



Informatica® Multidomain MDM
10.5 HotFix 3

Guia de implementação do Data Director

© Copyright Informatica LLC 2005, 2024

Este software e a documentação são fornecidos somente sob um contrato de licença separado, contendo restrições sobre uso e divulgação. Não está permitida de forma alguma a reprodução ou a transmissão de qualquer parte deste documento (seja por meio eletrônico, fotocópia, gravação ou quaisquer outros meios) sem o consentimento prévio da Informatica LLC.

DIREITOS DO GOVERNO DOS ESTADOS UNIDOS Programas, softwares, bancos de dados, bem como a documentação e os dados técnicos relacionados, distribuídos a clientes do Governo dos EUA são "softwares de computador comerciais" ou "dados técnicos comerciais", de acordo com o Regulamento de Aquisição Federal aplicável e os regulamentos suplementares específicos da agência. Como tal, a utilização, duplicação, divulgação, modificação e adaptação estão sujeitas às restrições e aos termos de licença estabelecidos no contrato governamental aplicável e, na medida do que for aplicável pelos termos do contrato governamental, aos direitos adicionais estabelecidos no FAR 52.227-19, Licença de Software de Computador Comercial.

Informatica e o logotipo Informatica são marcas comerciais ou marcas registradas da Informatica LLC nos Estados Unidos e em muitas jurisdições por todo o mundo. Uma lista atual das marcas comerciais da Informatica está disponível na Internet em <https://www.informatica.com/trademarks.html>. Os nomes de outras companhias e produtos podem ser nomes ou marcas comerciais de seus respectivos proprietários.

Partes deste software e/ou documentação estão sujeitas a copyright detido por terceiros. Os avisos de terceiros necessários são incluídos no produto.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. Se você encontrar quaisquer problemas nesta documentação, informe-os em infa_documentation@informatica.com.

Os produtos Informatica apresentam garantias segundo os termos e condições dos acordos em que são fornecidos. A INFORMATICA FORNECE AS INFORMAÇÕES NESTE DOCUMENTO "COMO ESTÃO" SEM GARANTIA DE QUALQUER TIPO, EXPRESSA OU IMPLÍCITA, INCLUINDO, SEM QUAISQUER GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM DETERMINADO FIM E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO-VIOLAÇÃO.

Data da Publicação: 2024-08-28

Conteúdo

Prefácio.....	10
Recursos da Informatica.	10
Informatica Network.	10
Base de Dados de Conhecimento da Informatica.	10
Documentação da Informatica.	11
Matrizes de Disponibilidade de Produto da Informatica.	11
Informatica Velocity.	11
Informatica Marketplace.	11
Suporte Global a Clientes da Informatica.	11
Capítulo 1: Introdução.....	12
Visão geral.	12
Pré-requisitos.	13
Capítulo 2: Conceitos do IDD.....	14
Aplicativo do IDD.	14
Gerenciador de Configuração IDD.	14
Arquivos de Configuração do IDD.	14
Ferramenta de Provisionamento.	15
Áreas de Assunto e Grupos de Áreas de Assunto.	15
Áreas de Assunto.	15
Grupos de Áreas de Assunto.	16
Relacionamentos em Áreas de Assunto.	16
Uso de Recursos do Informatica MDM Hub.	18
Estrutura de Integração de Serviços.	18
Autenticação do Usuário (SSO).	19
Objetos Base.	19
Caches e a opção Limpar Cache.	19
Caminhos de Correspondência.	20
Pesquisar.	20
Funções de Limpeza.	21
Confiança.	22
Fluxos de Trabalho e Tarefas.	22
Gerenciador de Hierarquia.	23
Gerenciador de Acesso à Segurança.	23
Histórico.	24
Tabelas de Pesquisa.	24
Linha do Tempo.	25
Regras de Linha do Tempo.	26
Indicadores.	26

Exibição de Dados.	27
Exibição de Hierarquia.	27
Tarefa.	28
Pesquisar.	28
Capítulo 3: Processo de Implementação.....	29
Visão Geral do Processo de Implementação.	29
Antes de Iniciar.	29
Processo de Configuração.	30
Etapa 1. Criar o Aplicativo do IDD.	30
Etapa 2. Configurar Grupos de Áreas de Assunto.	31
Etapa 3. Configurar Áreas de Assunto.	31
Etapa 4. Configurar a Limpeza e a Validação.	33
Etapa 5. Configurar a Pesquisa.	34
Etapa 6. Configurar o processo de correspondência.	35
Etapa 7. Configurar Fluxos de Trabalho MDM.	36
Etapa 8. Configurar a Segurança.	37
Etapa 9. Configurar Extensões da Interface do Usuário.	37
Etapa 10. Localizar o Aplicativo.	38
Capítulo 4: Gerenciador de Configuração IDD.....	39
Visão Geral do Gerenciador de Configuração IDD.	39
Iniciando o Gerenciador de Configuração do Informatica Data Director.	40
Página Inicial.	40
Associação do ORS.	41
Adicionar um Aplicativo do IDD.	42
Importar uma Configuração de Aplicativo do IDD.	42
Validação, Estado do Aplicativo e Implantação.	43
Validação.	43
Estado do Aplicativo.	44
Implantação.	44
Editar Aplicativo.	45
Bancos de Dados ORS Lógicos.	45
Tempo Limite da Sessão.	46
Áreas de Assunto.	46
Importar um modelo de importação de dados.	50
Pacote de provedor de logon personalizado.	50
Carregando o pacote de provedor de logon personalizado.	51
Bibliotecas de terceiros.	52
Implementar o Provedor de Logon Personalizado.	52
Criar a Biblioteca do Provedores de Logon.	56
Configurar a Autenticação SSO do Salesforce (WebLogic).	56
Configurar a Autenticação SSO do Salesforce (WebSphere).	56

Capítulo 5: Configuração Manual do IDD.....	58
Visão Geral da Configuração Manual do IDD.	58
Ferramentas de XML.	59
Trabalhar com o Arquivo XML de Configuração do IDD.	59
Área de Assunto.	61
Coluna de Pesquisa.	61
Exibir os Campos Secundários de um Objeto Base na Guia Filho.	63
Exibindo um Pai de um Objeto Primário em uma Guia Filho.	64
Expandir uma Área de Assunto Filho na Exibição de Dados por Padrão	65
Criar Referência Irmã	65
Netos.	65
Links de Área de Assunto.	66
Agrupamento Lógico de Menus.	66
Adicionando grupos na janela Novo.	67
Personalizando Rótulos de Coluna.	67
Configurar o Estilo de Edição de Caixa de Seleção.	68
Configuração do Gerenciador de Hierarquia.	68
Adicionar Relacionamentos.	70
Otimização de Renderização.	70
Tipos de relacionamento do Gerenciador de Hierarquia	70
Filtro do Gerenciador de Hierarquia.	70
Ativando Relacionamentos Inativos.	71
Registros de Tabela de Relacionamento de Exibição de Hierarquia.	71
Exibição de Hierarquia.	71
Personalizações.	72
Extensões da Interface do Usuário.	73
Guias de Espaço de Trabalho de Nível Superior.	73
Guias de Nível Superior Personalizadas.	73
Espaço de Trabalho Início.	74
Guias Filho Personalizadas.	76
Ações Personalizadas.	79
Segurança para Extensões Personalizadas.	81
Saídas de Usuário.	82
Saídas de Usuário e a Estrutura do Entity 360.	82
Operações de Saída de Usuário.	82
Criando Saídas de Usuário.	87
Configurando uma Saída de Usuário.	87
Configurando uma saída de usuário para definir a data de início e a data de término de um período.	88
Mensagens de Saída de Usuário.	88
Solução de problemas.	89
Localização.	89

Configurando a página de logon e o idioma de exibição padrão do Gerenciador de Configuração.	90
Páginas de Erro Personalizadas.	91
Configurando uma Página de Erro Personalizada.	91
Ajuda Online.	91
Guia do Usuário do Data Director.	92
Ajuda Personalizada.	93
Capítulo 6: Propriedades Globais do IDD.	95
Referência a Propriedades Globais do Informatica Data Director.	95
Atualizando as Propriedades Globais.	105
Apêndice A: Requisitos de Dimensionamento e Plataforma.	109
Dimensionamento do Servidor de Banco de Dados.	109
Dimensionamento do Servidor de Aplicativos.	109
Dimensionamento do Cliente e da Rede.	109
Requisitos de Configuração do Navegador.	110
Apêndice B: Componentes de Aplicativo.	111
Referência a Componentes de Aplicativo.	111
Apêndice C: Configuração de Segurança do IDD.	112
Referência de Configuração de Segurança do IDD.	112
Apêndice D: Segurança de Dados.	119
Visão Geral da Segurança de Dados.	119
Segurança de Dados Usando Filtros.	119
Parâmetros de Segurança de Dados.	120
Exemplo de Configuração de Objetos Pai de Segurança de Dados.	120
Exemplo de Configuração de Objetos Neto de Segurança de Dados.	121
Aplicar a Segurança de Dados.	121
Segurança de Dados em Dados de Pesquisa.	122
Segurança de Dados em Dados de Entidade.	122
Segurança de Dados em Dados Hierárquicos.	125
Segurança de Dados em Dados Históricos.	126
Segurança de Dados em Links Profundos.	127
Apêndice E: Exemplo de Configuração de Segurança Baseada em Funções.	128
Visão Geral do Exemplo de Configuração de Segurança Baseada em Funções.	128
Principais Conceitos.	128
IDD, Gerenciador de Acesso de Segurança (SAM) e Estrutura de Integração de Serviços (SIF)	129
Ferramentas para Configurar a Segurança do IDD.	129
Leitura Relacionada.	129

Segurança de Objetos de Tarefas.	129
Dicas de Design de Segurança para Uso do IDD.	129
Outras Considerações.	130
Tarefas de Configuração de Segurança do IDD.	130
Configurar Objetos de Design no Console do Hub.	131
Configurar os Usuários de Aplicativos IDD (Ferramenta Usuários).	131
Configurar Recursos Seguros (Ferramenta Recursos Seguros).	132
Criar e Configurar um Novo Aplicativo do IDD (Gerenciador de Configuração IDD).	132
Exibir Recursos Personalizados (ferramenta Recursos Seguros).	132
Configurar Funções e Privilégios de Recursos (Ferramenta Funções).	133
Atribuir Funções a Usuários (Ferramenta Usuários e Grupos).	137
Que IDD de Amostra os Usuários Podem Ver e Realizar.	137
Apêndice F: Mascaramento de dados.	138
Visão Geral do Mascaramento de Dados.	138
Expressões.	138
Padrões de Amostra.	139
Definição de Máscara de Amostra.	139
Apêndice G: Mecanismo de Fluxo de Trabalho do Siperian BPM.	140
O Siperian BPM está Obsoleto.	140
Fluxos de Trabalho e Tarefas.	141
Diagrama de Componentes de Configuração de Fluxo de Trabalho e Tarefas.	141
Descrições de Componentes de Configuração de Fluxo de Trabalho e Tarefas.	142
Configuração de Tarefas.	142
Tipos de Tarefa.	143
Tipos de Tarefa - XML de Amostra.	143
Atributos e Marcas TaskType.	144
nome.	145
displayName.	145
creationType.	145
displayType.	146
dataUpdateType.	146
pendingBVT.	146
defaultApproval.	146
Marca de Descrição.	147
Marca de Ação.	147
Marca de Tarefa de Destino.	147
Personalização do Tipo de Tarefa.	147
Tipos de Ação.	148
Tipos de Ação - XML de Amostra.	148
Atributos e Marcas ActionType.	149
nome.	149

displayName.	149
Marca de Descrição.	149
manualReassign.	150
closeTaskView.	150
cancelTask.	150
Marca de Classe.	150
Configuração da Segurança de Tarefas.	150
Atribuição de Tarefas.	151
Configuração de Atribuição de Tarefas.	151
Interface do Usuário de Configuração de Atribuição de Tarefas.	152
Atribuição Automática de Tarefas.	152
Personalizando a Atribuição Automática de Tarefas.	153
Atribuição Manual de Tarefas.	153
Personalizando a Atribuição de Tarefas.	153
Alterando Tarefas Atribuídas.	153
Notificação de Tarefas.	154
Configurando o E-mail de Notificação de Tarefa.	154
Configuração do Gerenciador de Usuários no Console do Hub.	154
Relatórios e métricas de gerenciamento de tarefas.	155
Segurança de Dados em Dados de Tarefas.	156
Tarefa de Revisão.	156
Abrir Tarefas de Revisão com uma Única Função.	156
Abrir Tarefas de Revisão com Várias Funções.	157
Filtrar Registro Filho na Exibição de Tarefas.	158
Abrir Tarefas de Mesclagem/Desfazer Mesclagem.	158
Atribuição de Tarefas com Reconhecimento de Dados.	158
Apêndice H: Códigos de Localidade.	159
Códigos de Idioma.	159
Códigos de país A-L.	164
Códigos de PaísM-Z.	169
Apêndice I: Solução de problemas.	174
Visão Geral de Solução de Problemas.	174
Verificar a Configuração do SAM.	174
Verificar a Configuração da Função de Limpeza.	175
Os Metadados do Informatica Data Director Não Foram Atualizados.	175
O Informatica Data Director Para de Responder quando Você Troca de Entidades.	175
A Configuração do Informatica Data Director não é Válida.	176
O Desempenho de Correspondência é Muito Lento.	176

