características de contraseña de las cuentas de usuario de Informatica MDM Hub, como la longitud de contraseña, la caducidad, la configuración de inicio de sesión, la reutilización de contraseña y otros requisitos. Puede definir una directiva de contraseña global para todas las cuentas de usuario de una implementación de Informatica MDM Hub, y puede reemplazar estos valores para usuarios concretos.

Dynamic Data Masking

Un producto de seguridad de datos que opera entre un cliente y una base de datos para impedir el acceso no autorizado a información confidencial. Dynamic Data Masking intercepta las solicitudes enviadas a la base de datos y aplica las reglas de enmascaramiento de datos a la solicitud para enmascarar los datos antes de devolverlos al cliente.

entorno de trabajo

Un mecanismo para agrupar herramientas similares de la Consola del concentrador. Un entorno de trabajo es una colección lógica de herramientas relacionadas. Por ejemplo, el entorno de trabajo modelo contiene las herramientas de modelado de datos, como Esquema, Consultas, Paquetes y Asignaciones.

Entorno de trabajo de configuración

Incluye herramientas para configurar diversos objetos del MDM Hub, como el Almacén de referencias operativas, los usuarios, la seguridad, las colas de mensajes y la validación de metadatos.

Entorno de trabajo del Administrador de acceso de seguridad

Incluye herramientas para administrar usuarios, grupos, recursos y funciones.

función

Define un conjunto de privilegios para acceder a recursos seguros de Informatica MDM Hub.

gestor de datos

Usuario de Informatica MDM Hub que es responsable principalmente de la calidad de los datos. Los gestores de datos acceden a Informatica MDM Hub mediante la Consola del concentrador y utilizan las herramientas de Informatica MDM Hub para configurar los objetos del Almacén del concentrador.

grupo por lotes

Un conjunto de tareas por lotes individuales (por ejemplo: las tareas de transferencia a tabla provisional, de carga y de coincidencia) que se puede ejecutar con un solo comando. Cada tarea por lotes de un grupo se puede ejecutar a continuación de la tarea anterior o en paralelo con otras tareas.

Hierarchy Manager

The Administrador de jerarquía allows users to manage hierarchy data that is associated with the records managed in the MDM Hub. For more information, see the *Multidomain MDM Configuration Guide*.

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.

Kerberos

Protocolo de autenticación de red de equipo que permite que los nodos que se comunican a través de una red no segura prueben su identidad el uno al otro de modo seguro. El Instituto Tecnológico de Massachusetts desarrolló el protocolo y realiza una implementación de Kerberos que está disponible de forma gratuita.

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.

objeto base

Una tabla que contiene información sobre una entidad relevante para su negocio, como un cliente o una cuenta.

paquete

Un *paquete* es una vista pública de una o varias tablas subyacentes de Informatica MDM Hub. Los paquetes representan subconjuntos de las columnas de esas tablas, junto con las tablas que estén unidas a las tablas. Un paquete se basa en una consulta. La consulta subyacente puede seleccionar un subconjunto de registros de la tabla o de otro paquete.

perfil

En Administrador de jerarquía, describe qué campos y registros puede mostrar, editar o añadir un usuario de HM. Por ejemplo: un perfil puede permitir acceso completo de lectura/escritura a todas las entidades y relaciones, mientras que otro perfil puede ser de solo lectura (no permite añadir ni editar).

privilegio

Permiso para acceder a un recurso de MDM Hub. Con la autorización interna de MDM Hub, a cada función se le asigna uno de los siguientes privilegios.

Privilegio	Permite al usuario...
READ	Visualizar datos.
CREATE	Crear registros de datos en el Almacén del concentrador.
UPDATE	Actualizar registros de datos en el Almacén del concentrador.
MERGE	Fusionar y anular la fusión de datos.
EXECUTE	Ejecutar funciones de limpieza y grupos por lotes.
DELETE	Eliminar los registros de datos del Almacén del concentrador.

Los privilegios determinan el acceso que los usuarios de aplicaciones externas tienen a los recursos de MDM Hub. Por ejemplo, una función puede configurarse para tener privilegios READ, CREATE, UPDATE y MERGE en paquetes y columnas de paquete concretos. Estos privilegios no se aplicarán cuando se use la Consola del concentrador, aunque la configuración afectará al uso de la Consola del concentrador en cierto modo.

proveedor

Consulte *proveedor de seguridad* en la página 68.

proveedor de seguridad

Una aplicación de otros fabricantes que proporciona servicios de seguridad (autenticación, autorización y servicios de perfil de usuario) a los usuarios que acceden a Informatica MDM Hub.

puntos de decisión de directiva (PDP)

Puntos de comprobación de seguridad específicos que autentican la identidad del usuario y autorizan el acceso de usuarios a los recursos del MDM Hub.

puntos de refuerzo de directiva (PEP)

Puntos de comprobación de seguridad específicos que aplican, en tiempo de ejecución, directivas de seguridad a solicitudes de autenticación y autorización.

recurso privado

Un recurso de Informatica MDM Hub que está oculto para la herramienta Funciones, y que impide el acceso a través de operaciones del Marco de servicios de integración (SIF). Cuando añade un nuevo recurso en la Consola del concentrador (como un nuevo objeto base), se designa como un recurso PRIVATE de forma predeterminada.

seguridad

La capacidad para proteger la privacidad de la información, la confidencialidad, y la integridad de los datos mediante la protección frente a accesos no autorizados o falsificación de los datos y otros recursos de su implementación de Informatica MDM Hub.

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.

INDICE