Informatica

Informatica® Multidomain MDM
10.4 HotFix 2

Guia de Segurança

Informatica Multidomain MDM Guia de Segurança
10.4 HotFix 2
Dezembro 2020

Data da Publicação: 2021-01-14

Conteúdo

Prefácio

Use o Informatica® *Guia de Segurança do Multidomain MDM*para saber como habilitar a segurança no MDM Multidomínio. Aprenda como usar o Gerenciador de Acesso de Segurança para proteger os recursos do MDM Hub e como usar o Dynamic Data Masking para impedir o acesso a dados confidenciais. Aprenda como gerenciar usuários e grupos e como usar permissões, privilégios e funções para gerenciar a segurança do usuário.

Este guia parte do princípio de que você já tem os conhecimentos sobre sistemas operacionais, ambientes de banco de dados e o servidor de aplicativos.

Recursos da Informatica

A Informatica oferece uma variedade de recursos de produtos através da Rede da Informatica e outros portais on-line. Use os recursos para obter o máximo de seus produtos e soluções da Informatica e para aprender com outros usuários da Informatica e especialistas no assunto.

Rede da Informatica

A Rede da Informatica é a porta de entrada para muitos recursos, incluindo a Base de Dados de Conhecimento da Informatica e o Suporte Global a Clientes da Informatica. Para acessar a Rede da Informatica, visite https://network.informatica.com.

Como membro da Rede da Informatica, você tem as seguintes opções:

- Pesquisar por recursos do produto na Base de Dados de Conhecimento.
- Visualizar informações sobre disponibilidade de produtos.
- Criar e revisar seus casos de suporte.
- Encontrar a sua Rede de Grupo de Usuários da Informatica local e colaborar com seus colegas.

Base de Dados de Conhecimento da Informatica

Use a Base de Dados de Conhecimento da Informatica para encontrar recursos de produtos, como artigos de instruções, práticas recomendadas, tutoriais em vídeo e respostas a perguntas frequentes.

Para pesquisar na Base de Dados de Conhecimento, visite https://search.informatica.com. Em caso de dúvidas, comentários ou ideias sobre a Base de Dados de Conhecimento, entre em contato com a equipe da Base de Dados de Conhecimento da Informatica em KB_Feedback@informatica.com.

Documentação da Informatica

Use o Portal de Documentação da Informatica para explorar uma extensa biblioteca de documentação para versões de produtos atuais e recentes. Para explorar o Portal de Documentação, visite https://docs.informatica.com.

Em caso de dúvidas, comentários ou ideias sobre a documentação do produto, entre em contato com a equipe da Documentação da Informatica em infa_documentation@informatica.com.

Matrizes de Disponibilidade de Produto da Informatica

As Matrizes de Disponibilidade de Produto (PAMs) indicam as versões dos sistemas operacionais, os bancos de dados e tipos de fontes e destinos de dados com os quais uma versão de produto é compatível. Veja as PAMs da Informatica em https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

O Informatica Velocity é uma coleção de dicas e práticas recomendadas desenvolvidas pelos Serviços Profissionais da Informatica e baseada em experiências reais de centenas de projetos de gerenciamento de dados. O Informatica Velocity representa o conhecimento coletivo dos consultores da Informatica que trabalham com organizações em todo o mundo para planejar, desenvolver, implantar e manter soluções de gerenciamento de dados bem-sucedidas.

Encontre os recursos do Informatica Velocity em http://velocity.informatica.com. Se você tiver dúvidas, comentários ou ideias sobre o Informatica Velocity, entre em contato com os Serviços Profissionais da Informatica em ips@informatica.com.

Informatica Marketplace

O Informatica Marketplace é um fórum onde você pode encontrar soluções que ampliam e aprimoram suas implementações da Informatica. Aproveite as centenas de soluções dos desenvolvedores e parceiros da Informatica no Marketplace para melhorar sua produtividade e agilizar o tempo de implementação em seus projetos. Encontre o Informatica Marketplace em https://marketplace.informatica.com.

Suporte Global a Clientes da Informatica

Você pode entrar em contato com um Centro de Suporte Global por telefone ou por meio da Rede da Informatica.

Para descobrir o número de telefone local do Suporte Global a Clientes da Informatica, visite o site da Informatica no seguinte link: https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

Para encontrar recursos de suporte on-line na Rede da Informatica, visite https://network.informatica.com e selecione a opção eSupport.

CAPÍTULO 1

Introdução à Segurança do MDM Hub

Este capítulo inclui os seguintes tópicos:

Visão Geral da Segurança do MDM Hub

O MDM Hub protege os dados contra acesso não autorizado e alterações para proteger a privacidade das informações e a integridade dos dados.

Você pode usar o Gerenciador de Acesso de Segurança no Console do Hub para proteger os recursos do MDM Hub e impor as diretivas de segurança operacional, incluindo a autorização e a autenticação de usuário.

Você pode usar o Dynamic Data Masking para evitar o acesso a dados confidenciais. Por exemplo, você pode usar o Dynamic Data Masking para ocultar os números de cartão de crédito de todos os usuários que não tenham direitos administrativos.

Você pode configurar a segurança nas implementações do MDM Hub de várias formas. Você pode usar os provedores de segurança de terceiros para lidar com elementos específicos de segurança da sua organização, ou você configurar o MDM Hub para gerenciar todos os aspectos da segurança. Para obter mais informações sobre como usar o Estrutura de Integração de Serviços (SIF) para configurar a segurança, consulte o *Guia da Estrutura de Integração de Serviços do Multidomain MDM*.

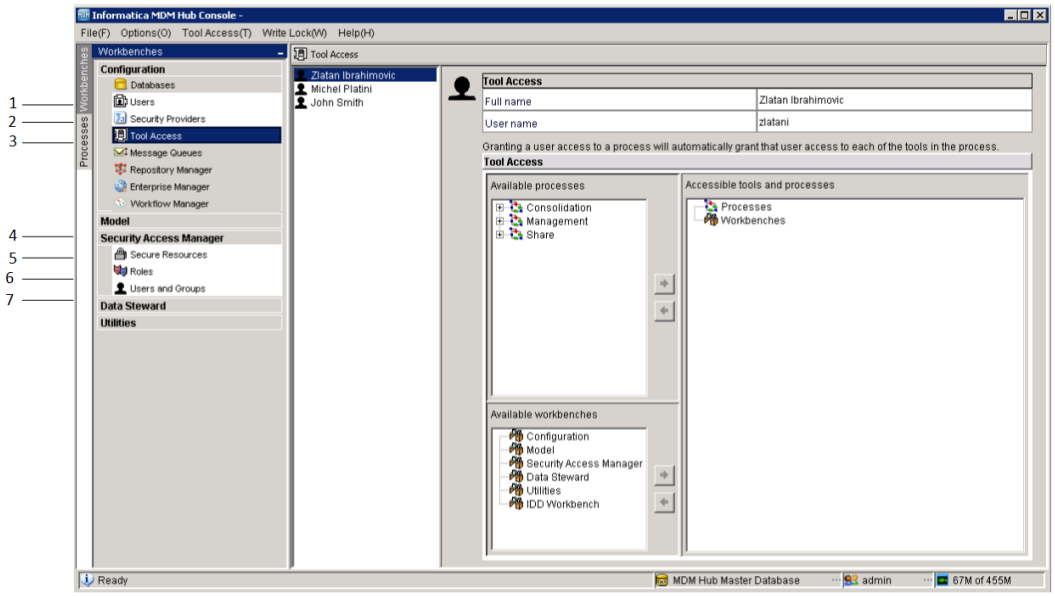
Importante: Antes de começar a proteger o MDM Multidomínio, verifique se o servidor de aplicativos e os dispositivos de armazenamento em cache estão protegidos.

Console do MDM Hub

Use o Console do Hub para configurar a segurança no MDM Hub .

Para controlar os privilégios de acesso às ferramentas do Console do Hub, você pode usar a ferramenta Acesso às Ferramentas no workbench de Configuração. Por exemplo, você pode usar a ferramenta Acesso às Ferramentas para negar o acesso dos administradores de dados a todas as ferramentas do Console do Hub, exceto às ferramentas Gerenciador de Dados e Gerenciador de Mesclagem.

A seguinte imagem mostra a interface do Console do Hub:



1. Ferramenta Usuários
2. Ferramenta Provedores de Segurança
3. Ferramenta Acesso às Ferramentas
4. Gerenciador de Acesso à Segurança
5. Ferramenta Recursos Seguros
6. Ferramenta Funções
7. Ferramenta Usuários e Grupos

Dynamic Data Masking

O Informatica Dynamic Data Masking é um produto de segurança de dados que opera entre um cliente e um banco de dados para evitar o acesso não autorizado às informações confidenciais. O Dynamic Data Masking intercepta solicitações enviadas ao banco de dados e aplica as regras de mascaramento de dados à solicitação para mascarar os dados antes de serem enviados novamente ao cliente.

Você pode usar o Dynamic Data Masking para mascarar ou evitar o acesso a dados confidenciais armazenados em bancos de dados de produção e de não produção gerenciados pelo MDM Hub . Configure as regras de conexão para identificar as solicitações de entrada e as regras de segurança e para definir como você deseja mascarar os dados. O Dynamic Data Masking monitora as solicitações do banco de dados

de entrada do MDM Hub e modifica a solicitação de banco de dados antes de enviá-la ao banco de dados. O banco de dados processa a solicitação de modificação e retorna os resultados mascarados para o Dynamic Data Masking. Em seguida, o Dynamic Data Masking envia os resultados para o MDM Hub .

Você pode usar o Dynamic Data Masking para mascarar os dados de solicitações de banco de dados com tipos específicos ou pode restringir o acesso de determinados grupos de uma organização aos dados. Por exemplo, você pode criar uma regra para aplicar uma função de mascaramento aos números de cartão de crédito quando a solicitação de banco de dados for proveniente de um membro da equipe de suporte. Quando o Dynamic Data Masking envia os dados novamente ao MDM Hub , o membro da equipe de suporte vê os números mascarados, em vez de números reais de cartão de crédito.

Nota: Para usar o Dynamic Data Masking no MDM Hub , você precisa ter o Dynamic Data Masking 9.6.0 e a Correção de Erro de Emergência14590 instalados. Versões anteriores do Dynamic Data Masking não são compatíveis com o MDM Hub .

Para obter mais informações sobre o Dynamic Data Masking, consulte a documentação do Dynamic Data Masking.

Gerenciador de Acesso de Segurança

O Gerenciador de Acesso de Segurança é o módulo de segurança do MDM Hub . O Gerenciador de Acesso de Segurança protege os recursos do MDM Hub contra acesso não autorizado.

O Gerenciador de Acesso de Segurança impõe as diretivas de segurança da sua organização na implementação do MDM Hub . O Gerenciador de Acesso de Segurança gerencia a autenticação e a autorização de usuário de acordo com sua configuração de segurança.

Nota: Você pode usar o Gerenciador de Acesso de Segurança para configurar o acesso do usuário aos recursos do MDM Hub de aplicativos de terceiros. No entanto, você não pode configurar a segurança das ferramentas e recursos do Console do Hub por meio do Gerenciador de Acesso de Segurança. O Console do Hub autentica os usuários e autoriza o acesso do usuário às ferramentas e recursos do Console do Hub por meio de um mecanismo de segurança separado.

Autenticação

A autenticação é o processo de verificação da identidade de um usuário.

O MDM Hub autentica os usuários com base nas credenciais fornecidas, como um nome de usuário e uma senha, ou dados binários brutos em uma carga de segurança.

O MDM Hub usa os seguintes tipos de autenticação:

Interna

Autentica os usuários no MDM Hub , em que o usuário faz logon com um nome de usuário e uma senha.

Diretório Externo

Autentica os usuários por meio de um diretório de usuário externo, com suporte nativo para os servidores de diretório ativados para LDAP, o Microsoft Active Directory e o Kerberos.

Provedores de Autenticação Externos

Autentica os usuários por meio de provedores de autenticação de terceiros.

As implementações do MDM Hub podem usar cada tipo de autenticação de forma exclusiva ou as implementações podem usar uma combinação de autenticações. O tipo de autenticação que você usa depende de como você configura a segurança.

Autorização

A autorização é o processo para determinar se um usuário tem privilégios suficientes para acessar uma solicitação de recurso do MDM Hub .

No MDM Hub , você pode usar as autorizações interna e externa:

Interna

Autoriza por meio do MDM Hub . O MDM Hub determina se é possível acessar recursos seguros examinando os privilégios associados a quaisquer funções atribuídas à sua conta de usuário.

Externo

Autoriza por meio de provedores de autorização de terceiros.

Você pode configurar o MDM Hub para usar qualquer tipo de autorização ou pode configurá-lo para usar os dois tipos de autorização.

Recursos e Privilégios Seguros

Você pode configurar vários recursos do MDM Hub como recursos seguros.

Os seguintes recursos são configuráveis:

- Objetos base
- Mapeamentos
- Pacotes
- Funções de limpeza
- Conjuntos de regras de correspondência
- Metadados
- Perfis
- Tabela de usuários

Você pode conceder acesso aos recursos do MDM Hub de acordo com os privilégios. O MDM Hub pode atribuir os seguintes privilégios:

- Leitura
- Criar
- Atualizar
- Mesclar
- Executar
- Excluir

Os recursos podem ser privados ou seguros. Por padrão, os recursos são seguros. O MDM Hub só pode conceder privilégios a recursos seguros.

Ao configurar a segurança no MDM Hub , considere os seguintes fatos:

- Um recurso específico é configurado para ser seguro.
- Uma função específica é configurada para ter acesso a um ou mais recursos seguros.
- Cada recurso seguro pode ser configurado com privilégios específicos, como leitura ou gravação, que definem o acesso da função ao recurso seguro.

Para executar uma solicitação do Estrutura de Integração de Serviços, o usuário conectado deve ter uma função com os privilégios necessários para acessar o recurso envolvido com a solicitação.

Funções

Uma função representa um conjunto de privilégios para acessar os recursos seguros do MDM Hub . Atribua uma função a um usuário para que ele obtenha privilégios.

Você pode usar a ferramenta Funções no workbench do Gerenciador de Acesso de Segurança para atribuir funções aos usuários e aos grupos de usuários. As funções atribuídas a um usuário ou um grupo de usuários determinam os privilégios de recurso de um usuário ou um grupo de usuários. Você não pode atribuir privilégios diretamente a usuários.

O Gerenciador de Acesso de Segurança aplica a autorização de recursos para solicitações de usuários de aplicativos externos. Os administradores e os administradores de dados que usam o Console do Hub para acessar recursos do MDM Hub não são afetados da mesma forma pelos privilégios de recurso.

Cenários de Implementação de Segurança

Você pode configurar a segurança nas implementações do MDM Hub de várias formas.

Um ponto de decisão de diretiva é um ponto de verificação de segurança específico que determina a identidade dos usuários no tempo de execução. Isso é chamado de autenticação. Um ponto de decisão de diretiva também confirma o que os usuários de recursos do MDM Hub podem acessar. Isso é chamado de autorização. O grau no qual os pontos de decisão de diretiva são tratados internamente pelo MDM Hub ou externamente por provedores de segurança de terceiros ou outros serviços de segurança depende da implementação do MDM Hub .