Apêndice J: Glossário.....	177
Índice.....	186

Prefácio

Use o Informatica® *Guia de Implementação do Multidomain MDM Data Director* para saber como configurar um aplicativo para o Informatica Data Director que usa o modelo de área de assunto. Aprenda sobre áreas de assunto, processos de implementação de aplicativos e configurações manuais do Data Director. Para obter informações sobre como configurar um aplicativo para o Data Director com entidades comerciais, consulte o *Guia da Ferramenta de Provisionamento do Multidomain MDM*.

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.

Informatica Network

A Informatica Network 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 Informatica Network, visite <https://network.informatica.com>.

Como membro da Informatica Network, 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

Este capítulo inclui os seguintes tópicos:

- [Visão geral, 12](#)
- [Pré-requisitos, 13](#)

Visão geral

Atenção: O Data Director com áreas de assunto foi descontinuado. A Informatica recomenda que você migre para o Data Director com entidades comerciais.

Este guia descreve como criar um aplicativo para o Data Director com áreas de assunto. Para obter instruções sobre como criar um aplicativo para o Data Director com entidades comerciais, consulte o documento *Guia da Ferramenta de Provisionamento do Multidomain MDM*.

O Data Director é um aplicativo de gerenciamento de dados que possibilita soluções de dados principais eficientes para todas as pessoas envolvidas na contabilização do gerenciamento de dados, entre elas:

- Usuários comerciais
- Administradores de dados
- Gerentes de TI

O Data Director permite que os usuários comerciais realizem com eficiência as funções descritas na tabela a seguir:

Funcionalidade	Descrição
Criar	Crie dados principais de alta qualidade, trabalhando individualmente ou de forma cooperativa por toda a sua empresa.
Gerenciar	Gerencie duplicatas, resolva correspondências, aprove e gerencie atualizações nos seus dados principais, crie e atribua tarefas aos usuários dos dados.
Consumir	Pesquise todos os dados principais em uma localização central, exiba os detalhes desses dados principais.
Monitorar	Rastreie linhagens e históricos, faça a auditoria de dados principais para conformidade e personalize seu painel.

Pré-requisitos

Este documento requer familiaridade com a arquitetura do MDM Multidomínio e um entendimento de todos os componentes no seu ambiente que são usados por aplicativos do Data Director.

Para obter mais informações, consulte a documentação do produto MDM Multidomínio.

CAPÍTULO 2

Conceitos do IDD

Este capítulo inclui os seguintes tópicos:

- [Aplicativo do IDD, 14](#)
- [Gerenciador de Configuração IDD, 14](#)
- [Arquivos de Configuração do IDD, 14](#)
- [Ferramenta de Provisionamento, 15](#)
- [Áreas de Assunto e Grupos de Áreas de Assunto, 15](#)
- [Uso de Recursos do Informatica MDM Hub, 18](#)
- [Indicadores, 26](#)

Aplicativo do IDD

Um aplicativo do IDD é unidade principal de configuração e implantação para implementações do IDD. Um aplicativo do IDD é o que os usuários comerciais visualizam quando iniciam o IDD e fazem login nele.

Gerenciador de Configuração IDD

O Gerenciador de Configuração IDD é um utilitário baseado na Web usado para adicionar, modificar e gerenciar aplicativos do IDD.

TÓPICOS RELACIONADOS:

- [“Gerenciador de Configuração IDD” na página 39](#)

Arquivos de Configuração do IDD

Um aplicativo do IDD consiste em um conjunto de arquivos de configuração: um arquivo de configuração do IDD (XML), pacotes de recursos, pacotes de mensagens de internacionalização, ajuda online e outros arquivos auxiliares. Você pode carregar ou modificar aplicativos do IDD no Gerenciador de Configuração IDD ou pode exportá-los e editá-los manualmente.

TÓPICOS RELACIONADOS:

- [“Componentes de Aplicativo” na página 111](#)

Ferramenta de Provisionamento

Você pode usar a ferramenta de Provisionamento para definir modelos, tarefas e transformações da entidade comercial, e criar a interface do usuário do Data Director.

O Informatica Data Director requer uma configuração de entidade comercial para recursos baseados na estrutura do Entity 360, como o Gerenciador de Tarefas e exibições de registros. O Informatica Data Director também requer uma configuração de área de assunto para alguns recursos, como a exibição Hierarquia, a exibição Referência Cruzada e a página Corresponder Comparação de Mesclagem.

Este guia descreve a configuração de áreas de assunto do Informatica Data Director. Para obter informações sobre a configuração da estrutura do Entity 360 e a configuração de entidades comerciais, consulte o *Guia da Ferramenta de Provisionamento do Multidomain MDM*.

Áreas de Assunto e Grupos de Áreas de Assunto

Em um aplicativo do IDD, os dados são organizados em torno de áreas de assunto e agregados em grupos de áreas de assunto.

Áreas de Assunto

A *área de assunto* é um conceito de organização principal de um aplicativo do Informatica Data Director.

Outros termos ou conceitos relacionados ou semelhantes a áreas de assunto incluem: objeto comercial e entidade hierárquica. O Informatica Data Director usa a definição de área de assunto para determinar como tratar cada um dos relacionamentos de chave externa em um Armazenamento de Referências Operacionais (ORS).

O Armazenamento de Hub mantém metadados detalhados sobre tabelas e relacionamentos definidos em um ORS. Esses metadados incluem relacionamentos entre tabelas de objetos base que podem representar:

- Referências a tabelas de pesquisa
- Links entre um pai e dados filho relacionados
- Vínculos associativos entre tabelas - que não representam um relacionamento de posse.

O Armazenamento de Hub oferece alguns dos metadados que permitem que o Informatica Data Director entenda como os relacionamentos devem ser tratados. Por exemplo, o indicador de pesquisa de objeto base instrui o Informatica Data Director no que diz respeito a quando tratar uma tabela relacionada como uma pesquisa com uma lista suspensa previamente preenchida que os usuários visualizam em um aplicativo do Informatica Data Director.

Para outros relacionamentos, um aplicativo do Informatica Data Director talvez precise de informações adicionais para entender os relacionamentos corretamente: se eles devem ser interpretados como relacionamentos entre tabelas em uma área de assunto ou como relacionamentos entre áreas de assunto. O Gerenciador de Configuração do Informatica Data Director é usado para especificar essas informações de

relacionamentos adicionais para aplicativos do Informatica Data Director. Não é possível usar aliases para uma área de assunto baseada em um relacionamento do Gerenciador de Hierarquia.

Uma área de assunto representa uma coleção de dados que devem ser tratados como uma unidade sob uma perspectiva comercial. Uma área de assunto tem:

- Um único registro raiz em um objeto base
- Alguns registros filho e neto (por meio de relacionamentos de um-para-muitos e de muitos-para-muitos).

Grupos de Áreas de Assunto

Um *grupo de áreas de assunto* é um conjunto de uma ou mais áreas de assunto que têm o mesmo objeto base em sua raiz (também chamada de *objeto primário*).

Por exemplo, um ORS usando um modelo Party (um único objeto base que representa diferentes tipos de entidade) terá um grupo de áreas de assunto com várias áreas de assunto.

Nota: Um objeto base só pode ser associado a um grupo de áreas de assunto.

Relacionamentos em Áreas de Assunto

Em um aplicativo do IDD, os relacionamentos dentro de áreas de assunto se baseiam nos relacionamentos que estão configurados entre objetos base no Armazenamento de Hub (usando o Gerenciador de Esquemas no Console do Hub).

O Gerenciador de Configuração IDD faz referência aos *componentes de caminho de correspondência* configurados, que se baseiam em relacionamentos de chave externa.

Relacionamentos Filho de Um-para-Muitos

Para relacionamentos de um-para-muitos, o registro filho tem uma chave externa direta para o objeto primário. O IDD dá suporte a dois tipos de relacionamentos de um-para-muitos.

A seguinte tabela descreve os tipos de relacionamentos filho de um-para-muitos:

Relacionamento	Descrição
Um-para-Muitos	A lista de registros filho será exibida em uma guia abaixo dos dados primários.
Um-para-Um Lógico	A expectativa é de que deve haver apenas um registro filho para cada objeto primário. Os dados são mostrados no formulário com o objeto primário. Se houver mais de um filho (por exemplo, devido à mesclagem de dois objetos primários), o aplicativo do IDD fornecerá uma maneira de resolver isso.

Relacionamentos Filho de Muitos-para-Muitos

Para relacionamentos de muitos-para-muitos, o registro filho está relacionado ao objeto primário por meio de uma tabela de relacionamentos.

A tabela de relacionamentos em um filho muitos para muitos deve conter duas chaves externas.

O IDD oferece suporte a dois tipos de relacionamentos muitos para muitos. A seguinte tabela descreve os tipos de relacionamentos filho de Muitos-para-Muitos:

Relacionamento	Descrição
Parte de	<p>O registro filho pertence ao objeto primário. Nenhuma outra área de assunto deve fazer referência a esse filho. Ao adicionar um filho, tanto o relacionamento quanto os registros filho são adicionados.</p> <p>Ao editar um filho, se outra área de assunto fizer referência a ele, uma cópia do filho será criada. Os dados referenciados pelo outro filho permanecerão inalterados.</p>
Referência	<p>O filho é outra área de assunto. Ao adicionar um filho, somente um registro de relacionamento é adicionado. O usuário do aplicativo IDD deve procurar o filho da área de assunto a ser relacionado.</p> <p>Para editar os dados do filho, a área de assunto desse filho deve estar aberta. Esse filho pode ser vinculado por meio de um Objeto Base de relacionamento padrão ou de um Objeto Base de relacionamento do HM.</p>

Relacionamentos Neto de Um-para-Muitos

Para relacionamentos de um-para-muitos, o registro neto tem uma chave externa direta para um objeto filho. O IDD dá suporte a dois tipos de relacionamentos de um-para-muitos: se o filho for do tipo muitos-para-muitos, a chave externa poderá ser para (consulte os exemplos de modelo de dados abaixo):

- O relacionamento filho
- Para o registro de relacionamentos

Relacionamento	Descrição
Um-para-Muitos	A lista de registros neto será exibida em uma guia abaixo dos dados filho.

Relacionamentos Neto de Muitos-para-Muitos

Para relacionamentos de muitos-para-muitos, o registro neto está relacionado ao objeto filho por meio de uma tabela de relacionamentos.

O IDD dá suporte a dois tipos de relacionamentos de muitos-para-muitos: Se o filho for do tipo muitos-para-muitos, a chave externa poderá ser para (consulte os exemplos de modelo de dados abaixo):

- Registro filho
- Registro de relacionamentos.

A seguinte tabela descreve os tipos de relacionamentos neto de muitos-para-muitos:

Relacionamento	Descrição
Parte de	O registro neto pertence ao objeto primário - nenhuma outra área de assunto deve fazer referência a esse neto. Ao adicionar um neto, tanto o relacionamento quanto os registros neto são adicionados. Ao editar um neto, se outra área de assunto fizer referência a ele, uma cópia do neto será criada. Os dados referenciados pelo outro filho permanecerão inalterados.
Referência	O neto é outra área de assunto. Ao adicionar um neto, somente um registro de relacionamento é adicionado. O usuário de aplicativo do IDD deve procurar o neto da área de assunto a ser referenciado. Para editar os dados do neto, a área de assunto desse neto deve estar aberta. Esse neto pode ser vinculado por meio de um Objeto Base de relacionamento padrão ou de um Objeto Base de relacionamento do HM.

Nota: Ao configurar o caminho de correspondência para netos no Gerenciador de Esquemas do Console do Hub, verifique se a opção **Verificar Filho Ausente** está desativada. O aplicativo do IDD não funcionará corretamente se a opção **Verificar Filho Ausente** estiver ativada.

Referências Irmãs

Uma referência irmã é um relacionamento de um registro em uma área de assunto com um registro filho dentro dessa área de assunto.

Para um modelo de dados, um cliente pode incluir registros filho de endereço e de número de telefone, com o número de telefone possuindo uma chave externa a ser associada a um endereço específico. O IDD pode ser configurado para dar suporte a esse tipo de relacionamento.

Ao adicionar ou editar a chave de endereço no número de telefone, o usuário do aplicativo do IDD recebe uma lista de endereços que contêm apenas os filhos dessa parte.

TÓPICOS RELACIONADOS:

- [“Configuração Manual do IDD” na página 58](#)

Registros Pai

Um registro que é pai do objeto primário pode ser incluído na área de assunto.

Ele é exibido em uma guia filho. Como há sempre apenas um registro nessa guia, ela sempre é mostrada em uma exibição de formulário. Esses dados são somente leitura. O IDD não permite a edição desses dados ou do relacionamento com eles.

Uso de Recursos do Informatica MDM Hub

Estrutura de Integração de Serviços

Toda a interação entre um aplicativo do Data Director e um ORS é feita por meio de chamadas da API da Estrutura de Integração de Serviços (SIF).

Não há acesso direto ao banco de dados ORS (com uma exceção: gráficos podem ser configurados para usar uma fonte de dados de servidor de aplicativos para buscar dados de relatórios). O Gerenciador de

Configuração IDD usa a SIF para acessar metadados sobre um ORS, mas usa uma fonte de dados para acessar diretamente a tabela CMX_SYSTEM.C_REPOS_DS_CONFIG.

Algumas das chamadas da API SIF são assíncronas. Para ativar o suporte a chamadas SIF assíncronas, o bloqueio em nível de linha deve ser ativado para o ORS usado pelo aplicativo do Data Director. Para obter mais informações, consulte a seção sobre bloqueio em nível de linha no *Guia de Configuração do Multidomain MDM*.

Usando um Servidor Web

Antes de implementar um servidor Web que atue como proxy reverso, configure o formato da URL de serviço que o IDD gera para chamadas SIF. Configure a propriedade "referer.url" no arquivo `cmxserver.properties` para especificar o formato da URL de serviço.

Adicione o seguinte texto ao arquivo `cmxserver.properties` para configurar o formato da URL de serviço:

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

Autenticação do Usuário (SSO)

Por padrão, o Data Director autentica os usuários com uma chamada SIF para o Servidor de Hub. Para o processo de autenticação, a implementação do MDM Hub requer que você configure usuários para o Banco de Dados Principal. Para obter mais informações sobre como configurar usuários do MDM Hub, consulte o *Guia de Segurança do Multidomain MDM*.

Como alternativa, você pode implementar o logon único (SSO) e autenticar usuários com provedores de identidade externos. O Provedor de Login no Data Director se comunica com o Provedor de Segurança do Hub (Módulo de Login). Para obter mais informações sobre arquivos do provedor, consulte o *Guia de Segurança do Multidomain MDM*.

Objetos Base

A segurança em nível de coluna é configurada no Gerenciador de Acesso de Segurança (SAM) por meio da definição do acesso baseado em função a objetos base e suas colunas, o que proporciona um controle granular sobre o acesso dos usuários aos dados.

O IDD faz referência a objetos base diretamente para todas as operações `GET` e `PUT`. O IDD usa somente pacotes para a exibição de resultados de pesquisa.

Caches e a opção Limpar Cache

O Informatica Data Director mantém um cache de metadados do MDM Hub que descreve objetos base, colunas, relacionamentos e outros detalhes. Se você alterar os metadados do MDM Hub, clique em **Limpar Cache** no Gerenciador de Configuração IDD antes de exportar um aplicativo IDD.

A opção Limpar Cache no Gerenciador de Configuração IDD limpa o cache para o aplicativo IDD selecionado. Em um ambiente do Microsoft SQL Server, a Informatica recomenda que você limpe o cache ao fazer alterações nos metadados do ORS através do Console de Hub. Por exemplo, se você adicionar um relacionamento a um objeto base no Console do Hub e, em seguida, salvar e validar a alteração, será possível reimplantar o aplicativo IDD para que essa alteração tenha efeito. No entanto, você deverá limpar o cache antes de exportar o aplicativo IDD para ver o novo relacionamento no arquivo `Metadatabundle.properties`.

Também é possível reiniciar o servidor de aplicativos para limpar o cache.

O IDD também mantém caches de atribuições e definições de função do SAM e valores de pesquisa. O IDD atualiza os caches a uma taxa que você pode configurar por meio das propriedades globais do IDD.

Caminhos de Correspondência

Defina os relacionamentos filho no IDD com caminhos de correspondência. Você pode configurar os caminhos de correspondência no Gerenciador de Esquemas do Hub Console.

Antes da introdução do IDD, os caminhos de correspondência eram usados estritamente para definir colunas e regras de correspondência. A definição do caminho de correspondência funciona igualmente bem para definir relacionamentos filho no IDD.

Para adicionar um filho a uma área de assunto, crie um novo caminho de correspondência para o filho, se ele não existir. Quando você cria um caminho de correspondência, ele deve ser baseado no ROWID_OBJECT.

Caminhos de correspondência também podem ser usados para ativar a pesquisa em tabelas relacionadas que não fazem parte de uma área de assunto. Por exemplo, suponha que você tem uma área de assunto Party relacionada a uma área de assunto Product. Product não pode fazer parte da área de assunto Party. No entanto, um caminho de correspondência pode ser definido de Party para Product. Usando esse caminho de correspondência, um usuário de aplicativo do IDD pode procurar Party com base nos atributos de um Product relacionado.

Pesquisar

A pesquisa por dados em uma área de assunto pode se basear em uma das seguintes APIs de pesquisa SIF: `searchQuery` e `searchMatch`.

Em ambos os casos, um pacote de exibição é usado para exibir os resultados de pesquisa.

Básica - Pesquisa baseada em SQL

A Pesquisa Básica usa a API `searchQuery`.

Uma pesquisa pode se basear em dados dos seguintes elementos:

- Registro de objeto primário
- Qualquer um de seus registros filho (OP)
- Qualquer registro relacionado por meio de um componente de caminho de correspondência

Você pode realizar uma pesquisa Básica sem distinção entre maiúsculas e minúsculas ao executar uma consulta de dados. A pesquisa básica localiza resultados usando comparações de strings e padrões de string.

Nota:

- Nos ambientes Microsoft SQL Server, a Pesquisa Básica não diferencia maiúsculas de minúsculas.
- Em ambientes Microsoft SQL Server, você não pode usar colchetes (`[]`) e um operador semelhante em uma solicitação de pesquisa. Para usar colchetes em uma consulta de pesquisa, coloque o primeiro colchete (`[`) em um par de colchetes extras (`[]`). Por exemplo, para procurar um registro que começa com um primeiro nome como `%[ABC123]%`, use a seguinte consulta de pesquisa:

```
first_name like '%[[]ABC123]%'
```

Estendida - Pesquisa baseada em Correspondência

A Pesquisa Estendida não faz distinção entre maiúsculas e minúsculas e usa a API **`searchMatch`** com `matchType=NONE`.

Ela foi projetada para pesquisa e, portanto, não usa um conjunto de regras de correspondência predefinido. Qualquer um dos dados na área de assunto que contribui com uma coluna de correspondência pode ser

usado como critério de pesquisa. Um aplicativo do IDD requer que os usuários insiram critérios na chave da correspondência difusa antes de poderem executar a pesquisa.

Pesquisa Avançada

A pesquisa avançada permite que os usuários de aplicativos do IDD construam consultas complexas definindo expressões do tipo SQL WHERE e texto de consulta em forma livre.

Você pode realizar uma pesquisa Avançada sem distinção entre maiúsculas e minúsculas ao executar uma consulta de dados. A pesquisa avançada permite que os usuários de aplicativos do IDD especifiquem condições de pesquisa que vão além das capacidades disponíveis nas pesquisas Básica ou Estendida.

Funções de Limpeza

O IDD usa a API **PUT** em vez de **cleansePut**.

No entanto, o IDD pode chamar a API **cleanse** para cada registro de objeto de base antes que esse seja salvo. Isso é às vezes chamado de *função de limpeza em linha*. A função de limpeza pode realizar uma operação regular de padronização e limpeza de dados, além de validações personalizadas nesses dados. Cada função de limpeza configurada é chamado antes que os dados sejam salvos.

- Na Exibição de Dados, a limpeza é chamada quando o botão **Aplicar** é clicado em um formulário de edição.
- Na Exibição de Hierarquia, a limpeza é chamada ao se clicar no botão **OK** de uma caixa de diálogo Adicionar/Editar relacionamento.

Limpeza de e Padronização

O Gerenciador de Configuração IDD fornece um meio simples e direto para conectar registros de objeto base às entradas e às saídas de uma função de limpeza.

Os dados no registro de objeto base são atualizados com as saídas da função de limpeza.

Nota: Apenas as colunas de objetos base que são selecionadas no layout da configuração da área de assunto podem servir como entradas ou saídas de função de limpeza.

Validação

Uma função de limpeza pode ser usada para realizar a validação de dados personalizada.

Os resultados de validação serão processados se a função de limpeza tiver um parâmetro de saída `validationStatus`.

- Se o parâmetro `validationStatus` estiver em branco, significa que não existem erros de validação, e o processo pode continuar.
- Se houver erros de validação, o parâmetro `validationStatus` incluirá uma série de mensagens de validação, descrevendo o nome de `inputParameter` e uma mensagem. Na interface de usuário do aplicativo do IDD, cada erro de validação é associado a um valor de entrada em uma coluna de entrada específica.

Nota: O Kit de Recursos contém a amostra `ValidationCleanserLib`, que fornece um exemplo de uma biblioteca de limpeza com funções que realizam a validação em um aplicativo do IDD.

Funções de Limpeza que Retornam NULL

Quando a saída de uma função de limpeza é um valor nulo, a API **cleanse** não retorna informações sobre esse campo.

Supõe-se que a função não esteja alterando esse campo. Se o objetivo for que a função de limpeza substitua um valor por NULL, as opções dependerão do tipo de dados, e o seguinte será necessário:

- String - A função pode ser alterada para retornar uma string vazia.
- Data ou numérico - Uma saída de usuário deve ser implementada para modificar os dados. Os métodos `beforeEverything()` ou `beforeSave()` do manipulador Save podem ser usados.

TÓPICOS RELACIONADOS:

- [“Saídas de Usuário” na página 82](#)

Confiança

Um aplicativo do Data Director está configurado para usar um único sistema de origem para todas as suas operações.