Os seguintes cenários são exemplos de maneiras de alto nível de acordo com as quais você pode configurar a segurança em implementações do MDM Hub :

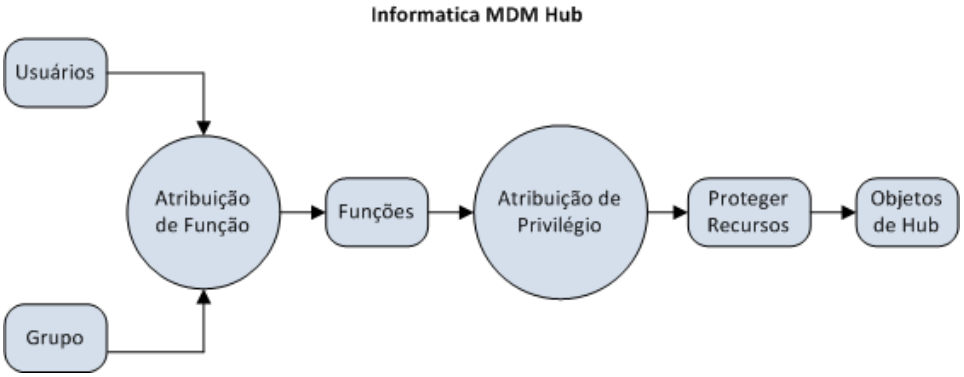
- Pontos de decisão de diretiva somente internos
- Diretório do Usuário Externo
- Pontos de decisão de diretiva Centralizados baseados em funções
- Pontos de decisão de diretiva Centralizados abrangentes

Nota: O MDM Hub não reflete as alterações a privilégios de recurso de um provedor de segurança externo. Se você fizer alterações nos privilégios de recursos usando um provedor de segurança externo, use outras formas de sincronizar as alterações com o MDM Hub .

Ponto de Decisão de Diretiva Interna

O MDM Hub pode lidar com todas as decisões de diretiva internamente.

A seguinte imagem mostra uma implantação de segurança na qual o MDM Hub lida com todas as decisões de diretiva internamente:



Nesse cenário, o MDM Hub toma todas as decisões de diretiva com base em como os usuários, os grupos, as funções, os privilégios e os recursos foram configurados usando o Console do Hub.

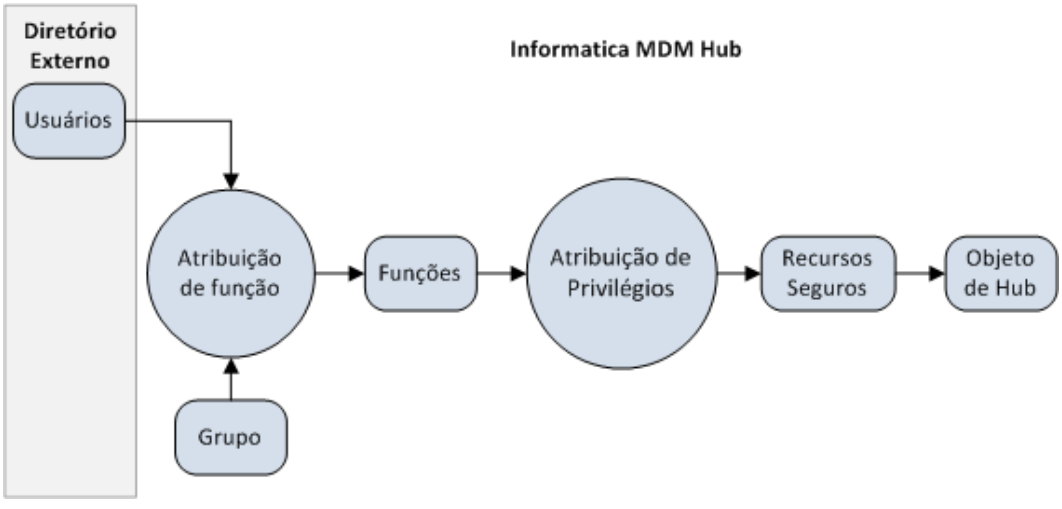
Diretório do Usuário Externo

O MDM Hub pode se integrar com um diretório do usuário externo.

Os usuários ou os grupos de usuários que são mantidos no diretório do usuário externo ainda devem ser registrados na MDM Hub . O registro é necessário antes que o MDM Hub possa atribuir funções e seus privilégios associados a esses usuários e grupos.

Atribua usuários do diretório externo a grupos no MDM Hub . Você deve manter os relacionamentos entre os usuários e grupos no MDM Hub , mesmo se também mantiver os relacionamentos por meio do Protocolo LDAP.

A seguinte imagem mostra uma implantação de segurança em que você gerencia usuários em um diretório externo, mas gerencia os grupos, a atribuição de funções e as atribuições de privilégio no MDM Hub .

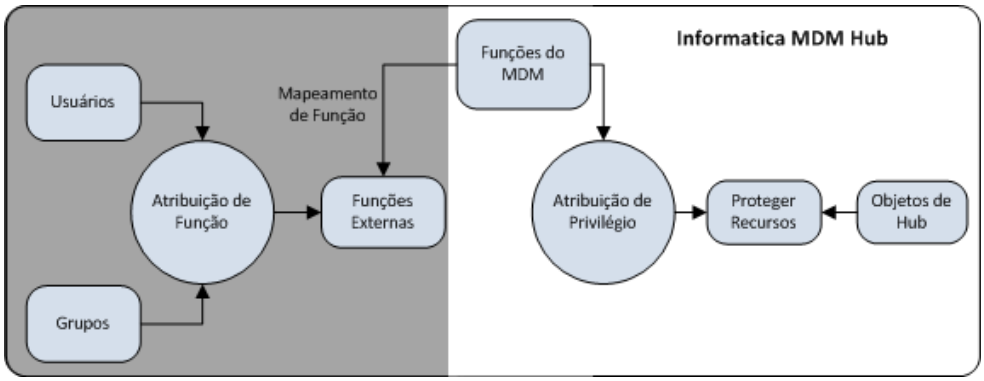


Nesse cenário, o diretório de usuários externos gerencia contas de usuários, grupos e perfis de usuários. O diretório do usuário externo pode autenticar os usuários e fornecer informações ao MDM Hub sobre os perfis de usuário e as associações a grupos.

Decisão de Diretiva Centralizada Baseada em Funções

O MDM Hub pode lidar com algumas decisões de diretiva internamente e receber atribuições de função externa.

A seguinte imagem mostra uma implantação de segurança em que a atribuição de funções, além das contas de usuário, grupos e perfis de usuário, ocorrem externamente ao MDM Hub :

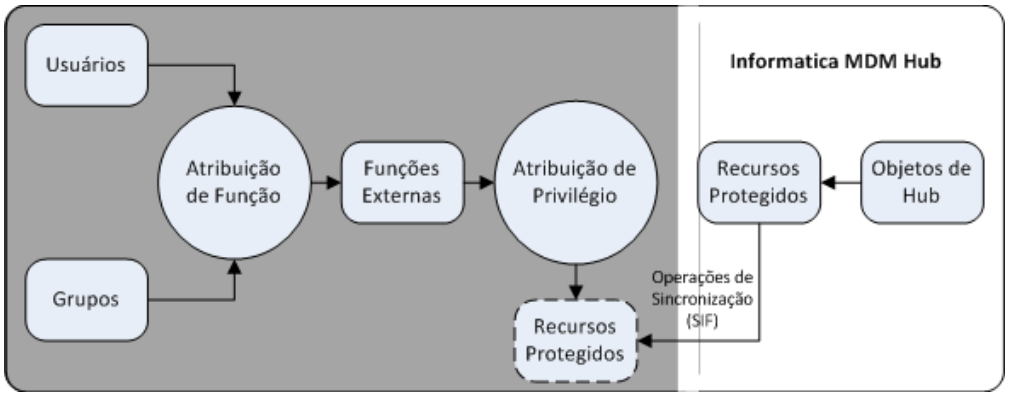


Nesse cenário, as funções externas são explicitamente mapeadas para as funções do MDM Hub .

Decisão de Diretiva Centralizada Abrangente

O MDM Hub pode controlar recursos protegidos internamente, mas aceita funções e privilégios atribuídos de um diretório externo.

A seguinte imagem mostra uma implantação de segurança cujas definição de função e atribuição privilégio ocorrem externamente ao MDM Hub . A figura também mostra que as contas de usuário, os grupos, os perfis de usuário e a atribuição de funções ocorrem externamente ao MDM Hub :



Nesse cenário, o MDM Hub simplesmente expõe os recursos protegidos usando proxies externos, os quais são sincronizados com os recursos protegidos internamente usando solicitações do Estrutura de Integração de Serviços. Todas as decisões de diretiva são externas ao MDM Hub .

Tarefas de Configuração para Cenários de Segurança

A tabela a seguir mostra as tarefas de configuração de segurança que pertencem a cada um dos cenários de implementação de segurança. Se uma célula contiver um "Sim", a tarefa associada ocorrerá no MDM Hub . Se uma célula contiver um "Não", a tarefa associada ocorrerá externamente ao MDM Hub .

Serviço/Tarefa	Pontos de Decisão de Diretiva Interna	Diretório do Usuário Externo	Pontos de Decisão de Diretiva Centralizada RoleNobased	Pontos de Decisão de Diretiva Centralizados Abrangentes
Configurar os usuários do MDM Hub	Sim	Sim	Não	Não
Usar a autenticação externa	Não	Sim	Não	Não
Atribuir usuários ao banco de dados do Armazenamento de Referências Operacionais atual	Sim	Sim	Não	Não
Gerenciar a diretiva de senha global	Sim	Não	Não	Não
Configurar os grupos de usuários	Sim	Sim	Não	Não
Recursos do MDM Hub seguros	Sim	Sim	Sim	Sim
Definir o status de um recurso do MDM Hub	Sim	Sim	Sim	Sim
Configurar funções	Sim	Sim	Sim	Não
Mapear as funções internas para as funções externas	Não	Não	Sim	Não
Atribuir os privilégios de recurso às funções	Sim	Sim	Sim	Não
Gerenciar os provedores de segurança	Não	Sim	Sim	Sim
Atribuir as funções aos usuários e aos grupos de usuários	Sim	Sim	Não	Não

Nota: Se você estiver usando provedores de segurança de terceiros para lidar com qualquer parte da segurança na implementação do MDM Hub , consulte as instruções de configuração do seu provedor de segurança.

Desativando o usuário administrativo padrão

Você pode desativar a conta do usuário administrativo padrão para evitar qualquer autenticação externa para fins de segurança. Como resultado, os usuários externos não podem usar essa conta para acessar o sistema MDM. Você deve criar e configurar um usuário administrativo não padrão no MDM Hub.

1. Crie um usuário administrativo no MDM Hub. Vá para **Usuários > Adicionar Usuário > Novo**, crie essa nova conta de usuário e marque a caixa de seleção **Ativar Administrador**.

2. Atribua o usuário ao ORS registrado. Use a guia **Banco de Dados de Destino** se desejar atribuí-lo a vários ORSs.
3. Para desativar a conta de usuário administrativo padrão, conecte-se ao Banco de Dados Principal do MDM Hub e execute o seguinte comando:

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

4. Atribua esse usuário para uso pelo **Serviço de Identidade** no Console do ActiveVOS.
   a. Acesse a pasta `<Diretório de instalação do MDM Hub>/hub/server/bin`.
   b. Abra o arquivo `build.properties`.
   c. Adicione a seguinte propriedade ao nome de usuário que você criou: `mdm.identity.user=<nome de usuário>`.
   d. Salve o arquivo.
5. Abra um prompt de comando e execute o seguinte script:
   - No Windows. `<Diretório de Instalação do MDM Hub>\hub\server\postInstallSetup.bat`
   - No UNIX. `<Diretório de Instalação do MDM Hub>/hub/server/postInstallSetup.sh`
6. Reinicie o servidor de aplicativos.
7. Faça login no ActiveVOS Console e atualize a senha deste novo usuário, adicionada ao **Serviço de Identidade**.
   a. Na guia **Admin**, vá para **Configurar Serviços > Serviço de Identidade**.
   b. Na guia **Conexão**, na seção **Configurações de Conexão**, especifique e confirme a nova senha.
   c. Clique em **Atualizar**.

   Quando você instalar um HotFix, a configuração `mdm.identity.user=<nome de usuário>` será removida do arquivo `build.properties` automaticamente. Você deve adicionar essa propriedade manualmente. Abra o arquivo `build.properties`, inclua a propriedade e salve o arquivo. Execute o script `postInstallSetup`. Reinicie o servidor de aplicativos.

CAPÍTULO 2

Recursos

Este capítulo inclui os seguintes tópicos:

Visão Geral dos Recursos

O Console do Hub permite que você exponha ou oculte os recursos do MDM Hub para aplicativos externos.

Um recurso seguro é um recurso protegido do MDM Hub exposto à ferramenta Funções, o que permite que o recurso seja adicionado às funções com privilégios específicos. Um grupo de recursos é uma coleção de recursos seguros que simplificam a atribuição de privilégios. Você pode usar a ferramenta Recursos Seguros para definir os grupos de recursos e criar uma hierarquia de recursos.

Você pode configurar os seguintes recursos do MDM Hub como recursos seguros:

Objeto Base

O usuário tem acesso a todos os objetos base seguros, colunas e metadados de conteúdo.

Função de Limpeza

O usuário pode executar todas as funções de limpeza segura.

Perfil do Gerenciador de Hierarquia

O usuário tem acesso a todos os perfis seguros do Gerenciador de Hierarquia.

Serviços de Entidade Comercial

O usuário tem acesso a todos os serviços seguros de Entidade Comercial.

Mapeamento

O usuário tem acesso a todos os mapeamentos seguros e suas colunas.

Pacote

O usuário tem acesso a todos os pacotes seguros e suas colunas.

Pacote Remoto

O usuário tem acesso a todos os pacotes remotos seguros.

Grupos em lote são seguros por padrão. Você não pode alterar o status de grupos em lote para privados. O grupo em lote tem privilégios de Leitura e Execução.

Além disso, você pode usar o Console do Hub para proteger outros recursos acessíveis por solicitações do SIF, incluindo metadados, conjuntos de regra de correspondência, a tabela de auditoria e a tabela de usuários.

Nota: Se você usar o Informatica Data Director, será possível usar os métodos HTTP GET ou POST para acessar o Servidor de Hub. Outros métodos HTTP, como DELETE ou PUT, retornam um erro de HTTP.

Recursos Seguros e Privados

Você pode configurar um recurso protegido do MDM Hub como seguro ou privado.

Seguro

Expõe esse recurso do MDM Hub à ferramenta Funções, o que permite que o recurso seja adicionado às funções com privilégios específicos. Quando você atribui uma função específica a um usuário, esse usuário pode usar as solicitações do SIF para acessar os recursos seguros de acordo com os privilégios associados àquela função. Por padrão, o MDM Hub designa um novo recurso, por exemplo, um objeto base, como seguro.

Privado

Oculta o recurso do MDM Hub da ferramenta Funções. Impede o acesso do recurso de solicitações do SIF.

Um recurso deve estar seguro para que os aplicativos externos possam usar as solicitações do SIF para acessar um recurso do MDM Hub .

Há certos recursos do MDM Hub que talvez você não queira expor a aplicativos externos. Por exemplo, a implementação do MDM Hub pode ter mapeamentos ou pacotes que são usados apenas em trabalhos em lote, e não em solicitações do SIF, para que eles possam permanecer privados.

Nota: O MDM Hub não considera as colunas de pacotes como recursos seguros. As colunas de pacotes herdam o status seguro e os privilégios das colunas do objeto base pai. Se as colunas de pacotes forem baseadas em colunas de tabela do sistema, você não precisará configurar sua segurança, porque elas são acessíveis por padrão.

Grupos de Recursos

Um grupo de recursos é uma coleção lógica de recursos seguros.

Você pode usar a ferramenta Recursos Seguros para definir os grupos de recursos e, em seguida, atribuir recursos relacionados a eles. Os grupos de recursos simplificam a atribuição de privilégios, o que permite que você atribua privilégios a vários recursos e atribua grupos de recursos a uma função.

Para simplificar a administração, considere a criação dos seguintes tipos de grupos de recursos:

- Defina um grupo de recursos ALL_RESOURCES que contém todos os recursos seguros, que permite definir privilégios mínimos globalmente.
- Defina os grupos de recursos por tipo do recurso, de forma que você possa definir os privilégios mínimos para esses tipos de recursos.
- Defina os grupos de recursos por área funcional, como TRAINING_RESOURCES, por exemplo.
- Define um grupo de recursos genérico que você pode atribuir a muitas funções diferentes que tenham privilégios semelhantes.