Os dados inseridos e atualizados por meio de um aplicativo do Data Director seguem todas as regras de confiança padrão, conforme descrito na ajuda online do Console de Administração ou no *Guia de Configuração do Multidomain MDM*. Os dados inseridos em um aplicativo do Data Director são aplicados ao registro de objeto base com base nas regras de confiança e validação configuradas no Informatica MDM Hub para esse sistema de origem. Ao visualizar dados de referências cruzadas, você pode promover o valor de um atributo de um registro de referência cruzada para colunas ativadas para confiança. Isso resulta em uma substituição de confiança para esse atributo.

Fluxos de Trabalho e Tarefas

Um aplicativo do IDD pode usar tarefas e fluxos de trabalho para oferecer suporte a um processo de aprovação de alteração de registros ativados por estado no Armazenamento de Hub.

Por exemplo, suponha que um Gerente Financeiro queira analisar todas as alterações das informações bancárias do cliente antes da alteração ser aceita como dados mestre. Você pode configurar um aplicativo do IDD, de forma que, quando alguém no departamento Financeiro usar o aplicativo para atualizar as informações, uma tarefa seja atribuída ao Gerente Financeiro para analisar as alterações pendentes e aprová-las ou rejeitá-las. Um processo de aprovação de alteração garante que apenas os registros aprovados contribuam com os registros Melhor Versão da Verdade (BVT).

Um aplicativo do IDD coordena atividades de tarefa entre a Caixa de Entrada de Tarefas do IDD, uma ferramenta de gerenciamento de processo comercial (BMP) e tabelas ativadas por estado no Armazenamento de Hub. Para incluir o suporte ao fluxo de trabalho no seu aplicativo, consulte o [“Etapa 7. Configurar Fluxos de Trabalho MDM” na página 36](#).

Tarefas e Ações

Uma *tarefa* é uma etapa em um processo de fluxo de trabalho.

Para qualquer tarefa, haverá uma ou mais ações que podem ser realizadas. Tarefas e suas ações associadas podem ser configuradas como parte de um aplicativo do IDD.

Dados em Andamento

Dados em andamento são dados comerciais que podem passar por diferentes estados (ACTIVE, PENDING ou DELETED) ao progredirem por um fluxo de trabalho.

O IDD oferece suporte para dados em andamento usando a funcionalidade de gerenciamento de estado e recursos de gerenciamento de tarefas do Informatica MDM Hub.

Dados podem ser adicionados ou atualizados e "Enviados para Aprovação" em vez de serem salvos. As alterações de dados são armazenadas como alterações pendentes (PENDING) - os dados não são aplicados ao objeto base. Uma tarefa é criada por outro usuário aprovar essa alteração. Uma vez aprovados, os dados PENDING são promovidos para ACTIVE, e depois são aplicados ao objeto base.

Gerenciador de Hierarquia

Se o Gerenciador de Hierarquia (HM) estiver configurado para um ORS, você poderá configurar um aplicativo do IDD para trabalhar com essa configuração.

Configure o aplicativo IDD de acordo com as seguintes regras:

- Qualquer entidade do HM que use um aplicativo do IDD deve ser configurada como uma área de assunto no Gerenciador de Configuração IDD. O HM é usado para modelar os relacionamentos entre as áreas de assunto.
- Um aplicativo do IDD opera em uma única configuração do HM (combinação de perfil/área restrita). O IDD usa a configuração de controle de acesso do SAM, em vez de diferentes configurações do HM, para gerenciar o controle de acesso dos usuários. A configuração do HM usada por um aplicativo do IDD deve incluir todos os tipos de entidade e relacionamento do HM que serão usados no aplicativo do IDD.

Gerenciador de Acesso à Segurança

Use o Gerenciador de Acesso de Segurança para conceder a funções de usuário acesso granular aos objetos base e a outros recursos. O Data Director herda as funções de usuário e implementa o mesmo acesso granular aos registros.

Para obter mais informações, consulte o *Guia de Segurança do Multidomain MDM*.

TÓPICOS RELACIONADOS:

- [“Configuração de Segurança do IDD” na página 112](#)

Segurança de Objetos e Colunas

O SAM fornece privilégios de segurança com base em função em objetos de design e colunas definidos em um ORS.

Um aplicativo do IDD usa essa configuração de segurança para que os dados exibidos, e as operações disponíveis para um usuário individuais, dependam de uma ou mais funções atribuídas a essa conta de usuário. Os usuários de aplicativos do IDD visualizam apenas os dados e as funcionalidades aos quais eles receberam acesso. Por exemplo, se um usuário não tiver acesso READ à tabela HISTORY para um objeto base, no aplicativo do IDD, o comando Histórico para essa área de assunto não estará disponível para esse usuário.

Nota: Um usuário do Hub com acesso de Administrador (configurado na ferramenta Usuários do Console do Hub) é um super usuário do IDD e tem privilégios totais em todos os objetos.

Segurança de Dados

O SAM não fornece a segurança de dados em nível de linha (impedindo que os usuários vejam determinados registros com base no conteúdo desses registros).

O IDD, no entanto, fornece um mecanismo simples de segurança de dados. Para cada área de assunto, *filtros de segurança* podem ser definidos no arquivo de configuração do IDD. Um filtro de segurança especifica uma condição de filtro que o IDD aplica a todos os dados acessados por usuários atribuídos a uma função específica. Por exemplo, um filtro de segurança pode especificar `COUNTRY_CODE = 'US'`, que pode se aplicar a usuários com a função de Administrador de Dados nos EUA. Cada filtro pode ser aplicado a várias funções. Qualquer número de filtros pode ser criado para uma área de assunto para qualquer número de funções.

Mascaramento de dados

O IDD fornece um mecanismo para o ocultamento (mascaramento) de informações com base em funções de segurança.

Você pode definir uma máscara para cada campo em um layout de coluna. Máscaras podem ser especificadas para uma única função, para um conjunto de funções ou para todos os usuários não administradores. Quando você especifica uma máscara, todo o valor, ou parte dele, é substituído por um asterisco (*).

TÓPICOS RELACIONADOS:

- [“Mascaramento de dados” na página 138](#)

Histórico

O IDD fornece uma exibição de área de assunto do histórico de alterações para cada registro.

Essa funcionalidade requer que o histórico esteja ativado no objeto base. Se o histórico não estiver ativado para um objeto base, a Exibição de Histórico não estará disponível para a área de assunto associada no aplicativo do IDD. O IDD mostra uma exibição de linha de tempo de eventos para o registro e seus registros filho. Uma exibição de ponto no tempo dos dados também pode ser mostrado.

Tabelas de Pesquisa

Uma tabela de pesquisa, também chamada de objeto base de pesquisa ou simplesmente de pesquisa, é uma tabela que armazena uma lista de valores predefinidos. O Data Director (IDD) consulta a tabela de pesquisa para recuperar um valor com base no valor de origem de entrada e na condição de pesquisa. Em seguida, o Data Director preenche uma lista suspensa de valores no aplicativo. Por exemplo, se você inserir um valor em um campo País, o aplicativo listará os países armazenados na tabela de objetos base de pesquisa LU_COUNTRY.

É possível definir valores de pesquisa das seguintes maneiras:

- Em uma tabela física de objetos base de pesquisa com uma chave externa entre o objeto base e o objeto base de pesquisa. O Data Director usa metadados sobre essa chave externa para preencher os valores de pesquisa.
- Em uma tabela física de objetos base de pesquisa sem uma chave externa entre o objeto base e o objeto base de pesquisa. A configuração do IDD descreve o relacionamento da chave externa, que preenche os valores de pesquisa.
- Em uma lista estática de valores na configuração do IDD.

Para as pesquisas definidas em uma tabela física, a coluna LOOKUP_IND em C_REPOS_TABLE indica se a tabela contém valores de pesquisa ou dados regulares. Você ativa o indicador de pesquisa por meio da

ferramenta Esquema no Console do Hub. Por padrão, o indicador de pesquisa está desativado quando você cria um objeto base. Quando o indicador de pesquisa é ativado, o MDM Hub considera o objeto base como uma pesquisa. Para obter mais informações sobre a ferramenta Esquema, consulte o *Guia de Configuração do Multidomain MDM*.

Nota: Ao criar uma pesquisa, use um nome de exibição exclusivo. O Data Director não consegue distinguir tabelas de pesquisa diferentes que compartilham o mesmo nome de exibição.

Quando o Data Director reconhece que uma coluna tem uma chave externa em outra tabela, o Data Director determina se a tabela relacionada é uma tabela de pesquisa. Se a tabela relacionada for uma tabela de pesquisa, o Data Director criará uma lista suspensa no aplicativo para essa coluna, preenchida com valores dessa tabela de pesquisa. A coluna na tabela de pesquisa usada varia de acordo com o campo **Nome de Exibição da Pesquisa** configurado para o relacionamento na ferramenta Esquema.

TÓPICOS RELACIONADOS:

- [“Coluna de Pesquisa” na página 61](#)

Pesquisas Dependentes

Uma pesquisa dependente é uma tabela de pesquisa que depende de outra tabela de pesquisa.

Exemplos típicos de uma tabela de pesquisa dependente são uma tabela de pesquisa de tipos e uma tabela de pesquisa de subtipos. A lista de valores que aparece no campo de subtipo depende do valor selecionado no campo de tipo no IDD. Por exemplo, se você tiver selecionado Estados Unidos em um campo País, quando inserir um valor em um campo Estado, o IDD listará os estados dos EUA armazenados na pesquisa dependente LU_STATE.

Linha do Tempo

A linha do tempo permite exibir e gerenciar eventos de alteração de dados de entidades comerciais e seus relacionamentos. Você pode definir os eventos de alteração de dados ou as versões de entidades comerciais e seus relacionamentos em termos dos seus períodos efetivos.

Alterações de dados ocorrem ao longo do tempo e são independentes do seu relacionamento com outros dados. As alterações no resultado de dados em um novo período de vigência ou em um período de vigência no presente, passado ou futuro. O recurso de linha do tempo permite que você acompanhe essas alterações nos dados ao longo de um período de tempo.

Por exemplo, João Silva morou em São Paulo de 31 janeiro de 2008 a 20 de outubro de 2010. Ele mora em Ribeirão Preto desde 21 de outubro de 2010. Ele vai morar em Varginha a partir de 25 de novembro de 2014. Use linhas do tempo para rastrear alterações aos dados no presente, passado e futuro, como os dados de endereço de João Silva.

Nota: Você pode especificar o período efetivo no formato de data. O sistema usa a localidade de tempo do banco de dados para datas.

Recursos de linha do tempo proporcionam uma visibilidade bidimensional nos dados, com base no período de vigência e no histórico. O período de vigência de um registro é definido pelas datas de início e de término efetivas de um registro de objeto base. O histórico é uma data a partir do histórico de um registro para a qual você precisa exibir o valor. Você pode gerenciar eventos de dados de entidades comerciais, como o endereço do cliente, o número de telefone e os seus relacionamentos por meio da ativação da linha do tempo para objetos base relevantes. Para ativar a linha do tempo de um objeto base filho, primeiro é necessário ativar a linha do tempo do objeto base pai. O MDM Hub usa as tabelas de referência cruzada (XREF) que estão associadas aos objetos base ativados da linha do tempo para manter os períodos de vigência dos registros do objeto base.

Nota: Você deve ativar a linha do tempo para cada objeto base no Console do Hub, exceto para o objeto base de relacionamento filho habilitado para hierarquia.

Para obter mais informações, consulte o *Guia de Configuração do Multidomain MDM*.

Regras de Linha do Tempo

Quando você define e mantém informações de linha do tempo, o MDM Hub aplica regras de linha do tempo.

Você precisa compreender as regras aplicadas pelo MDM Hub para gerenciar linhas do tempo de entidades comerciais e relacionamentos. Em qualquer ponto no tempo, o MDM Hub considera efetiva apenas uma versão de um registro, com base nas datas de início e de término efetivas. Quando você usa processos em lote, a Estrutura de Integração de Serviços ou o Data Director para alterar dados, o MDM Hub persiste os dados efetivos atuais. Além disso, quando vários sistemas contribuem para um registro de objeto base, o MDM Hub aplica regras para atualizar a versão do registro, com base nos registros efetivos contribuintes.

Você também pode usar saídas de usuário para definir e aplicar regras personalizadas para gerenciar linhas do tempo e datas efetivas.

Para obter mais informações, consulte o *Guia de Configuração do Multidomain MDM*.

Indicadores

Indicadores são URLs que abrem um aplicativo IDD e mostram uma exibição, tarefa ou pesquisa.

Nota: Marcadores estão disponíveis para aplicativos IDD que usam o modelo de área de assunto.

A URL especifica qual aplicativo IDD deve ser invocado, qual parte do aplicativo deve ser aberta e qual entidade deve ser exibida. Indicadores podem ser usados para invocar o IDD a partir de um aplicativo externo (por exemplo, o Informatica MDM Data Control ou o IDC) ou de um navegador. Os usuários podem compartilhar uma URL de indicador com outros usuários. Quando o usuário abre a URL em um navegador, ele deve fazer logon com sucesso no aplicativo IDD para visualizar a exibição.

Dentro de um aplicativo IDD, você pode estabelecer um link para comandos Mostrar Indicador nas páginas. Esses comandos fornecem o link de URL para a entidade atual. Indicadores estão disponíveis para as seguintes funcionalidades: Exibição de Dados, Exibição de Hierarquia, tarefas e pesquisas.

O formato da URL é:

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

Em que:

Variável	Descrição
<i>host</i>	Nome da máquina que hospeda o Informatica MDM Hub.
<i>port</i>	Opcional. Número da porta.

Variável	Descrição
<i>operation</i>	Um dos valores a seguir: <ul style="list-style-type: none"> - openrecord;dv - abre uma entidade na Exibição de Dados - openrecord;hm - abre uma entidade na Exibição de Hierarquia - opentask - abre uma janela de tarefa - search - abre uma janela de pesquisa
<i>iddAppName</i>	Nome do aplicativo IDD.
<i>subjectAreaID</i>	Identifica a área de assunto. Usa o seguinte formato: subjectAreaGroupName/SubjectAreaName
<i>param1</i>	Define quais dados devem ser exibidos e depende da operação.
<i>param2</i>	Opcional. Dependente da operação.

Nota: Qualquer caractere não permitido em uma URL deve ser codificado duplamente. A codificação dupla (execução do processo de codificação duas vezes) é necessária para permitir que servidores da Web aceitem solicitações contendo barras ("/" e "\") em seus parâmetros. Solicitações que contêm barras de codificação simples usada em parâmetros são rejeitadas pelos servidores da Web. Somente os valores de parâmetros devem ter codificação dupla.

Exibição de Dados

A operação *openrecord;dv* é usada para abrir uma exibição de dados.

subjectAreaID identifica a área de assunto, enquanto *param1* identifica o registro. Como acontece com APIs SIF, um registro pode ser identificado por rowid ou pelo nome do sistema e pela chave de origem. Ao usar a chave de origem, não se esqueça de incluir espaços à esquerda ou direita no valor.

Além disso, *param2* pode ser usado para especificar *xref*, *history* e *duplicates* de forma a abrir a Exibição de Dados com as telas **Referências Cruzadas**, **Histórico** ou **Localizar Duplicatas**.

Exemplos:

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

Registros mesclados são um caso especial. Se você mesclar um registro com outro, o registro mesclado resultante terá o rowid do registro sobrevivente. Porém, você pode continuar a usar uma URL de indicador que faz referência ao rowid não sobrevivente. Nesse caso, a URL é redirecionada ao rowid de registro mesclado. Por exemplo, digamos que você mescle dois registros com os rowids 1 e 2, e o registro mesclado tenha o rowid 1. Se você usar uma URL de indicador e especificar rowid 2, o link será redirecionado e recuperará o registro mesclado com rowid 1.

Exibição de Hierarquia

A operação *openrecord;hm* é usada para abrir uma Exibição de Hierarquia.

subjectAreaID identifica a área de assunto, enquanto *param1* identifica o registro. O uso desses parâmetros é idêntico ao uso com os parâmetros da Exibição de Dados.

Exemplos:

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

Tarefa

A operação *opentask* é usada para abrir uma tarefa.

subjectAreaID identifica a área de assunto, enquanto *param1* identifica a tarefa, ou seja, simplesmente o valor de ROWID_TASK para a tarefa.

Exemplo:

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

Pesquisar

A operação *search* é usada para abrir uma guia Pesquisar e executar uma pesquisa.

subjectAreaID identifica a área de assunto, enquanto *param1* define os campos e os valores no formulário de pesquisa. Use o comando Mostrar Indicador para ver exemplos de *param1*.

CAPÍTULO 3

Processo de Implementação

Este capítulo inclui os seguintes tópicos:

- [Visão Geral do Processo de Implementação, 29](#)
- [Antes de Iniciar, 29](#)
- [Processo de Configuração, 30](#)

Visão Geral do Processo de Implementação

Esta seção descreve o processo de alto nível recomendado para a configuração de aplicativos do IDD.

Esse processo deve ser usado como modelo para criar planos de implementação do IDD. O objetivo principal é esquematizar as etapas no ciclo de criação/teste que fornecerão um modelo eficiente para o rápido desenvolvimento do IDD. Tal abordagem permite que você use os estágios intermediário do processo de configuração para obter mais feedback e validar requisitos com o cliente.

Antes de Iniciar

Esta seção pressupõe os seguintes pré-requisitos:

- O Informatica MDM Hub, os adaptadores de limpeza e o Servidores de Processos já estão configurados e em operação no seu ambiente. Para obter mais informações, consulte o *Guia de Instalação do Multidomain MDM*.
- Os esquemas do ORS devem estar configurados e conter alguns dados de teste. A configuração de um aplicativo do IDD requer o uso do Gerenciador de Configuração IDD e do Console do Hub. O Console do Hub é usado para criar os elementos de configuração necessários no ORS de destino (como objetos base, pacotes, pesquisas, componentes de caminho de correspondência e assim por diante).
- Todos os objetos base (e metadados associados) exigidos para um aplicativo IDD precisam ser configurados como seguros (SECURE) na ferramenta Recursos Seguros do Console do Hub.
- O processo de configuração e teste inicial precisa ser feito com o uso de uma conta de usuário do MDM Hub que possua privilégios irrestritos para os esquemas do ORS de destino. Você pode usar a conta de administrador ou qualquer outra conta que esteja configurada com todos os privilégios para o grupo ALL_GLOBAL_RESOURCES.

Nota: ALL_GLOBAL_RESOURCES não inclui os recursos personalizados adicionados como parte do aplicativo do IDD - estes devem ser configurados individualmente.

- O processo de análise e modelagem de dados para a definição das áreas de assunto e das regras comerciais deve estar concluído.
- Se você quiser oferecer suporte aos fluxos de trabalho, no MDM Hub, deverá ativar o gerenciamento de estado nas tabelas do objeto base de destino e determinar qual ferramenta BMP deseja usar para o mecanismo de fluxo de trabalho. Talvez você precise concluir as etapas de integração das ferramentas BPM autônomas. Para obter mais informações, consulte o *Guia de Configuração do Multidomain MDM*.
- Outras áreas do Armazenamento de Hub precisam ser configuradas:
 - Segurança
 - Funções de limpeza (se elas forem ser usadas para verificar os dados inseridos pelo usuário do IDD em um aplicativo do IDD)
 - Gerenciador de Hierarquia (se for usado em um aplicativo do IDD).

Nota: Se você ativar o gerenciamento de estado em qualquer entidade Gerenciador de Hierarquia ou em tabelas de relacionamento, deverá ativar o recurso em todas elas.

Para obter mais informações sobre a ferramenta Console do Hub, consulte a ajuda online do Console de Administração ou o *Guia de Configuração do Multidomain MDM*.

Processo de Configuração

Siga o processo de configuração para fazer alterações de configuração no Informatica Data Director.

O processo de configuração é um procedimento repetitivo que não é linear nem único. Você pode gerenciar a maioria das configurações do aplicativo IDD diretamente no Gerenciador de Configuração do Informatica Data Director. Algumas etapas do processo de configuração exigem a edição manual dos componentes do aplicativo IDD.

Se você tiver alterado os metadados no Armazenamento de Referências Operacionais, clique em **Limpar Cache** para obter os metadados mais recentes do MDM Hub.

Nota: Não implante o IDD durante a execução de um trabalho em lote de Carregamento do MDM Hub ou enquanto outro usuário estiver fazendo alterações no Console do MDM Hub. Se você implantar o IDD durante essas atividades do MDM Hub, o IDD gerará erros de validação do Armazenamento de Referências Operacionais.

TÓPICOS RELACIONADOS:

- [“Gerenciador de Configuração IDD” na página 39](#)

Etapa 1. Criar o Aplicativo do IDD

Crie o aplicativo de IDD no Gerenciador de Configuração IDD.

1. Para instâncias do IDD que abrangem vários bancos de dados ORS (ou seja, você pode criar áreas de assunto de diferentes ORSs, mas a área de assunto filho de uma área de assunto deve ser proveniente do mesmo ORS), crie as áreas de assunto individuais para cada ORS separadamente (em aplicativos do IDD separados).
2. Exporte a configuração.

- Integre os arquivos de configuração XML individuais mesclando-os a fim de criar uma instância do IDD com vários ORS.

Considere os seguintes problemas de configuração:

Consideração	Descrição
Sistema de Origem do Aplicativo	<p>A propriedade mais importante definida no nível do aplicativo do IDD é o sistema de origem utilizado por um aplicativo do IDD para acompanhar as atualizações feitas no próprio aplicativo do IDD (como edições feitas por usuários de aplicativo do IDD em uma Exibição de Dados).</p> <p>Por padrão, o sistema Admin é usado. Usando a ferramenta Sistemas e Confiança no Console do Hub, você pode criar um sistema de origem de aplicativo. Para configurar a confiança em colunas de OB para outro sistema, você deve criar uma tabela de preparação fictícia e mapeá-la para o sistema de origem do IDD.</p> <p>Independentemente de qual sistema de origem de aplicativo do IDD for utilizado, este precisa ser configurado para ter o nível mais alto de confiança, de forma a garantir que as alterações aplicadas por usuários de aplicativo do IDD substituam quaisquer outros valores contribuintes e terminem na BVT (registro principal). Se esse não for o caso, os resultados de uma atualização serão muito confusos para os usuários de aplicativos do IDD.</p>
Configuração do HM	<p>Se você estiver planejando usar a funcionalidade HM do IDD, precisará definir o perfil do HM (usando a ferramenta Hierarquias no Console do Hub) que será usado para configurar a funcionalidade Gerenciador de Hierarquia do IDD.</p> <p>A configuração do HM precisa ser especificada com antecedência para garantir que as definições de área de assunto sejam consistentes com as definições de Entidade do HM.</p>

Etapa 2. Configurar Grupos de Áreas de Assunto

Configure grupos de área de assunto.

- Use o Gerenciador de Configuração IDD para criar quaisquer grupos de áreas de assunto necessários. Por exemplo, você pode criar um grupo de áreas de assunto Cliente para conter duas áreas de assunto: Pessoa e Organização.

Etapa 3. Configurar Áreas de Assunto

Configure áreas de assunto.

- Se o grupo de áreas de assunto contiver várias áreas de assunto, identifique o atributo de dados do objeto raiz de área de assunto que será usado para diferenciar as áreas de assunto. Por exemplo, um atributo `party_type` diferenciaria entidades de parte por tipo.

Etapa 3.1. Configurar Áreas de Assunto no Console do Hub

Configure áreas de assunto no Console do Hub.

- No Gerenciador de Esquemas, revise os componentes de caminho de correspondência que estão configurados para o objeto de raiz da área de assunto e verifique se não há caminhos de correspondência para cada um dos objetos filho que precisam ser incluídos nessa área de assunto e para objetos relacionados que precisam ser usados em pesquisas.
- Na ferramenta Pacotes, crie o pacote de exibição de pesquisa que será usado para exibir os resultados de pesquisa da área de assunto. Este é um pacote com o objeto raiz de área de assunto como sua tabela primária.