Hierarquias de Grupos de Recursos

Um grupo de recursos também pode conter outros grupos de recursos, exceto um grupo de recursos ao qual ele pertence. Isso significa que você pode criar uma hierarquia de grupos de recursos e simplificar o gerenciamento de uma grande coleção de recursos.

Recursos Seguros

Somente os recursos seguros podem pertencer a grupos de recursos. Os recursos privados não podem pertencer aos grupos de recursos.

Se você alterar o status de um recurso para privado, o MDM Hub removerá o recurso de qualquer grupo de recursos ao qual ele pertence. Quando você define o status de um recurso para seguro, o MDM Hub adiciona o recurso no grupo de recursos apropriado.

Ferramenta Recursos Seguros

Use a ferramenta Recursos Seguros no Console do Hub para gerenciar a segurança dos recursos do MDM Hub em detalhes, incluindo a definição do status de qualquer recurso do MDM Hub como seguro ou privado. Você também pode usar grupos de recursos para configurar uma hierarquia de recursos.

A ferramenta Recursos Seguros contém as seguintes guias:

Recursos

Usado para definir o status de recursos individuais do MDM Hub como seguro ou privado. O MDM Hub exibe os recursos como uma hierarquia que mostra os relacionamentos entre os recursos. Recursos globais aparecem na parte superior da hierarquia.

Grupos de Recursos

Usada para configurar grupos de recursos.

Você pode usar a ferramenta Recursos Seguros para expor ou ocultar recursos da ferramenta Funções e das solicitações do SIF. Você deve se conectar a um Armazenamento de Referências Operacionais antes de usar a ferramenta.

Configuração de Recursos Seguros

Para procurar e configurar recursos do MDM Hub , use a guia Recursos na ferramenta Recursos Seguros.

Configurando o Status de um Recurso do MDM Hub

Você pode configurar o status do recurso como seguro ou privado para qualquer recurso do MDM Hub .

Nota: Essa configuração de status não se aplica aos grupos de recursos, que contêm somente recursos seguros ou recursos globais.

1. Inicie a ferramenta Proteger Recursos.
2. Adquira um bloqueio de gravação.
3. Na guia Recursos, navegue até a árvore de Recursos para localizar os recursos que você deseja configurar.
4. Clique duas vezes no nome do recurso para alternar entre seguro ou privado. Para alterar o status de vários recursos de uma só vez, execute as etapas 5 e 6.
5. Selecione os recursos que exigem uma alteração de status. Você pode selecionar vários recursos, se desejar.
6. Atualize o status dos recursos selecionados.
   - Clique no botão **Seguro** para alterar o status dos recursos selecionados para seguro.
   - Clique no botão **Privado** para alterar o status dos recursos selecionados para privado.
7. Clique no botão **Salvar** para salvar as alterações.

Filtrando Recursos

Para simplificar a alteração de status de uma coleção de recursos do MDM Hub , você pode especificar um filtro que exibe apenas os recursos que você deseja alterar.

1. Inicie a ferramenta Proteger Recursos.
2. Adquira um bloqueio de gravação.
3. Clique no botão **Filtrar Recursos**.

   A ferramenta Recursos Seguros exibe a caixa de diálogo Filtro de Recursos.
4. Selecione os tipos de recurso.
   - Selecione os tipos de recurso que você deseja incluir no filtro.
   - Desmarque os tipos de recurso que você deseja excluir no filtro.
5. Clique em **OK**.

   A ferramenta Recursos Seguros exibe as árvore de Recursos filtrados.

Configuração dos Grupos de Recursos

Você pode usar a ferramenta Recursos Seguros para definir os grupos de recursos e criar uma hierarquia de recursos. Você pode usar a ferramenta Funções para atribuir privilégios a vários recursos em uma única operação.

A ferramenta Recursos Seguros faz distinção visual de recursos que pertencem direta e indiretamente ao grupo de recursos atual. Os recursos adicionados explicitamente a um grupo de recursos têm associação direta. Os recursos que pertencem a um grupo de recursos adicionados a um grupo de recursos têm associação indireta.

Por exemplo, você deseja ter dois grupos de recursos:

- O Grupo de Recursos A contém o objeto base do Consumidor, o que significa que o objeto base do Consumidor é um membro direto do Grupo de Recursos A.
- O Grupo de Recursos B contém o objeto base Endereço.
- O Grupo de Recursos A contém o Grupo de Recursos B, o que significa que o objeto base Endereço é um membro indireto do Grupo de Recursos A.

Neste exemplo, o objeto base Endereço não está disponível quando você edita o Grupo de Recursos A. Você deve editar o Grupo de Recursos B para editar o objeto base Endereço.

Adicionando Grupos de Recursos

Use a ferramenta Recursos Seguros para adicionar um grupo de recursos à lista de recursos.

1. Inicie a ferramenta Proteger Recursos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Grupos de Recursos**.

   A ferramenta Proteger Recursos exibe a guia Grupo de Recursos.
4. Clique no botão **Adicionar**.

   O Proteger Recursos exibe a caixa de diálogo Adicionar Recursos ao Grupo de Recursos.
5. Insira um nome exclusivo e descritivo para o grupo de recursos.
6. Clique no sinal de mais (+) para expandir a hierarquia do recurso conforme necessário.

   Cada recurso tem uma caixa de seleção indicando sua associação no grupo de recursos. Se você selecionar um pai, todos os filhos também serão selecionados. Por exemplo, se você selecionar o item Objetos Base na árvore, todos os objetos base e seus recursos filhos serão selecionados.
7. Selecione os recursos que você deseja atribuir a este grupo de recursos.
8. Clique em **OK**.

   A ferramenta Proteger Recursos adiciona o novo recurso ao nó Grupos de Recursos.

Editando e Excluindo Grupos de Recursos

Você pode usar a ferramenta Recursos Seguros para editar ou excluir os grupos de recursos.

1. Inicie a ferramenta Proteger Recursos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Grupos de recursos**.
4. Selecione o grupo de recursos cujas propriedades você deseja editar ou excluir.
   - Clique no botão **Editar** para editar um grupo de recursos.
   - Clique no botão **Remover** para remover um grupo de recursos.

   A ferramenta Recursos Seguros exibe a caixa de diálogo Atribuir Recursos ao Grupo de Recursos. Ou a ferramenta Recursos Seguros remove o recurso excluído do nó Grupos de Recursos.
5. Edite o nome do grupo de recursos.
6. Clique no sinal de mais (+) para expandir a hierarquia do recurso.
7. Marque a caixa de seleção **Mostrar Apenas os Recursos Selecionados para esse Grupo de Recursos**.
8. Selecione os recursos que você deseja atribuir a este grupo de recursos.

9. Desmarque os recursos que você deseja remover deste grupo de recursos.
10. Clique em **OK**.

Atualizando a Lista de Recursos

Depois de adicionar um recurso, você pode atualizar a lista de recursos para atualizá-lo.

Para atualizar a lista de recursos, escolha **Atualizar** no menu Recursos Seguros.

A ferramenta Recursos Seguros atualiza a lista de Recursos.

Atualizando Outras Alterações de Segurança

Você também pode alterar o intervalo de atualização para todas as outras alterações de segurança.

Para definir a taxa de atualização das alterações de segurança, defina o seguinte parâmetro no arquivo `cmxserver.properties`:

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

Nota: O intervalo de atualização padrão é de 5 pulsos de relógio a uma taxa de 60.000 milissegundos para cada pulso, o que equivale a 5 minutos.

Configuração de Segurança para Serviços de Entidade Comercial do Data Director

Os serviços da entidade comercial são recursos protegidos e apenas funções de usuário com privilégios podem acessar os serviços da entidade comercial no Data Director.

Você pode configurar os seguintes recursos de serviço da entidade comercial no console do MDM Hub:

- Localizar-Substituir
- Importação de Arquivo
- Correspondência Adhoc

Você deve usar a ferramenta Recursos Seguros para configurar os serviços de entidade comercial como recursos seguros. Você pode usar a ferramenta Funções para atribuir privilégios às funções de usuário.

Configurando os Serviços de Entidade Comercial como um Recurso Seguro

Use a ferramenta Recursos Seguros no ambiente de trabalho do Gerenciador de Acesso à Segurança para configurar os recursos necessários como um recurso seguro.

1. Inicie a ferramenta Proteger Recursos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Recursos**.
4. Navegue para a árvore Recurso e expanda **Serviços de Entidade Comercial**.

5. Clique duas vezes no nome do recurso para alternar entre seguro ou privado.
    a. Clique no botão **Seguro** para alterar o status dos recursos selecionados para seguro.
    b. Clique no botão **Privado** para alterar o status dos recursos selecionados para privado.
6. Clique em **Salvar**.

Atribuindo Privilégios de Função aos Serviços de Entidade Comercial

Use a ferramenta Funções no ambiente de trabalho do Gerenciador de Acesso de Segurança para atribuir privilégios de serviço da entidade comercial às funções de usuário.

1. Inicie a ferramenta Funções.
2. Adquira um bloqueio de gravação.
3. Role pela lista de funções e selecione a função necessária.
4. Clique na guia **Privilégios de Recurso**.
5. Navegue para a árvore Recurso e expanda **Serviços de Entidade Comercial**.
6. Selecione o privilégio **Executar** para cada recurso de serviço da entidade comercial.
7. Clique em **Salvar**.

CAPÍTULO 3

Funções

Este capítulo inclui os seguintes tópicos:

Funções Visão Geral

Uma função é um conjunto de privilégios atribuídos a um usuário ou um grupo. Uma função representa um conjunto de privilégios para acessar os recursos seguros do MDM Hub .

Para os usuários exibirem ou manipularem um recurso seguro do MDM Hub , eles devem ter funções atribuídas que concedam a eles privilégios suficientes para acessar o recurso. As funções determinam o que um usuário está autorizado a acessar e quais tarefas eles podem realizar no MDM Hub .

As funções do MDM Hub são altamente granulares e flexíveis, o que permite que os administradores implementem proteções de segurança complexas de acordo com as diretivas de segurança da organização. Alguns usuários, como os administradores, podem ser atribuídos a uma única função com acesso a tudo. Outros usuários, como os administradores de dados, talvez tenham uma função com privilégios explicitamente restritos.

Uma função também pode ter outras funções atribuídas a ela, herdando assim os privilégios de acesso configurados para essas funções. Os privilégios são aditivos, o que significa que, ao combinar funções, você combina também os privilégios dessas funções. Por exemplo, a Função A tem privilégios de leitura em um objeto base de Endereço e a Função B tem privilégios de criação e atualização nesse objeto. Se a uma conta de usuário estiverem atribuídas as Funções A e B, ela terá privilégios de leitura, de criação e de atualização no objeto base de Endereço. Uma conta de usuário herda os privilégios configurados para qualquer função à qual ela foi atribuída.

Configuração da Função

Você pode criar, editar e excluir funções no MDM Hub .

Nota: Se você usar uma implantação de segurança centralizada abrangente, na qual os usuários são autorizados externamente, não será necessário configurar as funções.

Os privilégios de recurso variam com base no escopo de acesso necessário para que os usuários trabalhem. A prática recomendada para os administradores é seguir o princípio do privilégio mínimo. Atribua aos usuários o nível mais baixo do privilégio necessário para trabalhar.

Adicionando Funções

Para configurar funções e atribuir privilégios de acesso aos recursos do MDM Hub , use a ferramenta Funções no workbench do Gerenciador de Acesso de Segurança.

Sugestão: Evite espaços em nomes de função. Espaços podem causar erros quando o MDM Hub se comunica com o ActiveVOS.

1. Inicie a ferramenta Funções.
2. Adquira um bloqueio de gravação.
3. Aponte em qualquer lugar no painel de navegação, clique com o botão direito do mouse e escolha **Adicionar Função**.

   A ferramenta Funções exibe a caixa de diálogo Adicionar Função.
4. Insira o nome da função.
5. Insira uma descrição opcional da função.
6. Insira um nome externo ou um alias da função.
7. Clique em **OK**.

   A nova função aparece na lista de funções.

Editando e Excluindo Funções

Para editar ou excluir uma função existente, use a ferramenta Funções no workbench do Gerenciador de Acesso de Segurança.

1. Inicie a ferramenta Funções.
2. Adquira um bloqueio de gravação.
3. Role a lista de funções e selecione a função que você deseja editar.
   - Para cada propriedade que você deseja editar, clique no botão **Editar** ao lado dela e especifique o novo valor.
   - Aponte em qualquer lugar no painel de navegação, clique com o botão direito do mouse e escolha **Excluir Função**, e clique em **Sim** quando for solicitada a confirmação.
4. Clique no botão **Salvar** para salvar as alterações.

Privilégios

Com a autorização interna do MDM Hub , você pode atribuir privilégios a funções.

Você pode atribuir os seguintes privilégios a funções:

Leitura

O usuário pode exibir, mas não pode alterar os dados.

Criar

O usuário pode criar registros de dados no Armazenamento de Hub.

Atualizar

O usuário pode atualizar registros de dados no Armazenamento de Hub.

Excluir

O usuário pode excluir registros de dados no Armazenamento de Hub.

Mesclar

O usuário pode mesclar e desfazer a mesclagem de dados.

Executar

O usuário pode executar funções de limpeza e grupos em lote.

Os privilégios determinam o acesso que os usuários de aplicativos externos têm aos recursos do MDM Hub . Por exemplo, você pode configurar uma função para ter privilégios de leitura, criação, atualização e mesclagem em determinados pacotes.

Nota: Cada privilégio é distinta e deve ser explicitamente atribuídos. Privilégios não agregam outros privilégios. Por exemplo, um usuário com acesso de atualização a um recurso não tem necessariamente acesso de leitura a ele. Ambos os privilégios devem ser atribuídos individualmente.

Quando você usa o Console do Hub, os privilégios não são aplicados, embora as configurações ainda afetem o uso do Console do Hub. Por exemplo, os administradores de dados não podem exibir qualquer pacote no Gerenciador de Mesclagem e no Gerenciador de Dados, exceto os quais eles têm privilégios de leitura. Para que os administradores de dados editem e salvem as alterações nos dados em um determinado pacote, eles devem ter privilégios de atualização e criação para o pacote.

Se os administradores de dados não tiverem privilégios de atualização ou criação, eles não poderão alterar quaisquer dados no Gerenciador de Dados. Da mesma forma, um administrador de dados deve ter privilégios de mesclagem para usar o Gerenciador de Mesclagem para mesclar ou desfazer a mesclagem de registros. Para obter mais informações sobre as ferramentas Gerenciador de Mesclagem e Gerenciador de Dados, consulte o *Guia do Administrador de Dados do Multidomain MDM*.

Funções Internas e Funções Externas

Em uma implementação de segurança centralizada baseada em função, você deve criar um mapeamento entre a função interna e a função externa do MDM Hub que é gerenciado separadamente no MDM Hub .

O nome da função externa pode ser diferente do nome da função interna usado em um ambiente do MDM Hub .

Os detalhes da configuração dependem da implementação do mapeamento da função do provedor de segurança. Mapeie funções em um arquivo de configuração. Você pode mapear uma função externa para mais de uma função interna.

Nota: Embora os mapeamentos geralmente sejam criados no XML, não há um formato predefinido para um arquivo de configuração. Ele não pode ser um arquivo XML e nem mesmo um arquivo. O mapeamento é parte do perfil do usuário personalizado ou da implementação do provedor de autenticação. O objetivo do mapeamento é preencher uma lista de funções do objeto de perfil do usuário com IDs de função interna.

Atribuindo Privilégios de Recurso a Funções

Você pode usar a ferramenta Funções no workbench do Gerenciador de Acesso de Segurança para atribuir e editar privilégios de recurso a funções.

1. Inicie a ferramenta Funções.
2. Adquira um bloqueio de gravação.
3. Role a lista de funções e selecione a função à qual você deseja atribuir privilégios de recurso.
4. Clique na guia **Privilégios de Recurso**.
5. Expanda a hierarquia Recursos para mostrar os recursos seguros que você deseja configurar para essa função.
6. Para cada recurso que você desejar configurar:
   - Selecione todos os privilégios que você deseja conceder à essa função.
   - Limpe todos os privilégios que você deseja remover dessa função.
7. Clique no botão **Salvar** para salvar as alterações.