3. No Gerenciador de Esquemas, verifique dependências de pesquisa de áreas de assunto.

Mecanismo de Pesquisa	Descrição
Tabelas de pesquisa de código	Tabelas de pesquisa de código devem ter o Indicador de Pesquisa definido como TRUE (marcado) nas propriedades do objeto base no Gerenciador de Esquemas.
Pesquisas de Entidade	Pesquisas de entidade podem ser especificadas somente para entidades que estão configuradas como áreas de assunto. Isso pode introduzir dependências complexas entre as áreas de assunto. Como parte do desenvolvimento repetitivo de um aplicativo do IDD, você poderá excluir pesquisas de entidades da configuração do IDD inicial se existirem dependências pelas outras áreas de assunto que não foram configuradas. Os campos de pesquisa poderão ser adicionados depois que todas as dependências de áreas de assunto forem atendidas.

Etapa 3.2. Configurar Áreas de Assunto no Gerenciador de Configuração IDD

Configure áreas de assunto no Gerenciador de Configuração IDD.

1. Crie a configuração básica de áreas de assunto e teste-a validando e implantando o aplicativo.

Essa configuração inclui a definição do layout (colunas a serem exibidas com o tipo de campo e o tamanho de cada uma - este é o mínimo que deve ser configurado), as configurações de correspondência usadas para verificações de duplicatas, a configuração de quaisquer funções de limpeza a serem usadas para verificar os dados inseridos por usuários de aplicativos do IDD (usada para limpeza de dados e/ou validação), a configuração do rótulo para a área de assunto e as atribuições de tarefas de áreas de assunto.

2. Adicione os filhos e os netos à área de assunto.

Todos os filhos e netos precisam ter um caminho de correspondência devidamente configurado para o objeto raiz da área de assunto (configurado no painel Detalhes de Configuração de Correspondência/Mesclagem do Gerenciador de Esquemas). Ao criar um novo filho, o Gerenciador de Configuração IDD exibe os nomes dos componentes de caminho de correspondência, e não os nomes dos objetos filho.

Somente os componentes de caminho de correspondência que forem relevantes para o tipo do filho serão mostrados. Essa configuração inclui definir o layout (colunas a serem exibidas com o tipo de campo e o tamanho de cada uma) e a configuração de uma função de limpeza (opcional) a ser aplicada ao registro (usado para limpeza e/ou validação).

Dica sobre como adicionar filhos e netos

Para simplificar a solução de problemas com a configuração de filhos e netos, considere adicioná-los um de cada vez e, em seguida, implantar/testar a configuração depois que cada um for adicionado (antes da adição do próximo), para isolar qualquer problema de configuração que possa surgir de maneira incremental.

Configuração do Layout

A configuração do layout é usada para:

- Especificar quais campos devem ser mostrados a partir do objeto base.
- Especificar o número de colunas para layouts de forma.
- Especificar o formato de data e hora.
- Especificar o tamanho de campos da interface do usuário para todos os campos (pequeno, médio ou grande).
- Especificar os campos obrigatórios - que não podem ter um valor NULL (isso é configurado no arquivo de configuração do IDD).

- Especificar quais campos devem ser mostrados como hiperlinks.

Nota: Somente tipo de dados de coluna String definido no Console do Hub pode ser marcado com **Mostrar como Hiperlink** no Gerenciador de Configuração IDD. Somente campos com uma URL ou um endereço de e-mail válido serão analisados como um hiperlink.

Etapa 3.3. Validar, Implantar e Testar as Alterações

No aplicativo do IDD, valide, implante e teste as alterações.

1. Crie uma consulta para uma nova pesquisa.
2. Verifique se todos os atributos apropriados estão disponíveis (atributos definidos nos layouts dos objetos raiz e filho).
3. Adicione uma nova entidade (registro) a uma área de assunto.
 - a. Valide se todos os filhos podem ser criados e se todos os campos são exibidos na ordem esperada.
 - b. Valide se todos os campos de pesquisa são exibidos corretamente e têm a lista de valores correta. Se os campos não exibirem os controles de pesquisa, você precisará ajustar a configuração do campo de Pesquisa (definir o Indicador de Pesquisa como TRUE no Gerenciador de Esquemas).

Etapa 3.4. Configurar Outras Guias Filho

Para configurar guias filho de áreas de assunto adicionais, atualize o arquivo de configuração do Informatica Data Director.

Você pode configurar guias filho de áreas de assunto **Parte de Objeto Primário de e XREF**.

Etapa 4. Configurar a Limpeza e a Validação

Validação e limpeza são elementos opcionais para primaryObject, one2ManyChild e many2ManyChild.

O Gerenciador de Configuração IDD não cria o elemento cleanseFunction: ele apenas associa a função de limpeza a colunas no objeto base.

Os dados que o usuário de aplicativo do IDD inseriu nos atributos da área de assunto são alimentados na função de limpeza como entradas. O registro de objeto base é então atualizado pelas saídas da função de limpeza.

A função de limpeza poderá relatar erros de validação se estiver configurada com uma saída validationStatus. Se forem encontrados erros de validação, o aplicativo do IDD exibirá todos os erros ao lado de quaisquer campos com problemas.

1. Crie a biblioteca de funções de validação usando a amostra de ValidationCleanseLib no Kit de Recursos do Informatica MDM Hub como modelo.
2. Usando a ferramenta Funções de Limpeza no Console do Hub, implante a biblioteca de limpeza criada no ORS.
3. Usando as ferramentas Funções de Limpeza e Mapeamentos no Console do Hub, crie funções de limpeza e mapeamentos a serem usados em aplicativos do IDD.
4. Usando o Gerente de Configuração, configure essas funções para uso em um aplicativo do IDD (na caixa de diálogo Editar área de assunto).
5. Implante e teste as funções de limpeza e validação. Verifique se todos os campos estão devidamente limpos e validados.

Etapa 5. Configurar a Pesquisa

A configuração da pesquisa envolve a Pesquisa Básica e a Pesquisa Estendida, bem como consultas públicas.

A Pesquisa Avançada vem pré-configurada, sem definições de configuração editáveis.

Etapa 5.1. Configurar a Pesquisa Básica

A Pesquisa Básica permite que usuários de aplicativos do IDD procurem instâncias de área de assunto por meio da criação de consultas na área de assunto.

Os resultados são exibidos usando um pacote do MDM Hub que é criado com a ferramenta Pacotes no Console do Hub. O IDD usa o novo modo da API **searchQuery** para exibir os resultados.

O pacote de pesquisa precisa atender aos seguintes critérios:

- Baseado no objeto base raiz da área de assunto.
- Retorna uma única linha de resultado para cada entidade de área de assunto.
- Contém o ROWID_OBJECT do objeto base raiz da área de assunto.

O pacote usado para a pesquisa deve conter as colunas que são necessárias para apresentar os resultados da pesquisa ao usuário. Um aplicativo IDD pesquisa diretamente com base em um objeto base raiz e nos filhos associadas. Ele não consulta com base nos atributos do pacote de exibição.

O IDD não remove duplicatas dos resultados da pesquisa. Um pacote precisa ser construído de forma a retornar uma única linha para cada entidade encontrada.

1. Para garantir que um pacote de pesquisa retorne uma única linha para cada entidade, teste o pacote de pesquisa diretamente via SQL. Um método de teste é executar verificações rápidas nas entidades com um número conhecido de filhos de diferentes tipos.
2. Identifique os atributos pesquisáveis primários. No Gerenciador de Esquemas, crie os índices personalizados adequados para dar suporte a essas pesquisas.
3. Para testar as pesquisas, crie os diferentes tipos de consultas e execute-os em um aplicativo IDD. Use diferentes combinações de critérios de pesquisa para garantir o desempenho satisfatório dessas pesquisas.
4. Além disso, a pesquisa pode ser configurada para objetos que não fazem parte da área de assunto quando você utiliza a guia Pesquisa em Filho na configuração de pesquisa. Isso permite que você pesquise em qualquer objeto para o qual existe um caminho de correspondências a partir do objeto primário. Esses objetos estarão disponíveis no Construtor de Consultas.

A Pesquisa em Filho permite pesquisar os seguintes tipos de dados:

- Dados relacionados que não fazem parte da área de assunto.
- Referências cruzadas de dados dentro da área de assunto.
- Em geral, quaisquer dados que podem ser relacionados ao objeto primário por um caminho de correspondência.

Etapa 5.2. Configure a Pesquisa Estendida

A Pesquisa Estendida usa a API **searchMatch** para solicitar pesquisas difusas pelos dados.

1. É necessário garantir que todas as colunas de correspondência necessárias tenham sido criadas. Nenhuma configuração extra é necessária em um aplicativo do IDD para ativar a pesquisa difusa. O IDD mapeará automaticamente os critérios de pesquisa fornecidos pelo usuário de aplicativo do IDD para as colunas ativadas para correspondência disponíveis e, em seguida, executará a pesquisa.

2. Antes de testar a configuração da Pesquisa Estendida, verifique se os dados foram devidamente tokenizados e, em seguida, teste os recursos de pesquisa difusa criando as consultas de pesquisa de forma a incluir os atributos de área de assunto que possuem colunas ativadas para correspondência subjacentes.

Para obter mais informações, consulte "Configurando o processo de correspondência" no *Guia de Configuração do Multidomain MDM* ou na ajuda online do Console do Hub, bem como a descrição da API `searchMatch` no *Guia da Estrutura de Integração de Serviços do Multidomain MDM* ou no Javadoc.

3. A Pesquisa Estendida usa a API **`searchMatch`** com `matchType=NONE`. Na configuração padrão, todas as colunas de correspondência possíveis são geradas em cada solicitação `searchMatch`. O IDD pode ser configurado para gerar apenas colunas de correspondência específicas. Na guia Pesquisar da caixa de diálogo da área de assunto, você pode especificar o conjunto específico de colunas de correspondência que devem ser geradas.

Nota: Por padrão, nesse modo de `searchMatch`, o nível de pesquisa usa "Estreito" como padrão. Este é o nível mais restritivo, mas pode ser substituído por meio da definição da seguinte configuração em `cmxcleanse.properties`:

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

em que `<level>` é uma das seguintes configurações: Estreito, Típico, Abrangente ou Extremo. Para obter mais informações sobre níveis de pesquisa em propriedades de conjuntos de correspondências, consulte "Configurando o processo de correspondência" no *Guia de Configuração do Multidomain MDM*.

Etapa 5.3. Configurar Consultas Públicas

O IDD permite que administradores e usuários avançados compartilhem as consultas que eles criam com todos os outros usuários.

- Recomendamos que você configure como pública pelo menos uma pesquisa usada com mais frequência para cada uma das áreas de assunto definidas em um aplicativo do IDD.

Isto permitirá que os usuários naveguem rapidamente por todas as áreas de assunto sem a necessidade de criar suas próprias versões das consultas comuns.

Pesquisa sem Distinção entre Maiúsculas e Minúsculas

A Pesquisa Estendida, por se basear na capacidade de correspondência do Informatica MDM Hub, não faz distinção entre maiúsculas e minúsculas.

Em geral, pesquisas sem distinção entre maiúsculas e minúsculas não estão disponíveis para a Pesquisa Básica. Uma exceção é quando todos os dados da área de assunto já estão todos em maiúsculas ou minúsculas. Nesse cenário, a API `searchQuery` pode ser configurada para converter os termos de pesquisa de entrada em maiúsculas ou minúsculas antes de executar a consulta. Para mais informações, consulte a descrição de `SearchQuery` no *Guia da Estrutura de Integração de Serviços do Multidomain MDM* ou no Javadoc.

Etapa 6. Configurar o processo de correspondência

Configure como o processo de correspondência identifica registros duplicados.

Você configura o processo de correspondência na guia **Configurações de Correspondência** da caixa de diálogo **Área de Assunto**. Você especifica um conjunto de regras de correspondência predefinido e o tipo de correspondência. Também pode selecionar colunas de correspondência.