Atribuindo Funções a Outras Funções

Uma função também pode herdar outras funções, exceto uma função à qual ela já pertence. Por exemplo, se você atribuir a Função B à Função A, a Função A herdará os privilégios de acesso da Função B.

1. Inicie a ferramenta Funções.
2. Adquira um bloqueio de gravação.
3. Role a lista de funções e selecione a função à qual você deseja atribuir outras funções.
4. Clique na guia **Funções**.

   A ferramenta Funções exibe as funções que podem ser atribuídas à função selecionada.
5. Selecione todas as funções que você deseja atribuir à função selecionada.
6. Limpe todas as funções que você deseja remover dessa função.
7. Clique no botão **Salvar** para salvar as alterações.

Gerando um Relatório de Privilégios de Recurso para Funções

Você pode gerar um relatório que descreve os privilégios de recurso concedidos a uma determinada função.

1. Inicie a ferramenta Funções.
2. Adquira um bloqueio de gravação.
3. Role a lista de funções e selecione a função para a qual você deseja gerar um relatório.
4. Clique na guia **Relatórios**.
5. Clique em **Gerar**.

   A ferramenta Funções gera o relatório e o exibe na guia Relatório.

Salvando o Relatório Gerado como um Arquivo HTML

1. Clique em **Salvar**.

   A ferramenta Funções solicita que você especifique a localização de destino para o relatório salvo.
2. Navegue até a localização de destino.

3. Clique em **Salvar**.

   O Gerenciador de Acesso de Segurança salva o relatório usando a seguinte convenção de nomenclatura:

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

   em que:

   - *ORS_Name* é o nome do banco de dados de destino.
   - *Role_Name* é a função associada ao relatório gerado.

   A ferramenta Funções salva o relatório atual como um arquivo HTML na localização de destino. Mais tarde, você pode exibir esse relatório usando um navegador.

CAPÍTULO 4

Usuários e Grupos de Usuários

Este capítulo inclui os seguintes tópicos:

Visão Geral de Usuários e Grupos de Usuários

Um usuário do MDM Hub é um indivíduo que pode acessar os recursos do MDM Hub .

As contas de usuário são definidas no Banco de Dados Principais e no Armazenamento de Hub. Para obter uma introdução aos usuários do MDM Hub , consulte o *Guia de Visão Geral do Multidomain MDM*.

Uma conta de usuário ganha acesso aos recursos do MDM Hub usando as funções atribuídas a ele, ao herdar os privilégios configurados para cada função.

Você pode usar a ferramenta Usuários no workbench de Configuração para configurar contas de usuários para os usuários do MDM Hub e também para alterar senhas e ativar a autenticação externa. Os aplicativos externos com autorização suficiente também podem registrar contas de usuário usando solicitações SIF, conforme descrito no *Guia da Estrutura de Integração de Serviços do Multidomain MDM*.

Configuração do Usuário

Você pode criar, editar e excluir usuários no MDM Hub .

Dependendo de como você implantou a segurança, sua implementação do MDM Hub pode exigir a adição de usuários no Banco de Dados Principais.

Você deve configurar os usuários no Banco de Dados Principais nos seguintes cenários:

- Você está usando autorização interna no MDM Hub .
- Você está usando autorização externa com o MDM Hub .
- Vários usuários acessam o Console do Hub usando diferentes contas.

Um usuário precisa ser definido somente uma vez, mesmo se o mesmo usuário for acessar mais de um Armazenamento de Referências Operacionais associado ao Banco de Dados Principais.

Acesso do Usuário aos Recursos do MDM Hub

Os usuários, incluindo administradores e administradores de dados, podem acessar os recursos do MDM Hub das seguintes formas:

Aplicativos MDM

Os usuários podem interagir com o MDM Hub fazendo o logon no Console do Hub e usando as ferramentas às quais eles têm acesso. Os usuários também podem usar o IDD ou a ferramenta de Provisionamento para acessar dados em objetos base e em entidades comerciais.

Aplicativos de Terceiros

Os usuários podem interagir com dados do MDM Hub indiretamente usando os aplicativos de terceiros que usam as classes SIF. Esses usuários nunca fazem logon no Console do Hub. Eles fazer logon no MDM Hub usando os aplicativos que podem invocar as classes SIF. Esses usuários são conhecidos como usuários de aplicativos externos. Para saber mais sobre os tipos de solicitações SIF que os desenvolvedores podem invocar, consulte o *Guia da Estrutura de Integração de Serviços do Multidomain MDM*.

Adicionando Contas de Usuário

Use a ferramenta Usuários no workbench do Gerenciador de Acesso de Segurança para adicionar uma conta de usuário no MDM Hub .

1. Inicie a ferramenta Usuários.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Usuários**.
4. Clique no botão **Adicionar usuário**.

   A ferramenta Usuários exibe a caixa de diálogo **Adicionar Usuário**.
5. Insira um nome, nome do meio e sobrenome para o usuário.
6. Insira um nome para o usuário.

   Nota: Os nomes de usuário não diferenciam maiúsculas de minúsculas e são armazenados como caracteres minúsculos.
7. Insira um endereço de e-mail válido para o usuário. O MDM Hub envia a senha dessa conta de usuário para esse endereço de e-mail.
8. Insira o banco de dados padrão para o usuário. Esse é o banco de dados selecionado por padrão quando o usuário faz logon no Console do Hub.
9. Se a conta de usuário é para um aplicativo, marque a caixa de seleção **Usuário do aplicativo**.

   Nota: Os usuários do aplicativo são usados para autenticação baseada em certificado de solicitações que são geradas por um aplicativo confiável em nome do usuário.
10. Insira e verifique uma senha para o usuário.
11. Escolha o tipo de autenticação.
    - Marque a caixa de seleção **Usar autenticação externa** se a sua implementação do MDM Hub usar a autenticação por meio de um provedor de segurança de terceiros.
    - Desmarque a caixa de seleção **Usar autenticação externa** se você deseja usar a autenticação interna no MDM Hub .

12. Procure um certificado público para o usuário. Esse certificado pode ser usado pelo MDM Hub para autenticação das solicitações do usuário.

    Nota: Se a conta de usuário for para um usuário do aplicativo, você deverá selecionar um certificado.

13. Clique em **OK**.

    A ferramenta Usuários adiciona o novo usuário à lista de usuários na guia **Usuários**.

Editando e Excluindo Contas de Usuário

Você pode usar a ferramenta Usuários no workbench do Gerenciador de Acesso de Segurança para editar ou remover as contas de usuário.

1. Inicie a ferramenta Usuários.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Usuários**.
4. Se você deseja excluir um usuário, selecione a conta de usuário que você deseja remover.
5. Clique no botão **Excluir**.

   A ferramenta Usuários solicita que você confirme a exclusão.

6. Clique em **Sim** para confirmar a exclusão.

   A ferramenta Usuários remove a conta do usuário excluído da lista de usuários.

7. Se você deseja editar um usuário, selecione a conta de usuário que você deseja configurar.
8. Para alterar um nome, clique duas vezes na célula e digite um nome diferente.
9. Se você desejar, selecione um banco de dados de logon e um servidor diferentes.
10. Marque a caixa de seleção **Administrador** para dar a esse usuário acesso administrativo, que permite acesso às ferramentas do Console do Hub e a todos os bancos de dados.
11. Marque a caixa de seleção **Ativar** para ativar essa conta de usuário e permitir que esse usuário faça logon.

    Nota: Se você usar a autenticação externa para um usuário, não poderá desativar a conta de usuário por meio do Console do Hub.

12. Clique no botão **Salvar**.

    A ferramenta Usuários salva as alterações na conta de usuário.

Editando Informações Complementares do Usuário

Você pode usar o MDM Hub para gerenciar informações complementares de cada usuário, como números de telefone ou endereços de e-mail. O MDM Hub não exige que você forneça essas informações, o MDM Hub não usa essas informações de maneira especial.

Nota: Não é possível alterar o endereço de e-mail do usuário `admin` no Console do Hub. Para alterar o endereço de e-mail do usuário administrador, atualize a entrada do usuário administrador diretamente na tabela C_REPOS_USER no esquema CMX_SYSTEM.

1. Inicie a ferramenta Usuários.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Usuários**.
4. Selecione o usuário cujas propriedades você deseja editar.
5. Clique no botão **Editar**.

A ferramenta Usuários exibe a caixa de diálogo **Editar Usuário**.

6. Especifique qualquer uma das propriedades do usuário, como título, endereço de e-mail ou mensagens de logon. A mensagem de logon é a mensagem que o Console do Hub exibe depois que esse usuário faz logon.
7. Clique em **OK**.
8. Clique no botão **Salvar** para salvar as alterações.

Alterando Configurações de Senha para Contas de Usuário

Você pode alterar as configurações de senha para um usuário. As últimas informações sobre a senha mais recente e quem alterou a senha são mantidas. O histórico de senhas não está disponível.

1. Inicie a ferramenta Usuários.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Usuários**.
4. Selecione o usuário cuja senha você deseja alterar.
5. Clique no botão **Alterar Senha**.

   A ferramenta Usuários exibe a caixa de diálogo **Alterar Senha** para o usuário selecionado.
6. Especifique e verifique a nova senha.
7. Escolha o tipo de autenticação.
   - Marque a caixa de seleção **Usar autenticação externa** se a sua implementação do MDM Hub usar a autenticação por meio de um provedor de segurança de terceiros.
   - Desmarque a caixa de seleção **Usar autenticação externa** se você deseja usar a autenticação interna no MDM Hub .
8. Clique em **OK**.

Configurando o Acesso do Usuário ao Armazenamento de Referências Operacionais

Você pode configurar o acesso do usuário aos bancos de dados do Armazenamento de Referências Operacionais.

1. Inicie a ferramenta Usuários.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Banco de Dados de Destino**.

   A ferramenta Usuários exibe a guia Banco de Dados de Destino.
4. Expanda cada nó de banco de dados para ver quais usuários podem acessar esse banco de dados.
5. Para alterar as atribuições de usuário para um banco de dados, clique com o botão direito do mouse no nome do banco de dados e escolha **Atribuir Usuário**.

   A ferramenta Usuários exibe a caixa de diálogo **Atribuir Usuário ao Banco de Dados**.
6. Marque os nomes dos usuários que você deseja atribuir ao banco de dados selecionado.
7. Desmarque os nomes dos usuários que você não deseja atribuir ao banco de dados selecionado.
8. Clique em **OK**.

Configuração da Diretiva de Senha

Você pode definir políticas globais de senha para todos os usuários. Configure políticas de senha privadas para substituir políticas de senha globais para usuários individuais. Todas as senhas diferenciam maiúsculas de minúsculas.

Nota: se você implantar o MDM Hub no servidor de aplicativos JBoss com segurança ativada, verifique se a senha definida atende à diretiva de senha do JBoss. A senha também deve atender à diretiva de senha global do MDM Hub . Isso é importante porque as senhas para o Console do Hub e para o JBoss devem ser correspondentes.

Configurações da Diretiva de Senha

Você pode especificar configurações de diretiva de senha para os usuários do MDM Hub .

O MDM Hub permite que você defina usuários para as seguintes diretivas de senha privadas:

Comprimento da Senha

Comprimento mínimo e máximo de uma senha em caracteres.

Expiração da Senha

Especifica se uma senha expira ou não e o número de dias que uma senha é válida.

Marque a caixa de seleção **Expiração da senha** para definir um período de expiração para senhas. Desmarque a caixa de seleção **Expiração da senha** para definir as senhas que não expiram.

Se você marcar a caixa de seleção **Expiração da senha**, especifique o número de dias que a senha deve expirar. O período mínimo de expiração de senha que você pode definir é `10`.

Configurações de Logon

Número de logons permitidos e número máximo de logons com falha permitidos.

Histórico de Senhas

Número de vezes que uma senha pode ser reutilizada.

Requisitos de Senha

Marque a caixa de seleção **Padrão de validação de senha ativado** para impor uma senha padrão. Você pode especificar os seguintes critérios para o padrão de senha:

- Número mínimo de caracteres exclusivos
- A senha deve começar com
- A senha deve conter
- A senha deve terminar com

Gerenciando a Diretiva de Senha Global

A diretiva de senha global se aplica aos usuários que não têm diretivas de senha privada especificadas para eles.

1. Inicie a ferramenta **Usuários**.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Diretiva de Senha Global**.

   A janela Diretiva de Senha Global é exibida.

4. Especifique as configurações de diretiva de senha.
5. Clique em **OK**.
6. Clique no botão **Salvar** para salvar as configurações globais.

Gerenciando as Diretivas de Senha Privadas

É possível especificar uma diretiva de senha particular que substitua a diretiva de senha global para qualquer usuário.

Nota: As práticas recomendadas para o gerenciamento de diretivas de senha é para garantir que a maioria das senhas de usuário seja gerenciada por uma diretiva global em vez de várias diretivas privadas.

1. Inicie a ferramenta Usuários.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Usuários**.
4. Selecione o usuário para o qual você deseja definir a diretiva de senha particular.
5. Clique em **Gerenciar diretiva de senha**.

   É exibida a janela **Diretiva de Senha Particular** do usuário selecionado.
6. Ative a opção **Diretiva de senha particular ativada**.
7. Especifique as configurações de diretiva de senha para o usuário.
8. Clique em **OK**.
9. Clique no botão **Salvar** para salvar as alterações.

Configuração de Segurança das Fontes de Dados JDBC

Nas implementações do MDM Hub , se uma fonte de dados JDBC usar a segurança do servidor de aplicativos, você deverá definir as configurações no arquivo cmxserver.properties.

Você deve armazenar o nome de usuário e a senha do servidor de aplicativos para a fonte de dados JDBC no arquivo cmxserver.properties. As senhas não podem aparecer como texto simples. Você deve criptografar as senhas antes de salvá-las no arquivo cmxserver.properties.

Para aprender mais sobre origens de dados JDBC protegidas, consulte a documentação do servidor de aplicativos.

Nomes de Usuários e Senhas para uma Fonte de Dados JDBC Protegida

Para configurar nomes de usuários e senhas para uma origem de dados JDBC protegida no arquivo de cmxserver.properties, use os seguintes parâmetros:

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

Onde databaseId é o identificador exclusivo da origem de dados JDBC.

ID do Banco de Dados para Tipos de Conexão Oracle SID

Para um tipo de conexão Oracle SID, o databaseId consiste nas seguintes strings:

```
<nome do host do banco de dados>-<Oracle SID>-<nome do esquema>
```

Por exemplo, com as seguintes configurações:

- `<nome do host do banco de dados>` = `localhost`
- `<Oracle SID>` = `MDMHUB`
- `<nome do esquema>` = `Test_ORS`

as propriedades da senha e do nome de usuário seriam:

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

ID do Banco de Dados para Tipos de Conexão de Serviço Oracle

Para um tipo de conexão de Serviço Oracle, o databaseId consiste nas seguintes strings:

```
<nome do serviço>-<nome do esquema>
```

Por exemplo, com as seguintes configurações:

- `<nome do serviço>` = `MDM_Service`
- `<nome do esquema>` = `Test_ORS`

as propriedades da senha e do nome de usuário seriam:

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

ID do Banco de Dados para Tipos de Conexão do IBM DB2

Para um tipo de conexão do IBM DB2, o databaseId consiste nas seguintes strings:

```
<nome do host do banco de dados>-<nome do banco de dados>-<nome do esquema>
```

Por exemplo, com as seguintes configurações:

- `<nome do host do banco de dados>` = `localhost`
- `<nome do banco de dados>` = `dsui2`
- `<nome do esquema>` = `DS_UI2`

as propriedades da senha e do nome de usuário seriam:

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

ID do Banco de Dados para Tipos de Conexão do Microsoft SQL Server

Para um tipo de conexão Microsoft SQL Server, o databaseId consiste nas seguintes strings:

```
<nome do host do banco de dados>-<nome do banco de dados>
```

Por exemplo, com as seguintes configurações:

- `<nome do host do banco de dados>` = `localhost`
- `<nome do banco de dados>` = `ds_ui1`

as propriedades da senha e do nome de usuário seriam:

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

ID do Banco de Dados para o Banco de Dados Principais

Se você deseja proteger a fonte de dados JDBC que acessa o Banco de Dados Principais, o `databaseId` será CMX_SYSTEM. Nesse caso, as propriedades seriam:

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

Criptografia de Senha

Para gerar uma senha criptografada para um esquema de banco de dados, use os seguintes comandos:

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

Configuração do Grupo de Usuários

Um grupo de usuários é uma coleção lógica de contas de usuário.

Os grupos de usuários simplificam a administração de segurança. Por exemplo, você pode combinar usuários de aplicativos externos em um grupo de usuários e conceder funções de segurança para o grupo de usuários em vez de para cada usuário individual. Além de usuários, os grupos de usuários podem conter outros grupos de usuários.

Use a guia Grupos na ferramenta Usuários e Grupos no workbench do Gerenciador de Acesso de Segurança para configurar grupos de usuários.

Iniciando a Ferramenta Usuários e Grupos

Você inicia a ferramenta Usuários e Grupos no Console do Hub.

1. No Console do Hub, conecte-se a um Armazenamento de Referências Operacionais, caso ainda não o tenha feito.
2. Expanda o workbench do Gerenciador de Acesso de Segurança e clique em **Usuários e Grupos**.

   O Console do Hub exibe a ferramenta Usuários e Grupos.

   A ferramenta Usuários e Grupos contém as seguintes guias:

   Grupos

   Usado para definir grupos de usuários e atribuir usuários a grupos de usuários.

   Usuários Atribuídos ao Banco de Dados

   Usado para associar contas de usuário a um banco de dados.

   Atribuir Usuários/Grupos à Função

   Usado para associar usuários e grupos de usuários com funções.

   Atribuir Funções a um Usuário/Grupo

   Usado para associar funções a usuários e grupos de usuários.

Adicionando Grupos de Usuários

Você pode usar a ferramenta Usuários e Grupos no workbench do Gerenciador de Acesso de Segurança para adicionar grupos de usuários.

1. Inicie a ferramenta Usuários e Grupos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Grupos**.
4. Clique no botão **Adicionar**.

   A ferramenta Usuários e Grupos exibe a caixa de diálogo **Adicionar Grupo de Usuários**.
5. Insira um nome descritivo para o grupo de usuários.
6. Opcionalmente, insira uma descrição do grupo de usuários.
7. Clique em **OK**.

   A ferramenta Usuários e Grupos adiciona o novo grupo de usuários à lista.

Editando e Excluindo Grupos de Usuários

Você também pode usar a ferramenta Usuários e Grupos para editar ou remover grupos de usuários.

1. Inicie a ferramenta Usuários e Grupos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Grupos**.
4. Role a lista de grupos de usuários e selecione o grupo de usuários que você deseja editar.
5. Se você deseja remover um grupo de usuários, clique no botão **Excluir**.

   A ferramenta de Usuários e grupos solicita que você confirme a exclusão.
6. Clique em **Sim**.

   A ferramenta de Usuários e grupos remove o grupo de usuários excluído grupo da lista.
7. Se você deseja editar um grupo de usuários, clique no botão **Editar** ao lado de cada propriedade que você deseja editar e especifique o novo valor.
8. Clique no botão **Salvar** para salvar as alterações.

Atribuindo Usuários e Grupos de Usuários a Grupos de Usuários

Para atribuir membros a um grupo de usuários:

1. Inicie a ferramenta Usuários e Grupos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Grupo**.
4. Role a lista de grupos de usuários e selecione o grupo de usuários que você deseja editar.
5. Clique com o botão direito do mouse no grupo de usuários que você acabou de criar e escolha **Atribuir Usuários e Grupos**.

   A ferramenta Usuários e Grupos exibe a caixa de diálogo **Atribuir ao Grupo de Usuários**.
6. Marque os nomes dos usuários e grupos de usuários que você deseja atribuir ao grupo de usuários selecionado.
7. Desmarque os nomes dos usuários e grupos de usuários que você não deseja atribuir ao grupo de usuários selecionado.

8. Clique em **OK**.

Atribuindo Usuários ao Banco de Dados ORS Atual

Para atribuir usuários ao atual banco da dados do Armazenamento de Referências Operacionais:

1. Inicie a ferramenta Usuários e Grupos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Usuários Atribuídos ao Banco de Dados**.
4. Clique no botão **Atribuir usuários ao banco de dados** para atribuir usuários a um banco de dados do Armazenamento de Referências Operacionais.

   A ferramenta Usuários e Grupos exibe a caixa de diálogo **Atribuir Usuário ao Banco de Dados**.
5. Marque os nomes dos usuários que você deseja atribuir ao banco de dados do Armazenamento de Referências Operacionais selecionado.
6. Desmarque os nomes dos usuários que você não deseja atribuir ao banco de dados do Armazenamento de Referências Operacionais selecionado.
7. Clique em **OK**.

Associações entre Funções, Usuários e Grupos de Usuários

Você pode associar funções a usuários e grupos de usuários. Você pode usar a ferramenta **Usuários e Grupos** para associar funções a usuários das seguintes maneiras:

- Atribuir usuários e grupos de usuários a funções.
- Atribuir funções a usuários e grupos de usuários.

Escolha a maneira mais adequada à sua implementação.

Atribuindo Usuários e Grupos de Usuários a Funções

Para atribuir usuários e grupos de usuários a uma função:

1. Inicie a ferramenta Usuários e Grupos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Atribuir Usuários/Grupos a Função**.
4. Selecione a função à qual deseja atribuir usuários e grupos de usuários.
5. Clique no botão **Editar**.

   A ferramenta Usuários e Grupos exibe a caixa de diálogo **Atribuir Usuários à Função**.
6. Marque os nomes dos usuários e grupos de usuários que você deseja atribuir à função selecionada.
7. Desmarque os nomes dos usuários e grupos de usuários que você não deseja atribuir à função selecionada.
8. Clique em **OK**.

Atribuindo Funções a Usuários e Grupos de Usuários

Para atribuir funções a usuários e grupos de usuários:

1. Inicie a ferramenta Usuários e Grupos.
2. Adquira um bloqueio de gravação.
3. Clique na guia **Atribuir Funções ao Usuário/Grupo**.
4. Selecione o usuário ou o grupo de usuários ao qual você deseja atribuir funções.
5. Clique no botão **Editar**.

   A ferramenta Usuários e Grupos exibe a caixa de diálogo **Atribuir Funções ao Usuário**.
6. Marque as funções que você deseja atribuir ao usuário selecionado ou ao grupo de usuários.
7. Desmarque as funções que você não deseja atribuir ao usuário selecionado ou ao grupo de usuários.
8. Clique em **OK**.

CAPÍTULO 5

Provedores de Segurança

Este capítulo inclui os seguintes tópicos:

Visão Geral dos Provedores de Segurança

Um provedor de segurança é um aplicativo de terceiros que oferece serviços de segurança, como autenticação e autorização, para os usuários que acessam o MDM Hub . Os provedores de segurança fazem parte de alguns cenários de implantação de segurança do MDM Hub .

Um arquivo de provedor contém informações de perfil de um provedor de segurança. Se você deseja usar outros provedores de segurança de terceiros, use a ferramenta Provedores de Segurança para carregar arquivos de provedor no MDM Hub . Você também pode usar a ferramenta Provedores de Segurança para modificar, excluir, ativar ou desativar os provedores de segurança na lista de Provedores.

O MDM Hub vem com um conjunto de provedores internos de segurança padrão. Você também pode adicionar os provedores de segurança de terceiros. Os provedores internos de segurança não podem ser removidos.

Gerenciamento de Provedor de Segurança

Você pode gerenciar os provedores de segurança na implementação do MDM Hub por meio da ferramenta Provedores de Segurança no workbench de Configuração do Console do Hub.

Você pode adicionar os provedores de segurança da seleção interna padrão no MDM Hub ou da sua própria seleção de provedores adicionados de forma personalizada. Os provedores internos de segurança não podem ser removidos.

O MDM Hub dá suporte aos seguintes tipos de provedores de segurança:

Provedor de autenticação

Autentica um usuário validando sua identidade. Informa o MDM Hub que os usuários são quem dizem ser. Esse tipo de provedor de segurança não valida se os usuários têm os privilégios necessários para acessar determinados recursos do MDM Hub .

Provedor de autorização

Informa o MDM Hub se os usuários têm os privilégios necessários para acessar determinados recursos do MDM Hub .

Provedor de perfil do usuário

Informa o MDM Hub sobre usuários individuais, como atributos específicos de usuário e as funções para as quais o usuário pertence.

Os provedores internos representam implementações internas do MDM Hub para autenticação, autorização e serviços de perfil do usuário.

Alguns dos provedores padrão do MDM Hub são superprovedores. Os superprovedores sempre retornam uma resposta positiva para solicitações de autenticação e autorização. Use um superprovedor em um ambiente de desenvolvimento quando você não quiser configurar usuários, funções e privilégios. Os superprovedores também podem ser usados em um ambiente de produção no qual a segurança é fornecida como uma camada em acréscimo às solicitações SIF para ganhos de desempenho.

Gerenciamento do Arquivo de Provedor

Um arquivo de provedor contém informações de perfil de um provedor de segurança.

Se você desejar usar seus próprios provedores de segurança de terceiros, deverá registrá-los explicitamente na ferramenta de Provedores de Segurança. Para registrar um provedor de segurança, carregue um arquivo de provedor que contém as informações de perfil necessárias para o registro.

Um arquivo de provedor é um arquivo JAR que contém os seguintes dados:

- Um manifesto que descreve um ou mais provedores de segurança externos. Cada provedor de segurança tem as seguintes configurações:
  - Nome do Provedor
  - Descrição do Provedor
  - Provider Type
  - Nome da Classe de Fábrica do Provedor
  - Propriedades que especificam detalhes da configuração do provedor. Isso pode ser uma lista de pares de nome e valor: nomes de propriedade com valores padrão.
- Implementação do provedor e qualquer biblioteca de terceiros necessária.

O InformaticaKit de Recursos copia uma implementação de amostra de um arquivo de provedor no Servidor de hub. Para obter mais informações sobre o arquivo de provedor de amostra, consulte o *Guia do Kit de Recursos do Multidomain MDM*.

Carregando um Arquivo de Provedor

Carregue um arquivo de provedor para adicionar ou atualizar as informações do provedor.

1. Inicie a ferramenta Provedores de Segurança.

2. Adquira um bloqueio de gravação.
3. No painel de navegação esquerdo, clique com o botão direito do mouse e escolha **Carregar Arquivo do Provedor**.

   A ferramenta Provedor de Segurança solicita que você selecione o arquivo JAR para esse provedor.
4. Especifique o arquivo JAR, navegando pelo sistema de arquivos conforme necessário e selecionando o arquivo JAR que você deseja carregar.
5. Clique em **Abrir**.

   A ferramenta Provedor de Segurança verifica o arquivo selecionado para determinar se ele é um arquivo de provedor válido.
6. Se o arquivo de provedor que você carregou tiver o mesmo nome que um arquivo de provedor existente, a ferramenta Provedor de Segurança perguntará se deseja substituir o arquivo de provedor existente. Clique em **Sim** para confirmar.

   A ferramenta Provedor de Segurança preenche a lista de Provedores com as informações adicionais do provedor. Depois de carregar o arquivo de provedor, você pode remover o arquivo original do sistema de arquivos.

Excluindo um Arquivo do Provedor

É possível excluir um arquivo de provedor se você já não usar o provedor de segurança.

1. Inicie a ferramenta Provedores de Segurança.
2. Adquira um bloqueio de gravação.
3. No painel de navegação esquerdo, clique com o botão direito do mouse no arquivo do provedor que você deseja excluir e escolha **Excluir Arquivo do Provedor**.

   A ferramenta Provedor de Segurança solicita que você confirme a exclusão.
4. Clique em **Sim**.

   A ferramenta Provedor de Segurança remove o arquivo do provedor excluído da lista.

   Nota: você não pode excluir os arquivos internos do provedor que acompanham o MDM Hub .

Configurações do Provedor de Segurança

A ferramenta Provedores de Segurança exibe uma lista de provedores registrados.

A lista de provedores registrados é classificada pelo tipo de provedor. A sequência de provedores na lista Provedores também representa a ordem na qual eles são invocados. Um usuário precisa ser autenticado pelo menos por um provedor na lista de Provedores.

Por exemplo, quando você tenta fazer logon e fornece o nome de usuário e a senha, o MDM Hub envia suas credenciais de logon a cada provedor de autenticação na lista de autenticação. O MDM Hub continua sequencialmente pela lista. Se a autenticação for bem-sucedida com um dos fornecedores na lista, o MDM Hub autenticará você. Se a autenticação falhar com todos os provedores de autenticação disponíveis, você não será autenticado.

Alterando as Configurações do Provedor de Segurança

Para alterar as configurações de um provedor de segurança, realize as seguintes etapas:

1. Inicie a ferramenta Provedores de Segurança.
2. Adquira um bloqueio de gravação.
3. Selecione o provedor de segurança que você deseja modificar.
4. No painel Propriedades, clique no botão **Editar** ao lado de qualquer configuração que você deseja editar.
5. Clique no botão **Salvar** para salvar as alterações.

Ativar e desativar os provedores de segurança

1. Adquira um bloqueio de gravação.
2. Selecione o provedor de segurança que você deseja ativar ou desativar.
   - Marque a caixa de seleção **Ativado** para ativar um provedor de segurança desativado.
   - Desmarque a caixa de seleção **Ativado** para desativar um provedor de segurança.

   Uma vez desativado, o nome do provedor fica indisponível e se move até o final da lista de Provedores. Você não pode reorganizar os provedores desativados na lista de Provedores.
3. Clique no botão **Salvar** para salvar as alterações.

Movendo um Provedor de Segurança na Ordem de Processamento

O MDM Hub processa os provedores de segurança na ordem em que aparecem na lista de Provedores. Você pode reorganizar a ordem na qual os provedores de segurança são exibidos.

1. Inicie a ferramenta Provedores de Segurança.
2. Adquira um bloqueio de gravação.
3. Para mover um provedor para cima, clique com o botão direito do mouse no provedor que você deseja mover e selecione **Mover Provedor para Cima**.

   A ferramenta Provedor de Segurança move o provedor para cima do anterior na lista de Provedores e atualiza o painel de navegação.
4. Para mover um provedor para baixo, clique com o botão direito do mouse no provedor que você deseja mover e selecione **Mover Provedor para Baixo**.

   A ferramenta Provedor de Segurança move o provedor para baixo do anterior na lista de Provedores e atualiza o painel de navegação.

Propriedades do Provedor

O painel Provedor contém os seguintes campos:

Nome

Nome deste provedor de segurança.

Descrição

Descrição deste provedor de segurança.

Provider Type

Tipo de provedor de segurança. O tipo pode ser um dos seguintes valores:

- Autenticação
- Autorização
- Perfil do Usuário

Arquivo de Provedor

Nome do arquivo de provedor associado a este provedor de segurança, ou **Provedor Interno** para provedores internos.

Ativado

Indica se este provedor de segurança está ativado ou não. Um provedor de segurança ativado está marcado. Um provedor de segurança desativado não está marcado. Observe que provedores internos não podem ser desativados.

Propriedades

Propriedades adicionais para esse provedor de segurança, se definidas pelo provedor de segurança. Cada propriedade é um par de nome e valor. Um provedor de segurança pode exigir ou permitir propriedades exclusivas que você pode especificar aqui.

Adicionando Propriedades do Provedor

Para adicionar as propriedades do provedor, execute as etapas a seguir.