Para obter mais informações sobre como definir configurações de correspondência, consulte o *Ajuda Online do Gerenciador de Configuração do Multidomain MDM Data Director*. Para obter mais informações sobre

regras de correspondência e conjuntos de regras de correspondência, consulte o *Guia de Configuração do Multidomain MDM*.

Etapa 7. Configurar Fluxos de Trabalho MDM

Você pode configurar o aplicativo Data Director (IDD) para usar os fluxos de trabalho MDM predefinidos que são implantados quando você instala o ActiveVOS Server incorporado.

A etapa seguinte depende de se o seu ambiente MDM inclui o ActiveVOS Server:

- Se o seu ambiente incluir o ActiveVOS Server, selecione o fluxo de trabalho do MDM que você deseja usar como o fluxo de trabalho de aprovação.
- Se o seu ambiente não incluir o ActiveVOS Server, instale-o usando o instalador do Servidor de Hub. Para obter mais informações, consulte o *Guia de Instalação do Multidomain MDM*.

TÓPICOS RELACIONADOS:

- [“Fluxos de Trabalho e Tarefas” na página 141](#)
- [“Configuração Manual do IDD” na página 58](#)

Definindo um Fluxo de Trabalho de Aprovação Padrão para a Exibição de Dados de Área de Assunto

Quando os administradores de dados alteram dados mestre, eles podem enviar a atualização para aprovação clicando no botão **Enviar para Aprovação**. Essa ação abre a caixa de diálogo Criar Tarefa. O fluxo de trabalho de aprovação padrão é exibido no campo Tipo de Tarefa.

Antes de modificar o tipo de tarefa para definir um fluxo de trabalho de aprovação padrão, verifique se não há nenhuma tarefa no painel Tarefas do IDD.

1. No Configuration Manager do IDD, selecione o aplicativo e clique em **Editar**.
2. Clique na guia **Tarefas**.
3. Em Tipos de Tarefa, clique no tipo de tarefa com o nome do fluxo de trabalho de aprovação que você deseja usar como padrão e clique em **Editar**.
4. Marque a caixa de seleção **Criar tipo de tarefa por padrão ao aprovar** e clique em **OK**.

Nota: Se a caixa de seleção estiver desativada, outro tipo de tarefa terá essa opção definida. Edite os outros tipos de tarefa para localizar o tipo de tarefa com essa opção definida e desmarque a caixa de seleção. Em seguida, você poderá definir a opção no tipo de tarefa de fluxo de trabalho preferencial.

Atualizando fluxos de trabalho para oferecer suporte a várias ações de tarefa

Você pode configurar um fluxo de trabalho ActiveVOS para permitir que os revisores realizem várias ações em uma tarefa sem fechar a guia Tarefa. Para cada ação de tarefa na qual você deseja permitir várias ações sem fechar a guia Tarefa, defina a propriedade `closeTaskView` como `false`.

1. Abra o designer do ActiveVOS.
2. Abra o arquivo de fluxo de trabalho `.bpel`.
3. Para cada ação de tarefa que você deseja alterar, edite a definição da ação e especifique o seguinte parâmetro:

```
<mdmavxsd:closeTaskView>false</mdmavxsd:closeTaskView>
```

4. Implante o arquivo `.bpel` no ActiveVOS.

Etapa 8. Configurar a Segurança

Toda a segurança de aplicativos no Data Director é controlada por diretivas do Gerenciador de Acesso de Segurança (SAM) do MDM Hub configuradas no Console do Hub.

Os comportamentos do aplicativo Data Director podem ser muito sensíveis à configuração de segurança.

1. Para configurar e testar o aplicativo para o Data Director, use o usuário administrador ou um usuário com privilégios totais para todos os recursos seguros.

Para obter mais informações, consulte o *Guia de Segurança do Multidomain MDM*.

2. Para cada área de assunto, você pode configurar filtros de segurança em nível de linha. Por padrão, não há filtros de segurança definidos.

Na guia Pesquisar da caixa de diálogo de área de assunto, você pode configurar regras de segurança de dados.

3. Para qualquer usuário, as funções de usuário atribuídas podem incluir vários filtros de dados.

Por exemplo, um usuário pode ter direitos para registros com um endereço no CA por meio de uma função e direitos para registros com um endereço em NY por meio de outra função.

TÓPICOS RELACIONADOS:

- [“Segurança de Dados” na página 119](#)
- [“Configuração de Segurança do IDD” na página 112](#)

Etapa 9. Configurar Extensões da Interface do Usuário

Configure as extensões da interface do usuário.

1. Um aplicativo do IDD pode ser personalizado por meio da incorporação de conteúdo externo na página da Web e da invocação de ações de determinados locais no aplicativo do IDD.

O conteúdo pode ser incorporado usando o seguinte:

Elemento	Descrição
Guia de nível superior	Guias podem ser adicionadas ao lado das guias do Iniciar espaço de trabalho, do espaço de trabalho Dados e do espaço de trabalho Tarefas.
Iniciar espaço de trabalho	Um componente ou widget pode ser adicionado ao Iniciar espaço de trabalho.
Guia Filho na Exibição de Dados	Guias podem ser adicionadas como filhos de uma área de assunto.

2. Ações personalizadas podem ser configuradas de forma a serem invocadas de itens de menu em vários locais de um aplicativo do IDD.

Informações contextuais podem ser transmitidas durante a invocação da ação externa.

A seguinte tabela mostra áreas de um aplicativo do IDD em que essas ações podem ser configuradas, juntamente com os dados contextuais disponíveis.

Área	Dados Contextuais Disponíveis
Área de Assunto	rowid_object e dados do objeto primário
Filho de Um-para-Muitos	rowid_object e dados do filho
Filho de Muitos-para-Muitos	rowid_object e dados do filho
Resultados da pesquisa	rowid_object dos dados selecionados na lista de resultados de pesquisa

TÓPICOS RELACIONADOS:

- [“Extensões da Interface do Usuário” na página 73](#)

Etapa 10. Localizar o Aplicativo

Quatro conjuntos de pacotes de recursos contêm as strings que são exibidas em um aplicativo IDD.

Cada conjunto inclui os seguintes componentes:

- O arquivo padrão.
- Um arquivo de espaço reservado no idioma inglês. Esse arquivo pode estar vazio.
- Versões localizadas do arquivo, se necessárias.

Por exemplo, para o conjunto MessageBundle, há o arquivo padrão MessageBundle.properties e o arquivo no idioma inglês de espaço reservado, MessageBundle_en.properties.

Cada arquivo de pacote de recursos é um arquivos de propriedades codificado em UTF-8. Cada entrada no arquivo é um par de nome/valor, <name>=<value>. Exemplos:

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

Para cada entrada:

- <name> é um valor fixo que é referenciado pelo aplicativo IDD e não pode ser alterado
- <value> é a parte que pode ser localizada

Para localizar o aplicativo:

- ▶ Use o Gerenciador de Configuração IDD para adicionar arquivos de pacote de recursos a um aplicativo IDD, incluindo-as no arquivo ZIP do aplicativo que é importado ou os importando individualmente em um aplicativo IDD existente.

TÓPICOS RELACIONADOS:

- [“Componentes de Aplicativo” na página 111](#)

CAPÍTULO 4

Gerenciador de Configuração IDD

Este capítulo inclui os seguintes tópicos:

- [Visão Geral do Gerenciador de Configuração IDD, 39](#)
- [Iniciando o Gerenciador de Configuração do Informatica Data Director, 40](#)
- [Página Inicial, 40](#)
- [Associação do ORS, 41](#)
- [Adicionar um Aplicativo do IDD, 42](#)
- [Importar uma Configuração de Aplicativo do IDD, 42](#)
- [Validação, Estado do Aplicativo e Implantação, 43](#)
- [Editar Aplicativo, 45](#)
- [Pacote de provedor de logon personalizado, 50](#)

Visão Geral do Gerenciador de Configuração IDD

O Gerenciador de Configuração IDD é usado para adicionar, modificar e gerenciar aplicativos do IDD.

Um aplicativo do IDD consiste em um arquivo de configuração XML, pacotes de recursos, arquivos de ajuda e outros componentes. Um aplicativo do IDD completo pode ser importado ou exportado como um arquivo ZIP contendo todos esses componentes.

O Gerenciador de Configuração IDD foi projetado para criar e manter a configuração de um aplicativo do IDD. Ele não expõe todas as opções de configuração disponíveis: algumas funcionalidades devem ser configuradas manualmente, exportando e editando o arquivo de configuração XML diretamente e depois reimportando o arquivo de volta para o Gerenciador de Configuração IDD.

TÓPICOS RELACIONADOS:

- [“Componentes de Aplicativo” na página 111](#)
- [“Configuração Manual do IDD” na página 58](#)

Iniciando o Gerenciador de Configuração do Informatica Data Director

Para iniciar o Gerenciador de Configuração do Informatica Data Director, use um navegador da Web com suporte.

1. Abra um navegador da Web com suporte.

Para obter informações sobre navegadores da Web com suporte, consulte a Matriz de Disponibilidade de Produtos no Portal do Meu Suporte da Informatica, em <https://mysupport.informatica.com/community/my-support/product-availability-matrices>.

2. Na barra de endereços, insira o seguinte URL para acessar a página de logon do Gerenciador de Configuração do IDD:

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

3. Insira o nome de logon e a senha e clique em **Fazer Logon**.

Você deve fazer logon como um usuário que tem todos os privilégios para todos os objetos base. Para obter mais informações sobre a configuração de privilégios de usuário, consulte o *Guia de Segurança do Multidomain MDM*.

O Gerenciador de Configuração do Informatica Data Director é iniciado, e a página Aplicativos é exibida.

Página Inicial

A página inicial do IDD consiste nos seguintes elementos:

Elemento	Descrição
Lista de aplicativos	Lista de aplicativos existentes do IDD.
Barra de Comando	Comandos disponíveis (descritos a seguir)
Resumo de Aplicativos	Resumo de aplicativos do IDD existentes, incluindo as seguintes propriedades: <ul style="list-style-type: none">- Nome lógico e nome de exibição- Status de validação- Status da implantação- URL para iniciar o aplicativo do IDD
Tipos de Componentes	Disponível apenas se o recurso Componentes de Dados da Informatica (IDC) estiver licenciado para a sua implementação do Informatica MDM Hub. Para obter mais informações, consulte o <i>Ajuda Online do Gerenciador de Configuração do Multidomain MDM Data Director</i> e o <i>Guia de Implementação dos Componentes de Dados do Multidomain MDM</i> .
Configurações do Provedor de Logon	Atalho para a tela de configuração do módulo de Provedor de Logon Personalizado (Suporte para SSO).

A barra de comandos do IDD contém os seguintes comandos:

Comando	Descrição
Adicionar	Adiciona um novo aplicativo do IDD.
Editar	Edita a configuração do aplicativo do IDD selecionado.
Excluir	Exclui o aplicativo do IDD selecionado.
Exportar	Exporta uma configuração de aplicativo do IDD (arquivo ZIP).
Validar	Valida o aplicativo do IDD selecionado.
Migrar Pacote	Migre o pacote de metadados para localizar elementos da interface do usuário no aplicativo IDD.
Estado do Aplicativo	Altera o estado de implantação do aplicativo do IDD: completo, limitado ou não implantado.
Importar	Importa uma configuração de aplicativo do IDD (veja a seguir para conhecer os formatos).
Reimplantar	Remove e reimplanta um aplicativo do IDD.
Limpar Cache	Limpa o cache local do IDD para o aplicativo do IDD selecionado. Esse cache armazena metadados do Hub e deve ser limpo em caso de alterações nesses metadados.

Também há ajuda online disponível em qualquer página do Gerenciador de Configuração.

Associação do ORS

Uma configuração de aplicativo do IDD declara um ou mais bancos de dados ORS lógicos.

Um *banco de dados ORS lógico* é um ponteiro de configuração do IDD para um banco de dados ORS físico no Armazenamento de Hub que está configurado no Console do Hub. Todos os objetos do Informatica MDM Hub que são referenciados em uma configuração estão sempre no contexto de um determinado ORS lógico. Para que uma configuração do IDD seja válida, os objetos que ele referencia devem existir no ORS físico associado.