1. Inicie a ferramenta Provedores de Segurança.
2. Adquira um bloqueio de gravação.
3. No painel de navegação, selecione o provedor de autenticação no qual você deseja adicionar as propriedades.
4. Clique no botão **Adicionar**.

   A ferramenta Provedores de Segurança exibe a caixa de diálogo Adicionar Propriedade do Provedor.
5. Especifique o nome da propriedade.
6. Especifique o valor a ser atribuído a essa propriedade.
7. Clique em **OK**.

Editando propriedades do provedor

Para editar uma propriedade de provedor existente, realize as seguintes etapas.

1. Inicie a ferramenta Provedores de Segurança.
2. Adquira um bloqueio de gravação.
3. No painel de navegação, selecione o provedor de autenticação no qual você deseja editar as propriedades.
4. Para cada propriedade que você deseja editar, clique no botão **Editar** ao lado dela e especifique o novo valor.
5. Clique no botão **Salvar** para salvar as alterações.

Provedores Personalizados

Você pode empacotar classes de provedor personalizadas no arquivo JAR ou ZIP que formam o arquivo do provedor.

Especifique as configurações dos provedores personalizados no arquivo `providers.properties`. Em seguida, coloque o arquivo no JAR no diretório META-INF. As configurações são convertidas pelo carregador e são exibidas no Console do Hub.

Um arquivo provider.properties tem os seguintes elementos:

ProviderList

A lista separada por vírgula dos nomes de provedor contidos.

File-Description

A descrição do pacote.

XXX-Provider-Name

Nome de exibição do provedor *XXX*.

XXX-Provider-Description

Descrição do provedor *XXX*.

XXX-Provider-Type

Tipo do provedor *XXX*. Os valores possíveis são `USER_PROFILE_PROVIDER`, `JAAS_LOGIN_MODULE` e `AUTHORIZATION_PROVIDER`.

XXX-Provider-Factory-Class-Name

Classe de implementação do provedor, que também está no mesmo arquivo JAR ou ZIP.

XXX-Provider-Properties

Lista separada por vírgula de pares de nome/valor que define as propriedades do provedor.

Nota: O arquivo morto do provedor deve conter todas as classes necessárias para que o provedor personalizado seja funcional, além dos recursos necessários. Esses recursos são específicos da sua implementação.

Arquivo providers.properties de Amostra

Nota: Todas as configurações são necessárias exceto *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
```

Autenticação Externa

Você pode usar a autenticação externa com o MDM Hub para usuários por meio do Serviço de Autenticação e Autorização Java (JAAS).

MDM Hub oferece modelos para os seguintes tipos de padrões de autenticação:

- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory
- Autenticação de rede usando o protocolo Kerberos

Esses modelos fornecem as configurações, como os protocolos, nomes de servidor e portas, que são necessárias para esses padrões de autenticação. Você pode usar esses modelos para adicionar um novo módulo de logon com as configurações que precisar. Para obter mais informações sobre esses padrões de autenticação, consulte a documentação do fornecedor aplicável.

Adicionando um Módulo de Logon

Para configurar a autenticação externa no MDM Hub , você deve criar um módulo de logon.

1. Inicie a ferramenta Provedores de Segurança.
2. Adquira um bloqueio de gravação.
3. Clique com o botão direito do mouse em Provedores de Autenticação (Módulos de Logon) e selecione **Adicionar Módulo de Logon**.

   A ferramenta Provedores de Segurança exibe a caixa de diálogo Adicionar Módulo de Logon.
4. Clique na seta para baixo e selecione um modelo para o módulo de logon.

   OpenLDAP-template

   Baseado nas propriedades de autenticação LDAP.

   MicrosoftActiveDirectory-template

   Baseado nas propriedades de autenticação do Active Directory.

   Kerberos-template

   Baseado nas propriedades de autenticação Kerberos.
5. Clique em **OK**.

   A ferramenta Provedores de Segurança adiciona o novo módulo de logon à lista.
6. No painel Propriedades, clique no botão **Editar** ao lado de qualquer propriedade que você deseja editar. Especifique as configurações para o tipo do módulo de logon que você deseja criar.
7. Clique no botão **Salvar** para salvar as alterações.

Excluindo um Módulo de Logon

Você pode excluir um módulo de logon, se desejar.

1. Inicie a ferramenta Provedores de Segurança.
2. Adquira um bloqueio de gravação.
3. No painel de navegação, clique com o botão direito do mouse em um módulo de logon em Provedores de Autenticação (Módulos de Logon) e escolha **Excluir Módulo de Logon**.

   A ferramenta Provedor de Segurança solicita que você confirme a exclusão.
4. Clique em **Sim**.

   A ferramenta Provedor de Segurança remove o módulo de logon excluído da lista e atualiza o painel de navegação esquerdo.

CAPÍTULO 6

Segurança em nível de aplicativo

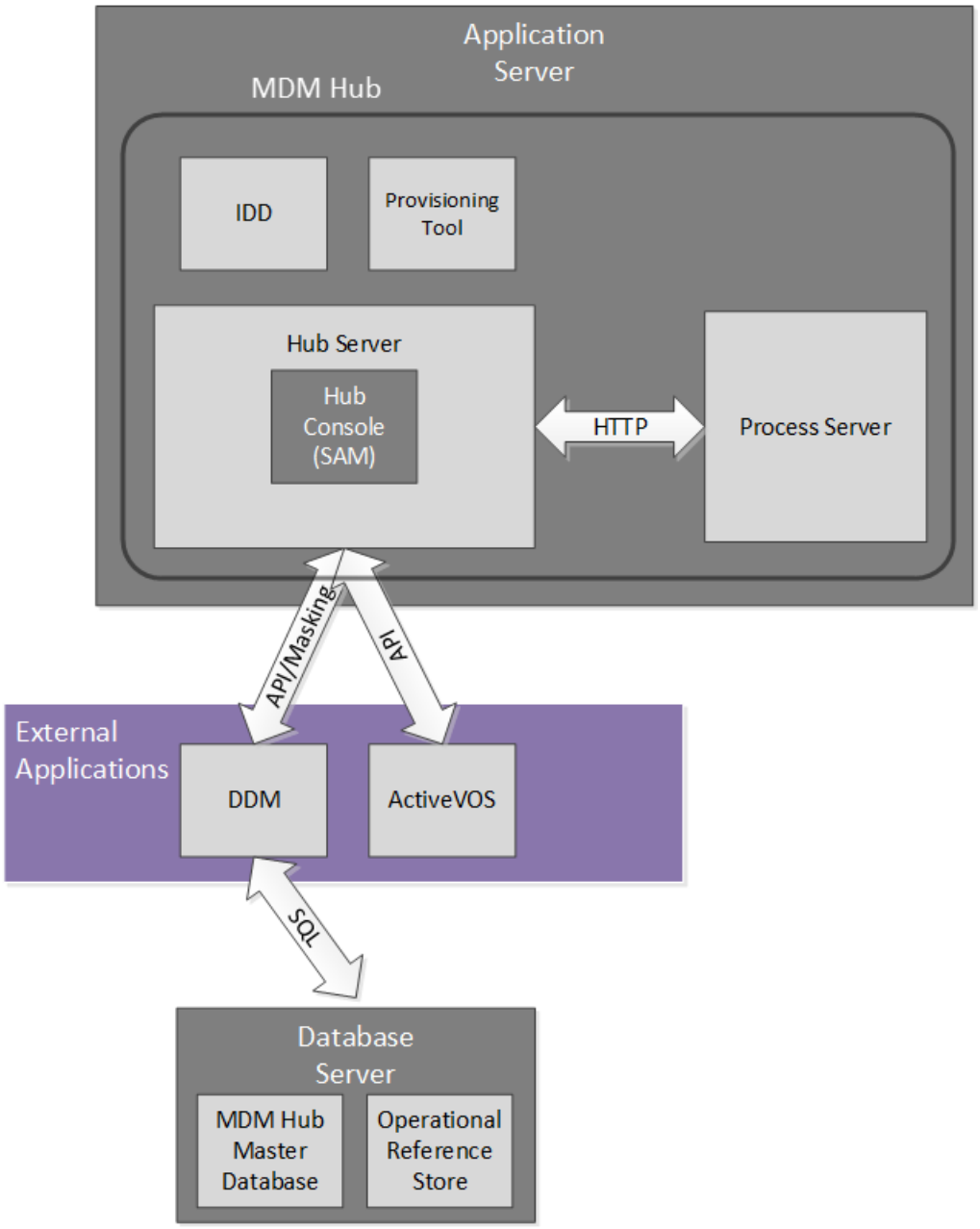
Este capítulo inclui os seguintes tópicos:

Visão geral de segurança no nível de aplicativo

O Gerenciador de Acesso de Segurança (SAM) é o módulo de segurança do MDM Hub, que controla credenciais e funções de usuários. Outros aplicativos e componentes em uma implementação do MDM Hub também têm configurações de segurança para garantir que eles se comuniquem com o MDM Hub de maneira segura. Por exemplo, você pode configurar a segurança em nível de dados para o Informatica Data Director.

A Informatica realiza testes de segurança internos de produtos Informatica. Por exemplo, a Informatica usa aplicativos de verificação padrão do setor para testar produtos em busca de vulnerabilidades de segurança, como ataques de injeção de SQL. Outros aplicativos de segurança Informatica, usados em conjunto com o SAM, adicionam uma camada extra de segurança a uma implementação do MDM Hub. O Informatica Dynamic Data Masking (DDM) aplica uma máscara de dados para impedir o acesso não autorizado a informações confidenciais. A ferramenta de Provisionamento do Informatica MDM e o Informatica ActiveVOS não são aplicativos de segurança, mas ainda se comunicam com segurança com o MDM Hub.

A imagem a seguir mostra um exemplo de implementação do MDM Hub e de como os componentes se conectam uns com os outros:



Informatica Data Director

O Informatica Data Director um aplicativo de gerenciamento de dados baseado na Web para o MDM Hub. Quando você configura um aplicativo do Data Director, os usuários comerciais podem criar, gerenciar, consumir e monitorar dados principais.

O Informatica Data Director adere às dez principais recomendações de segurança do OWASP (Open Web Application Security Project). A Informatica usa o IBM Security AppScan para testar vulnerabilidades de segurança, como um ataque de injeção de SQL. Os métodos HTTP GET ou POST podem recuperar informações do IDD, mas outros métodos HTTP, como DELETE e PUT, retornam um erro HTTP.

Ao configurar um aplicativo do Data Director, você pode organizar as tabelas no Armazenamento de Referências Operacionais em entidades comerciais ou em áreas de assunto. Ambas as abordagens fornecem uma maneira de agrupar dados relacionados que você deseja tratar como uma unidade, como todos os dados sobre um cliente. Entidades comerciais são a abordagem organizacional recomendada desde o MDM Multidomínio Versão 10.1. Elas são o núcleo da estrutura do Entity 360, que inclui serviços de entidades comerciais e exibições de entidades modernas.

Para a segurança dos dados, um aplicativo do Data Director usa as funções de usuário e os privilégios de recursos definidos no Armazenamento de Referências Operacionais. Lembre-se de que um administrador do MDM usa o workbench do Gerenciador de Acesso de Segurança no Console do Hub para definir privilégios de recursos para cada função de usuário. Em um aplicativo do Data Director, os usuários podem realizar as operações permitidas por sua função de usuário.

Os privilégios de função para entidades comerciais e áreas de assunto são derivados dos privilégios de recursos de diferentes maneiras e, portanto, a segurança pode ser um pouco diferente. No entanto, ambas as abordagens são igualmente seguras. Para obter mais informações sobre segurança para entidades comerciais, consulte o *Guia da Ferramenta de Provisionamento do Multidomain MDM*. Para obter mais informações sobre a configuração da segurança e a segurança dos dados para áreas de assunto, consulte o *Guia de Implementação do Multidomain MDM Data Director*.

Ferramenta de Provisionamento

Use a ferramenta de Provisionamento para criar modelos de entidade comercial com base nas informações de esquema definidas em um Armazenamento de referências operacionais (ORS). O modelo de entidade comercial é um componente fundamental da estrutura do Entity 360 no Data Director.

Você deve fazer login na ferramenta de Provisionamento antes de poder configurar entidades comerciais.

Como você trabalha em arquivos de configuração, salve as alterações em um espaço de trabalho temporário. A ferramenta de Provisionamento não aplicará as alterações até que você as publique. Se vários usuários alterarem a configuração da entidade comercial para um ORS simultaneamente, o MDM Hub será atualizado com a configuração publicada mais recentemente.

A ferramenta de Provisionamento deve estar em execução no mesmo servidor de aplicativos que o Servidor de Hub.

Para obter mais informações, consulte o *Guia da Ferramenta de Provisionamento do Multidomain MDM*.

ActiveVOS

Informatica ActiveVOS® é uma ferramenta de gerenciamento de processos comerciais (BPM) que ajuda você a automatizar processos comerciais. Você pode criar modelos de processos que integram pessoas, processos e sistemas, aumentando assim a eficiência dos seus negócios.

É possível usar o ActiveVOS para garantir que dados de entidade atualizados passem por um fluxo de trabalho de aprovação de alterações antes que os registros atualizados contribuam para os registros da Melhor Versão da Verdade (BVT). Por exemplo, um processo comercial pode exigir que um gerente sênior revise e aprove atualizações em dados de clientes antes que eles se tornem dados principais.

Para oferecer suporte a um fluxo de trabalho de aprovação de alterações, o MDM Hub e o Data Director se integram ao ActiveVOS Server. Fluxos de trabalho do MDM, tipos de tarefa e funções predefinidos permitem

que componentes sejam sincronizados uns com os outros. É possível configurar sua implementação do MDM para trabalhar com o ActiveVOS Server incorporado. Como alternativa, você pode executar uma instância independente do ActiveVOS no seu ambiente.

O ActiveVOS incorporado autentica solicitações do Data Director e do MDM Hub por uma entidade de segurança específica na qual tanto o MDM quanto o ActiveVOS confiam. Essa entidade de segurança é chamada de usuário confiável. O administrador do sistema cria as credenciais e funções para esse usuário confiável no servidor de aplicativos.

O ActiveVOS Server deve ser executado no mesmo servidor de aplicativos que o MDM Hub. Para obter mais informações, consulte o *Guia de Configuração do Multidomain MDM*.

Dynamic Data Masking

O Informatica Dynamic Data Masking é um produto de segurança de dados que opera entre um cliente e um banco de dados para evitar o acesso não autorizado às informações confidenciais. O Dynamic Data Masking intercepta as solicitações enviadas ao banco de dados e aplica um mascaramento nos dados antes de enviar os resultados da solicitação ao cliente.

O Dynamic Data Masking fornece um nível adicional de segurança de dados para os bancos de dados que gerenciam o MDM Hub . Use o Console de Gerenciamento do Dynamic Data Masking para configurar a conexão do Dynamic Data Masking com o Armazenamento de Referências Operacionais e definir as regras de mascaramento dos dados. Configure a conexão do MDM Hub com o Dynamic Data Masking quando você registra um Armazenamento de Referências Operacionais.

O instalador do MDM não instala o Dynamic Data Masking com o MDM Hub . Você deve instalar o Dynamic Data Masking separadamente. Para obter mais informações sobre a instalação do Dynamic Data Masking, consulte a documentação do Dynamic Data Masking.

Nota: Para usar o Dynamic Data Masking no MDM Hub , você deve ter o Dynamic Data Masking9.6.0 e a Correção de Erro de Emergência 14590 instalados. Versões anteriores do Dynamic Data Masking não são compatíveis com o MDM Hub .

Integração Entre o Dynamic Data Masking e o MDM Hub

Depois de instalar e configurar corretamente o Dynamic Data Masking, você pode integrar o Dynamic Data Masking com o MDM Hub .

As seguintes etapas descrevem o processo de integração:

1. No Console de Gerenciamento do Dynamic Data Masking, crie um serviço do Dynamic Data Masking. Configure o número de porta do ouvinte para corresponder ao número de porta à qual o cliente envia as solicitações ao banco de dados.
2. Defina as propriedades da conexão de banco de dados para o banco de dados que necessita de mascaramento de dados.
3. Crie uma regra de conexão. Configure a regra para identificar as solicitações de banco de dados que devem ser mascaradas. Atribua um banco de dados e um conjunto de regras de segurança ao conjunto de regras de conexão.
4. Crie um conjunto de regras de segurança. Defina as regras de mascaramento de dados enviadas novamente ao MDM Hub .
5. No Console do Hub, configure a conexão com o Dynamic Data Masking.

Quando você executa processos do Armazenamento de Referências Operacionais, o Dynamic Data Masking aplica as regras no banco de dados antes de retornar os dados para o MDM Hub .

Nota: Se você não adicionar a conexão do Dynamic Data Masking no Armazenamento de Referências Operacionais, o MDM Hub ignorará quaisquer regras do Dynamic Data Masking que você definir.

Para obter mais informações sobre como configurar o Dynamic Data Masking, consulte o *Guia do Administrador do Informatica Dynamic Data Masking*.

Práticas Recomendadas do Dynamic Data Masking para o MDM Hub

Você pode usar o Dynamic Data Masking de forma efetiva no MDM Hub com a ajuda das práticas recomendadas sugeridas.

A prática recomendada para criar as regras do Dynamic Data Masking no Editor de Regras

O Dynamic Data Masking avalia as regras no Editor de Regras, de cima para baixo. Portanto, se você criar regras de não mascaramento, deverá colocá-las acima quaisquer regras de mascaramento que você crie para que elas possam estar em vigor.

As práticas recomendadas para permitir que os usuários exibam os dados não mascarados

O Dynamic Data Masking não mascara dados no banco de dados. Quando você exibe os dados no MDM Hub , eles são exibidos com mascaramento. Use as instruções Criar Exibição no Dynamic Data Masking para conceder privilégios de usuários para exibir dados sem mascaramento.

Prática recomendada para bloquear usuários

Para evitar que usuários adicionem um registro ao qual o mascaramento é aplicado, você deve criar uma regra separada para cada objeto base afetado. Defina uma correspondência de texto como `%INSERT%<BO_NAME>%<ROLE NAME>%` e a ação de processamento Bloquear Instrução.

Práticas recomendada para permitir que os usuários atualizem os dados mascarados

Por padrão, o mecanismo do Dynamic Data Masking impede que os usuários editem tabelas com os dados mascarados. Se você deseja atualizar os dados mascarados no MDM Hub , poderá criar uma regra no Editor de Regras do Dynamic Data Masking para permitir que um usuário atualize as colunas mascaradas.

A prática recomendada para criar regras com o indicador de MDM_SYSTEM

O MDM Hub , o usuário MDM_SYSTEM é um indicador interno para as chamadas de sistema. O MDM_SYSTEM não aparece na lista de funções no Console do Hub. O Dynamic Data Masking aplica o mascaramento com base nas funções do MDM Hub que um usuário tem. Quando você cria regras do Dynamic Data Masking no Editor de Regras, não crie regras apenas para o indicador de MDM_SYSTEM. O YouChart do Guia de Configuração e Instalação de Contas deve combinar o MDM_SYSTEM com um nome de usuário ou com funções que pertencem a um usuário. Você pode combinar o indicador de MDM_SYSTEM com qualquer outra regra para criar regras granulares no Dynamic Data Masking.

Configurando o Dynamic Data Masking para um Armazenamento de Referências Operacionais

Configure a conexão do Dynamic Data Masking com o MDM Hub quando você registra um Armazenamento de Referências Operacionais por meio do Console do Hub.

1. Inicie o Console do Hub.

   A caixa de diálogo **Alterar banco de dados** é exibida.

2. Selecione o banco de dados Principais do MDM Hub e clique em **Conectar**.

3. No workbench de Configuração, inicie a ferramenta **Banco de Dados**.
4. Adquira um bloqueio de gravação.
5. Clique no botão **Registrar banco de dados**.

   O **Assistente de Conexão do Informatica MDM Hub** é exibido e solicita que você selecione o tipo de banco de dados.
6. Selecione o tipo de banco de dados e clique em **Avançar**.
7. Configure as propriedades da conexão para o banco de dados.
8. No campo **Porta**, a porta que você insere deve corresponder à porta do ouvinte do Dynamic Data Masking para o banco de dados.
9. No campo **URL da conexão DDM**, insira a URL do servidor do Dynamic Data Masking.
10. Clique em **Concluir.**

    A caixa de diálogo **Registrando Banco de Dados** é exibida.
11. Clique em **OK**.

    O MDM Hub registra o Armazenamento de Referências Operacionais.
12. Selecione o Armazenamento de Referências Operacionais registrado e clique no botão **Testar conexão de banco de dados** para testar as configurações do banco de dados.

    Se você usar o WebSphere, reinicie o WebSphere antes de testar a conexão de banco de dados.

    A caixa de diálogo Testar Banco de Dados exibe o resultado do teste de conexão de banco de dados.
13. Clique em **OK**.

    O Dynamic Data Masking se conecta ao Armazenamento de Referências Operacionais registrado.

Configurando um canal WebLogic T3S no Linux

O WebLogic T3S é um protocolo baseado em SSL que pode ser configurado para o MDM Hub.

As etapas a seguir pressupõem que você esteja familiarizado com a criação e o uso de um armazenamento de chaves, a configuração de uma instância de servidor para SSL e a criação de um canal. Para obter mais informações, consulte a documentação do WebLogic.

1. Antes de começar, é necessário ter um armazenamento de chaves que você queira usar para fins de identidade.
2. No Console de Administração do WebLogic, navegue até a instância de servidor usada com o MDM e configure o SSL com as seguintes propriedades:
   - **Identidade e Localização de Confiança** = **Armazenamento de Chaves**
   - **Localização da Chave Privada** = **do Armazenamento de Chaves de Identidade Personalizado**
   - **Alias da Chave Privada** = <Alias definido no armazenamento de chaves>
   - **Código de Acesso da Chave Privada** = <Código de acesso definido no armazenamento de chaves>
   - **Localização do Certificado** = **do Armazenamento de Chaves de Identidade Personalizado**
   - **Autoridades de Certificação Confiáveis** = **do Armazenamento de Chaves de Confiança Padrão Java**
3. Abra uma janela do Prompt de Comando do Administrador (cmd) e use o comando `keytool` para importar o armazenamento de chaves para os diretórios JDK e JRE em `lib/security/cacerts`.

O seguinte código de exemplo mostra a sintaxe:

```
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: Se precisar de ajuda com o comando `keytool`, consulte a documentação do Java.

4. Navegue até o arquivo `<domínio do WebLogic>/bin/startWebLogic.sh` e configure a seguinte opção Java:

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

5. No Console de Administração do WebLogic, crie um canal T3S que corresponda à configuração SSL. Defina as seguintes propriedades:
   - **Nome** = <Nome do canal>
   - **Protocolo** = t3s
   - **Endereço de Escuta** = <Nome do host definido no armazenamento de chaves>
   - **Porta de Escuta** = <Porta definida no armazenamento de chaves>
   - Selecione **Encapsulamento Ativado**
   - Selecione **SSL Bidirecional**
   - Verifique se o **Alias da Chave Privada do Servidor** exibe o alias que você especificou quando configurou o SSL.
6. Salve o canal e verifique se ele aparece na lista de canais de rede.
7. Se você usa o Informatica Data Director com exibições do Entity 360, navegue até o arquivo `<domínio WebLogic>/bin/setDomainEnv.sh` e defina as seguintes opções do MDM:
   - `e360.mdm.protocol=t3s`
   - `e360.mdm.host=<Endereço de Escuta do canal T3S>`
   - `e360.mdm.port=<Porta de Escuta do canal T3S>`
8. Reinicie o WebLogic.
9. Teste se o canal está funcionando executando ping nele.

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

10. Agora, você pode iniciar o Console de Hub usando HTTPS e a porta segura.

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

Ativando o Secure Siperian Bus no WebSphere Application Server

Para ativar a comunicação de mensagens seguras no Siperian Bus, você deve configurar o console do WebSphere e, em seguida, o `cmxserver.properties` relevante.

1. Abra o console do WebSphere.

2. Configure um novo usuário, na guia **Usuários e Grupos**.
    a. Clique em **Gerenciar Usuários** e em **Criar**.
    b. Na página **Criar um Novo Usuário**, insira as informações necessárias para criar um novo usuário. Não atribua privilégios a esse usuário.
    c. Clique em **Criar** para concluir a ação.
3. Defina as configurações na guia **Integração de Serviço**.
    a. Vá para **Barramentos** e clique no link do **SiperianBus**. A página **Configuração** é exibida.
    b. Na seção **Propriedades Adicionais**, clique em **Segurança**. A página **Barramentos > SiperianBus > Barramentos > Segurança para barramento SiperianBus** é exibida.
    c. Na seção **Propriedades Gerais**, marque a caixa de seleção **Ativar segurança do barramento**.
    d. Na seção **Política de Autorização**, clique em **Usuários e grupos na função de conector de barramento**.
    e. Clique em **Novo**, selecione o botão de opção **Usuários** e clique em **Avançar**.
    f. Selecione o usuário e clique em **Avançar** novamente. A página **Resumo** é exibida.
    g. Clique em **Concluir**.
    h. Retorne à página **Barramentos > SiperianBus > Barramentos > Segurança para barramento SiperianBus**.
    i. Em **Itens Relacionados**, clique no link **JAAS -J2C autenticar dados** e, em seguida, clique em **Novo**.
    j. Na seção **Propriedades Gerais**, especifique **Alias**, **ID do Usuário** e **Senha**. Clique em **OK**.
    k. Retorne à página **Barramentos > SiperianBus > Segurança para barramento SiperianBus**.
    l. Na seção **Propriedades Gerais**, selecione este Alias JAAS na lista **Alias de autenticação entre mecanismos**. Clique em **OK**.
4. Defina as configurações na guia **Recursos**.
    a. Acesse **JMS > Queue connection factory** e, em seguida, clique no link de connection factory para abrir o factory. A página **Configuração** é exibida.
    b. Na seção **Configurações de Segurança**, na lista **Alias de autenticação gerenciado por contêiner**, selecione o Alias JAAS definido anteriormente. Clique em **OK**.
    c. Acesse **JMS > Especificações de Ativação** e clique no link **SiperianActivation**. A página **Configuração** é exibida.
    d. Na seção **Configurações de Segurança**, na lista **Autenticar alias**, selecione o Alias JAAS definido anteriormente. Clique em **OK**.

Configure as propriedades relevantes no arquivo `cmxserver.properties`.

Configurando cmxserver.properties para Secure Siperian Bus

Você deve configurar o `cmxserver.properties` relevante para concluir a configuração segura do Siperian Bus. Em seguida, gere a senha criptografada. Antes de começar, ative a segurança para o Siperian Bus no servidor de aplicativos WebSphere.

1. No MDM Hub, abra o arquivo `cmxserver.properties`.

- No UNIX. `<diretório de instalação infamdm>/hub/server/resources`
- No Windows. `<diretório de instalação infamdm>\hub\server\resources`

2. Defina o nome de usuário a ser armazenado:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.username=<user name>
   ```

3. Defina a senha a ser armazenada:

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

   Por exemplo:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.password=UlRJz88k4O2EL5yDw2jypuCLAkEYHCwVg8F
   iNJavdfVvKnC8RFGIGE45IeKyQm5C2WJe2pX+ajXj1QeC/j
   +o7jQmItiaYoyrEMsIRWTvZiHg14ZKjYbFNJcwGSC3rpURvPqH+WMjaEWdXxcD8p7uZ1pphc7WXkE
   +VouCR6kRwy0=
   ```

4. Execute o seguinte comando para gerar a senha criptografada em seu ambiente:

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

   Por exemplo:

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

CAPÍTULO 7

Autenticação baseada em certificado

Este capítulo inclui os seguintes tópicos:

Autenticação baseada em certificado Visão Geral

O MDM Hub usa um mecanismo de autenticação baseado em certificado para proteger a comunicação entre os componentes do MDM Hub e aplicativos confiáveis. O mecanismo de autenticação também é suportado pelas APIs da Estrutura de Integração de Serviços (SIF) e de Serviços de Entidade Comercial.

Por padrão, o módulo de logon de certificado considera os aplicativos Informatica, como o Data Director, confiáveis. Para usar a autenticação baseada em certificado para aplicativos externos, você deve registrar os aplicativos como aplicativos confiáveis.

Um aplicativo externo registrado como aplicativo confiável passa ao MDM Hub uma concatenação do nome do aplicativo e do nome de usuário. Por exemplo, `IDD/admin`. O aplicativo externo também deve passar uma carga de segurança.

Autenticação com base em certificado e clientes externos

Clientes externos ao MDM Hub, como a API SiperianClient, podem enviar solicitações usando autenticação de nome de usuário e senha. No entanto, clientes externos também podem usar autenticação baseada em certificado.

Para configurar a autenticação com base em certificado para um cliente externo no MDM Hub, realize as seguintes etapas:

1. No Console do Hub, registre o certificado público para usuários associados ao cliente externo.

2. Use o cliente externo para acionar uma solicitação.

Aplicativos confiáveis

No MDM Hub, um aplicativo confiável tem um tipo de usuário chamado de usuário do aplicativo, que pode executar solicitações em nome de qualquer usuário regular do MDM Hub, incluindo o usuário administrador. Aplicativos confiáveis pertencem à estrutura de aplicativos confiáveis do MDM Hub.

Você deve usar o Console do Hub para registrar cada aplicativo personalizado que deseja usar como um aplicativo confiável. Por padrão, o MDM Hub considera como aplicativos confiáveis os aplicativos Informatica que são usados nas implementações do MDM Hub, como Data Director e ActiveVOS.

Por padrão, cada aplicativo confiável tem um conjunto configurado de chaves públicas e privadas. O MDM Hub autentica a solicitação de um aplicativo confiável por meio de autenticação baseada em certificado.

Para configurar um aplicativo personalizado como confiável, consulte "Adicionando Contas de Usuário" na página 31.

Adicionando um aplicativo externo como um aplicativo confiável

Você pode adicionar aplicativos externos à estrutura de aplicativos confiáveis do MDM Hub como aplicativos confiáveis.

1. No Console do Hub, adicione uma conta de usuário para o usuário do aplicativo que corresponde ao aplicativo externo.

   Nota: Certifique-se de marcar a caixa de seleção **Usuário do aplicativo** na caixa de diálogo **Adicionar Usuário** e de usar somente caracteres minúsculos para o nome da conta de usuário.
2. Registre um certificado público na conta de usuário do aplicativo.
3. Use o aplicativo externo para acionar uma solicitação.

   Nota: Se quiser usar a autenticação com base em certificados, defina o nome da solicitação como <nome do aplicativo>/<nome do usuário>. O <nome do aplicativo> deve ser o mesmo usado na etapa 1. O <nome do usuário> é o nome do usuário do MDM Hub que aciona a solicitação.

Gerenciamento de certificados e chaves

O MDM Hub usa uma autenticação baseada em certificado. Você deve manter os pares de certificado e chave privada para cada usuário em um local seguro.

Por padrão, o MDM Hub mantém chaves privadas e certificados no seguinte local:

```
<diretório de instalação do MDM Hub>/server/resources/certificates
```

Além disso, você pode configurar um provedor de certificado personalizado durante a instalação do Multidomain MDM.

Para implementar um provedor de certificado personalizado, você deve implementar uma interface `PKIUtil.java` no arquivo `siperian-server-pkiutil.jar`, que está no seguinte diretório:

```
<diretório de instalação do MDM Hub>/hub/server/lib/pkiutils
```

Se você usar um provedor de certificado personalizado, deverá manter o armazenamento de chaves e os certificados públicos que a implementação PKIUtil usa.

Nota: Se você precisar alterar o provedor de certificado, entre em contato com o Suporte Global a Clientes da Informatica para solicitar um utilitário de configuração de segurança.

Tópicos Relacionados:

- "Utilitário de configuração de segurança" na página 60

Utilitário de configuração de segurança

Você pode usar o utilitário de configuração de segurança para gerenciar algumas das configurações de segurança na implementação do MDM Hub.

Você pode usar o utilitário de configuração de segurança para executar as seguintes tarefas:

- Alterar o provedor de certificado usado para autenticação.
- Redefinir a senha para um usuário no MDM Hub.
- Alterar o algoritmo de hash usado para o hash de senha.
- Alterar a chave de hash de cliente usada para criar o algoritmo de hash.

Nota: Para obter o utilitário de configuração de segurança, entre em contato com o Suporte Global a Clientes da Informatica.

CAPÍTULO 8

Hash de senha

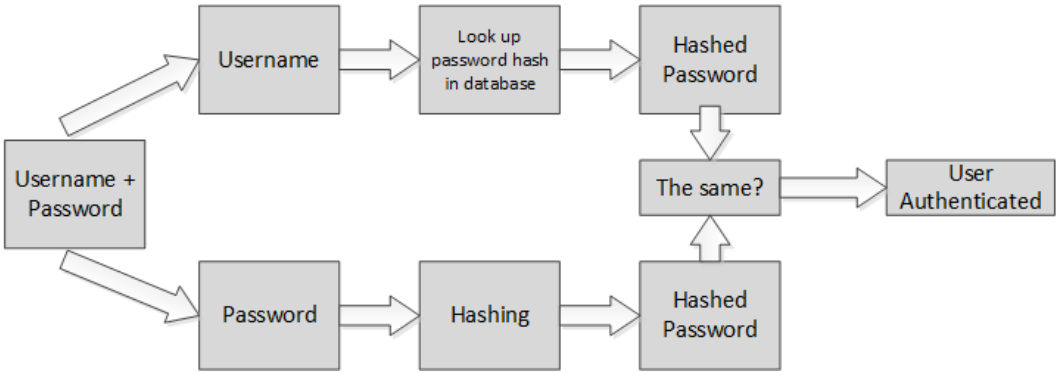
Este capítulo inclui os seguintes tópicos:

Visão geral do hash de senha

O hash de senha é uma forma de criptografar irreversivelmente senhas através de uma função de hash criptográfica. O MDM Hub usa um método de hash de senha para proteger as senhas de usuário e garantir que elas nunca sejam armazenadas no formato de texto simples em um banco de dados. O administrador do MDM Hub configura as opções de hash de senha, como o algoritmo e as chaves de hash do cliente, durante a instalação do Servidor de Hub.

A Informatica fornece um utilitário de configuração de segurança para gerenciar algumas das configurações de segurança em uma implementação do MDM Hub, incluindo a alteração do algoritmo de hash ou a redefinição das senhas de usuário do MDM Hub.

A imagem a seguir mostra como o MDM Hub autentica a senha do usuário:



Tópicos Relacionados:

- "Utilitário de configuração de segurança" na página 60

Opções de hash de senha

Durante a instalação do Servidor de Hub, você configura as seguintes opções de hash de senha:

- Se deve ser criada uma chave de hash personalizada como parte do algoritmo de hash
- Se deseja usar o algoritmo de hash SHA3 padrão ou criar um algoritmo de hash personalizado
- Se deseja usar o provedor de certificado padrão ou usar um provedor de certificado personalizado

Ambos os algoritmos de hash personalizado e SHA3 garantem que as senhas dos usuários do MDM Hub são criptografadas irreversivelmente e nunca armazenadas no formato de texto simples em um banco de dados. Independentemente de qual algoritmo de hash você usa, o algoritmo tem os seguintes componentes:

- Uma função de hash
- Um valor de salt
- Um valor opcional de pepper ou chave de hash, que é definido durante a instalação do MDM Hub. É responsabilidade do administrador do MDM Hub gerar essa chave e armazená-la com segurança.

Se você criar um valor de pepper, a Informatica recomendará usar uma chave contendo uma sequência de até 32 caracteres hexadecimais sem delimitadores.

Importante: Proteja o sigilo da chave de hash para evitar o risco de violação de dados. Se a chave de hash for roubada, você deverá redefinir todas as senhas.

O algoritmo de hash de senha e a implementação subjacente do algoritmo são armazenados nas propriedades do Servidor de Hub. Para obter mais informações sobre as propriedades do Servidor de Hub, consulte o *Guia de Configuração do Multidomain MDM*.

Algoritmo de hash personalizado

Processo de redefinição de senha

Se você esquecer sua senha, ou se achar que a segurança dos componentes secretos do algoritmo de hash pode estar comprometida, será possível redefinir a senha. Para redefinir sua senha, entre em contato com o Suporte Global a Clientes da Informatica.

Ao redefinir a senha, você receberá um e-mail com uma senha temporária. Use essa senha para fazer logon no MDM Hub e, em seguida, altere-a. É possível alterar a senha através do Console do Hub ou do Informatica Data Director.

Utilitário de configuração de segurança

Você pode usar o utilitário de configuração de segurança para gerenciar algumas das configurações de segurança na implementação do MDM Hub.

Você pode usar o utilitário de configuração de segurança para executar as seguintes tarefas:

- Alterar o provedor de certificado usado para autenticação.
- Redefinir a senha para um usuário no MDM Hub.
- Alterar o algoritmo de hash usado para o hash de senha.
- Alterar a chave de hash de cliente usada para criar o algoritmo de hash.

Nota: Para obter o utilitário de configuração de segurança, entre em contato com o Suporte Global a Clientes da Informatica.

Solução de problemas

Se você encontrar problemas, use as seguintes informações para solucioná-los.

Os usuários do MDM Hub não conseguem fazer login

Se o MDM Hub recriar o esquema CMX_SYSTEM após a instalação do Servidor de Hub, o MDM Hub não poderá reconhecer as senhas hash. Como resultado, os usuários não conseguirão fazer login no MDM Hub.

Para resolver o problema, execute o script `postInstallSetup` manualmente mais uma vez. Esse script garante que as senhas dos usuários do MDM Hub sejam definidas em hash novamente e que os usuários consigam fazer login.

Para obter mais informações sobre o script postInstallSetup, consulte o *Guia de Instalação do Multidomain MDM*.

APÊNDICE A

Glossário

administrador de dados

Usuário do Informatica MDM Hub que tem a responsabilidade principal pela qualidade de Dados. Os administradores de dados acessam o Informatica MDM Hub por meio do Console do Hub e usam as ferramenta de Informatica MDM Hub para configurar os objetos no Armazenamento de Hub.

Armazenamento de Hub

Em uma implementação do Informatica MDM Hub, o banco de dados que contém o Banco de Dados Principais e um ou mais banco de dados de Armazenamento de Referências Operacionais (ORS).

Armazenamento de referências operacionais (ORS)

Um banco de dados que contém os dados principais e as regras que regem os dados principais. Elas incluem as regras de processamento dos dados principais, as regras de gerenciamento do conjunto de objetos de dados principais, as regras de processamento e a lógica auxiliar que o MDM Hub usa para definir a melhor versão da verdade. Uma configuração do MDM Hub pode ter um ou mais Armazenamentos de Referências Operacionais. O nome padrão de um ORS é CMX_ORS.

autenticação

Processo de verificar a identidade de um usuário para assegurar que ele seja quem diz ser. No Informatica MDM Hub, os usuários são autenticados com base nas credenciais fornecidas — nome de usuário/senha, carga de segurança ou uma combinação de ambos. O Informatica MDM Hub fornece um mecanismo de autenticação interno e também oferece suporte à autenticação de usuário por meio de provedores de autenticação de terceiros.

autorização

Processo de determinar se um usuário tem privilégios suficientes para acessar um recurso solicitado do Informatica MDM Hub. No Informatica MDM Hub, os privilégios de recursos são alocados a funções. Os usuários e grupos de usuários são atribuídos a funções. Os privilégios de recursos de um usuário são determinados pela funções para as quais eles foram atribuídos, bem como pelas funções atribuídas ao(s) grupo(s) ao(s) qual(ais) o usuário pertence.

banco de dados

Coleção organizada de dados no Armazenamento de Hub. O Informatica MDM Hub dá suporte a dois tipos de bancos de dados: um Banco de Dados Principais e um Armazenamento de Referências Operacionais (ORS).

bloqueio de gravação

No Console do Hub, um bloqueio que é necessário para fazer alterações no esquema subjacente. Todas as ferramentas que não são do administrador de dados (exceto pelas ferramentas de segurança do Armazenamento de Referências Operacionais) estão no modo somente leitura, a menos que você adquira um bloqueio de gravação. Bloqueios de gravação permitem que vários usuários simultâneos façam alterações no esquema.

carga de segurança

Os dados binários brutos fornecidos para uma solicitação de operação do MDM Hub que pode conter os dados complementares necessários para autenticação ou autorização adicional.

Console do Hub

Informatica MDM Hub interface de usuário que consiste em um conjunto de ferramentas para administradores e administradores de dados. Cada ferramenta permite que os usuários realizem uma ação específica ou um conjunto de ações relacionadas, como criar o modelo de dados, executar trabalhos em lote, configurar o fluxo de dados, executar trabalhos em lote, configurar acesso a aplicativos externos para recursos do Informatica MDM Hub, assim como outras tarefas de configuração e operação do sistema.

diretiva de senha

Especifica as características de senha para contas de usuário do Informatica MDM Hub, como o comprimento da senha, sua expiração, as configurações de logon, a reutilização de senhas e outros requisitos. Você pode definir uma diretiva de senha global para todas as contas de usuário em uma implementação do Informatica MDM Hub, além de poder substituir essas configurações para usuários individuais.

Dynamic Data Masking

Um produto de segurança de dados que opera entre um cliente e um banco de dados para evitar o acesso não autorizado a informações confidenciais. O Dynamic Data Masking intercepta as solicitações enviadas ao banco de dados e aplica regras de mascaramento de dados à solicitação para mascarar os dados antes de que eles sejam enviados de volta ao cliente.

função

Define um conjunto de privilégios para acessar os recursos seguros do Informatica MDM Hub.

Gerenciador de Acesso à Segurança (SAM)

O Gerenciador de Acesso à Segurança (SAM) é o módulo de segurança para proteger os recursos do MDM Hub contra o acesso não autorizado. No tempo de execução, o SAM impõe as decisões de diretivas de segurança da sua organização para a sua implementação do MDM Hub , tratando a autenticação do usuário e a autorização de acesso de acordo com sua configuração de segurança.

Gerenciador de Dados

A ferramenta usada para analisar os resultados de todos as mesclagens — incluindo mesclagens automáticas — e corrigir conteúdo de dados, se necessário. Ele fornece a você uma exibição de linhagem de dados para cada registro de objeto base. O Gerenciador de dados também permite que você desfaça a mesclagem de registros mesclados anteriormente e exiba tipos diferentes de histórico em cada registro consolidado.

Use o Gerenciador de dados para pesquisar registros, exibir suas referências cruzadas, desfazer mesclagens de registros, desvincular registros, exibir registros de histórico, criar novos registros, editar registros e

substituir configurações de confiança. O Gerenciador de dados exibe todos os registros que atendem aos critérios de pesquisa que você definir.

grupo em lote

Um conjunto de trabalhos em lotes individuais (por exemplo, trabalhos Preparar, Carregar e Corresponder) que pode ser executado com um único comando. Cada trabalho em lotes de um grupo pode ser executado de forma sequencial ou paralela em relação a outros trabalhos.

Hierarchy Manager

The Gerenciador de Hierarquia 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*.

hierarquia

No Gerenciador de Hierarquia, um conjunto de tipos de relacionamento. Esses tipos de relacionamentos não são classificados com base no lugar das entidades da hierarquia, nem são eles necessariamente relacionados uns aos outros. Eles são apenas tipos de relacionamento agrupados para facilitar a classificação e a identificação.

Kerberos

Protocolo de autenticação de rede do computador que permite que os nós que se comunicam em uma rede não segura provem a sua identidade uns aos outros de uma forma segura. O Instituto de Tecnologia de Massachusetts desenvolveu o protocolo e faz uma implementação do Kerberos que está disponível livremente.

metadados

Dados que são usados para descrever outros dados. No Informatica MDM Hub, metadados são usados para descrever o esquema (modelo de dados) que é usado na sua implementação do Informatica MDM Hub, juntamente com as definições de configuração relacionadas.

objeto base

Uma tabela que contém informações sobre uma entidade que é relevante para a sua empresa, como cliente ou conta.

pacote

Um *pacote* é uma exibição pública de uma ou mais tabelas subjacentes do Informatica MDM Hub. Pacotes representam subconjuntos das colunas dessas tabelas, juntamente com outras tabelas que estão associadas às tabelas. Um pacote é baseado em uma consulta. A consulta subjacente pode selecionar um subconjunto de registros da tabela ou de outro pacote.

perfil

No Gerenciador de Hierarquia, descreve quais campos e registros um usuário do HM pode exibir, editar ou adicionar. Por exemplo, um perfil pode permitir acesso de leitura/gravação completo para todas as entidades e relacionamentos, enquanto outro pode ser somente leitura (sem permissão de operações de adicionar ou editar).

pontos de aplicação de diretiva (PEPs)

Pontos de verificação de segurança específicos que aplicam, em tempo de execução, diretivas de segurança para solicitações de autenticação e autorização.

pontos de decisão de diretiva (PDPs)

Os pontos de verificação de segurança específicos que autenticam a identidade de usuário e autorizam o acesso de usuário a recursos do MDM Hub .

privilégio

Permissão para acessar um recurso do MDM Hub. Com a autorização interna do MDM Hub, cada função recebe um dos seguintes privilégios.

Privilégio	Permite que o Usuário...
READ	Exiba dados.
CREATE	Crie registros de dados no Armazenamento de Hub.
UPDATE	Atualize registros de dados no Armazenamento de Hub.
MERGE	Mescle dados e desfaça a mesclagem de dados.
EXECUTE	Execute funções de limpeza e grupos em lote.
DELETE	Exclua registros de dados do Armazenamento de Hub.

Os privilégios determinam o acesso que os usuários de aplicativos externos têm aos recursos do MDM Hub. Por exemplo, uma função pode ser configurada para ter privilégios READ, CREATE, UPDATE e MERGE em determinado pacotes e colunas de pacotes. Esses privilégios não são aplicados ao se usar o Console do Hub, embora as configurações ainda afetem o uso do Console do Hub em um certo nível.

provedor

Consulte *provedor de segurança* na página 67.

provedor de segurança

Um aplicativo de terceiros que oferece serviços de segurança (serviços de autenticação, autorização e perfil de usuário) para usuários que acessam o Informatica MDM Hub.

recurso privado

Um recurso do Informatica MDM Hub que está oculto na ferramenta Funções, impedindo que ela acesse operações da Estrutura de Integração de Serviços (SIF). Quando você adiciona um novo recurso no Console do Hub (como um novo objeto base), ele é designado como um recurso PRIVATE por padrão.

segurança

A capacidade de proteger a privacidade das informações, sua confidencialidade e a integridade dos dados por meio da proteção contra o acesso não autorizado para ou a adulteração de dados e outros recursos na sua implementação do Informatica MDM Hub.

Servidor de Hub

Um componente de tempo de execução na camada intermediária (servidor de aplicativos) usado para serviços comuns e principais, incluindo acesso, segurança e gerenciamento de sessões.

workbench

No Console do Hub, um mecanismo para agrupamento de ferramentas semelhantes. Um workbench é uma coleção lógica de ferramentas relacionadas. Por exemplo, o Workbench modelo contém ferramentas de modelagem de dados como Esquema, Consultas, Pacotes e Mapeamentos.

Workbench de Configuração

Inclui ferramentas para configurar uma variedade de objetos do MDM Hub , incluindo o Armazenamento de Referências Operacionais, os usuários, a segurança, as filas de mensagens e a validação de metadados.

Workbench do Gerenciador de Acesso a Segurança

Inclui ferramentas para o gerenciamento de usuários, grupos, recursos e funções.

ÍNDICE