Quando um aplicativo do IDD é adicionado ou importado, os bancos de dados ORS lógicos que ele declara devem ser associados a um ORS físico registrado no Informatica MDM Hub.

A associação do ORS é usada para conectar um aplicativo do IDD a um ORS e para validar a configuração. Além disso, a associação do ORS é usada pelo Gerenciador de Configuração IDD para buscar metadados sobre o ORS.

Adicionar um Aplicativo do IDD

O comando Adicionar é usado para criar um novo aplicativo do IDD.

Um novo aplicativo do IDD é definido por seu nome, nome de exibição, descrição e lista de bancos de dados ORS lógicos. Depois de adicionar o aplicativo, escolha o comando Editar para fazer alterações mais detalhadas na configuração do aplicativo (como adicionar áreas de assunto).

Importar uma Configuração de Aplicativo do IDD

O comando Importar é usado para criar ou atualizar um aplicativo do IDD.

Ele fornece as seguintes três opções de importação - duas para importar um aplicativo completo e uma para importar um componente em um aplicativo existente:

Opção de Importação	Descrição
Importar somente configuração do IDD (XML)	<p>Criar um novo aplicativo do IDD importando o XML de configuração do IDD. Isso pode ser usado para substituir um aplicativo do IDD com o mesmo nome. Em caso afirmativo, o aplicativo existente é substituído inteiramente (como se você tivesse executado uma exclusão seguida de uma importação).</p> <p>Se um aplicativo com o nome do novo aplicativo já existir, você poderá usar a opção para importar esse aplicativo com um nome diferente.</p> <p>Nota: Se estiver substituindo um aplicativo do IDD, você precisará reconfigurar os Privilegios de Recursos atribuídos para todas as funções no Console do Hub.</p>
Importar aplicativo IDD completo (Zip)	<p>Crie um novo aplicativo do IDD ao importar um arquivo .zip que contém os vários arquivos de componentes, como XML, pacotes de recursos e arquivos de ajuda. O tamanho máximo do arquivo .zip que você pode importar é de 20 MB.</p> <p>Em ambientes IBM DB2, para importar um arquivo com mais de 1 MB, execute o seguinte comando para definir o tamanho máximo de arquivo permitido:</p> <pre>ALTER TABLE CMX_SYSTEM.C_REPOS_DS_CONFIG ALTER COLUMN BLOB_DATA SET DATA TYPE BLOB(<i>tamanho máximo do arquivo, bytes</i>);</pre> <p>Nota: Se estiver substituindo um aplicativo do IDD, você precisará reconfigurar os Privilegios de Recursos atribuídos para todas as funções no Console do Hub.</p>
Importar para aplicativo IDD existente	<p>Atualize um aplicativo do IDD importando um arquivo individual. Ele é usado para adicionar ou substituir qualquer um dos arquivos de componentes do aplicativo do IDD.</p> <p>Nota: Você também pode usar essa opção ao promover alterações de um ambiente para outro ambiente.</p>

TÓPICOS RELACIONADOS:

- [“Componentes de Aplicativo” na página 111](#)

Validação, Estado do Aplicativo e Implantação

Os seguintes parâmetros persistentes determinam como e se um aplicativo do IDD está implantado.

Parâmetro	Descrição
valid_ind	Contém o status de validação mais recente do aplicativo. O status de validação é um valor único que representa o erro mais alto (mais grave) que foi encontrado.
active_ind	Gerenciado diretamente pelo usuário para refletir a intenção de implantação do aplicativo.

Validação

Uma configuração de aplicativo do IDD é conectada flexivelmente com os metadados em um ORS.

A configuração contém referências a objetos em um ORS. As alterações em um ORS (adição, modificação ou remoção de objetos base, colunas, funções de limpeza e assim por diante) não são automaticamente refletidas na configuração do IDD. Por esse motivo, o processo de validação do IDD é necessário e deve ser repetido periodicamente.

A validação é executada nas seguintes circunstâncias:

- quando solicitado pelo usuário no Gerenciador de Configuração IDD
- ao importar uma configuração do IDD
- antes de implantar um aplicativo, quando o servidor de aplicativos é inicializado

Os seguintes níveis de validação estão disponíveis.

valid_ind	Nível de Validação	Descrição
-1	Não Validado	O aplicativo do IDD não foi validado.
0	Nenhum Erro	Nenhum erro ou aviso foi encontrado durante a validação.
1	Informações	Fornece informações para o usuário. Nenhuma alteração de configuração é necessária.
2	Aviso	Uma configuração talvez precise ser alterada, mas não deve causar problemas de tempo de execução.
3	Erro	Um erro de configuração deve ser corrigido. Problemas de tempo de execução podem ser esperados.
4	Erro Crítico	Igual a Erro, mas indica um problema que requer atenção ainda mais urgente.
5	Erro Fatal	Um erro que impede a execução geral do aplicativo do IDD. O aplicativo não será implantado em nenhuma circunstância.

Estado do Aplicativo

O estado do aplicativo é controlado pelo usuário no Gerenciador de Configuração IDD.

Ele armazena a implantação pretendida para o aplicativo do IDD.

Nota: Um aplicativo do IDD pode ser implantado mesmo quando a configuração contém erros. Somente erros fatais (descritos na seção anterior) impedirão que um aplicativo do IDD seja implantado. Pode ser útil implantar um aplicativo do IDD que contém erros durante a criação de um aplicativo, permitindo que o implementador teste partes da configuração enquanto outras partes estão incompletas.

active_ind	Nome	Descrição
-1	Não Implantado	O aplicativo do IDD não está implantado. Útil quando o aplicativo está em desenvolvimento. Alterações podem ser feitas e salvas sem a sobrecarga adicional de implantar o aplicativo.
0	Implantação Limitada	O aplicativo do IDD está implantado, mas somente os usuários que são administradores podem fazer logon. O aplicativo não será exibido na lista de aplicativos disponíveis. Você deve acessar o aplicativo usando sua URL completa: <code>http://<hostname>[:<port>]/bdd?bdd_name=name</code>
1	Implantação Total	O aplicativo do IDD está implantado para uso completo. Ele é exibido na lista de aplicativos, e qualquer usuário autorizado pode executá-lo.

Implantação

Implantação é o processo de obter uma configuração do IDD e disponibilizá-la como um aplicativo.

Um aplicativo não está implantado quando active_ind é -1 para esse aplicativo.

A implantação ocorre em resposta aos seguintes eventos:

Evento	Descrição
Inicialização do Servidor de Aplicativos	Todos os aplicativos do IDD com active_ind diferente de -1 são validados primeiramente. Se o nível de validação não for Erro Fatal, o aplicativo do IDD será implantado. No momento, somente uma validação parcial é executada para verificar se há erros fatais.
Importar/Salvar	A qualquer momento que um aplicativo do IDD é importado ou salvo, ele também é implantado, a menos que seu active_ind seja -1.
Reimplantação	O usuário reimplanta um aplicativo do IDD.

Editar Aplicativo

Na tela Editar Aplicativo, é possível visualizar e editar os detalhes de configuração para um aplicativo do IDD selecionado. O IDD usa metadados do ORS lógico para apresentar as opções de configuração disponíveis.

As seguintes guias estão disponíveis na parte inferior da tela:

Guia	Descrição
Áreas de Assunto	Definem grupos de áreas de assunto, áreas de assunto, filhos e netos de área de assunto para o aplicativo do IDD selecionado.
Tarefas	Definem as tarefas selecionadas para o aplicativo do IDD selecionado. Para obter mais informações, consulte a ajuda online do Gerenciador de Configuração.
Controles	Disponível apenas se o recurso Componentes de Dados da Informática (IDC) estiver licenciado para a sua implementação do Informática MDM Hub. Para obter mais informações, consulte o <i>Ajuda Online do Gerenciador de Configuração do Multidomain MDM Data Director</i> e o <i>Guia de Implementação dos Componentes de Dados do Multidomain MDM</i> .

Os seguintes botões de comando também estão disponíveis:

Botão	Descrição
Salvar	Salva as alterações mais recentes no banco de dados. Se o estado do aplicativo for qualquer coisa diferente de Não Implantado (-1), o aplicativo do IDD será reimplantado depois que você salvar as alterações.
Validar	Executa a validação na configuração do aplicativo do IDD atual e exibe o relatório de validação.
Associação	Usado para alterar a associação ao ORS lógico.
Gerar Esquema da Entidade Comercial	Gera arquivos de configuração para todas as entidades comerciais no aplicativo do IDD.
Migrar	Migra o pacote de metadados para localizar elementos da interface do usuário no aplicativo IDD.

TÓPICOS RELACIONADOS:

- [“Áreas de Assunto” na página 46](#)

Bancos de Dados ORS Lógicos

Ao editar uma configuração, a primeira tarefa a ser concluída é a configuração dos bancos de dados ORS lógicos.

Para cada um desses bancos de dados ORS, você deve selecionar um sistema de origem.

Se o Gerenciador de Hierarquia for ser usado pelo aplicativo do IDD, a configuração do HM também deverá ser selecionada. O ícone à direita da lista suspensa Configuração do HM é usada para configurações de parâmetros adicionais do HM (como saltos e configurações de relacionamento).

Nota: No Gerenciador de Configuração IDD, na janela **Configurações do HM**, o valor para **Total de Relacionamentos** não deve exceder 2000.

Tempo Limite da Sessão

Na tela Editar Aplicativo, é possível definir um tempo limite de sessão para um aplicativo do IDD selecionado.

Para definir o tempo limite de sessão, insira um valor em minutos no campo **Tempo Limite da Sessão**. Em seguida, salve o aplicativo do IDD. Por padrão, uma sessão expira depois de 30 minutos.

Se você alterar o valor de tempo limite da sessão, todas as sessões ativas no IDD se tornarão inválidas, e os usuários deverão fazer login novamente.

Áreas de Assunto

A guia Áreas de Assunto na parte inferior da tela fornece uma árvore que mostra como o aplicativo do IDD está configurado.

À medida que itens são selecionados na árvore, os botões Adicionar, Editar e Excluir são atualizados para refletir as opções disponíveis. Os níveis na árvore são:

Nível da Árvore	Descrição
Aplicativo do IDD	Grupos de áreas de assunto podem ser adicionados.
Grupo de Áreas de Assunto	<p>O grupo de áreas de assunto pode ser editado ou excluído. Áreas de assunto pode ser adicionadas.</p> <p>O grupo de áreas de assunto identifica o ORS lógico ao qual as áreas de assunto filho pertencem e qual objeto base é a tabela primária para essas áreas. Um grupo de áreas de assunto pode ter uma ou mais áreas de assunto filho: todas compartilhando a mesma tabela primária. Essas áreas de assunto são agrupadas no aplicativo do IDD.</p>
Área de Assunto	<p>A área de assunto pode ser editada ou excluída. Filhos de áreas de assunto podem ser adicionados.</p> <p>Se o grupo de áreas de assunto contiver mais de uma área de assunto, cada uma definirá o qualificador de tipo ou subtipo de entidade do HM que identifica a área de assunto. Você também especifica:</p> <ul style="list-style-type: none">- o pacote usado para exibir resultados de pesquisa- o conjunto de regras de correspondência e o tipo de correspondência a serem usados para verificações de duplicatas- as colunas da tabela Primária que fazem parte dessa área de assunto
Filho da Área de Assunto	<p>O filho da área de assunto pode ser editado ou excluído. Para cada filho de área de assunto, você deve especificar:</p> <ul style="list-style-type: none">- o tipo de relacionamentos (um-para-muitos, muitos-para-muitos e assim por diante)- que caminho de correspondência leva à tabela filho (a lista de caminhos de correspondência é preenchida com base na seleção do tipo de relacionamento)- As colunas da tabela filho que devem ser exibidas.
Neto da Área de Assunto	<p>O neto da área de assunto pode ser editado ou excluído. Para cada neto de área de assunto, você deve especificar:</p> <ul style="list-style-type: none">- o tipo de relacionamento (um-para-muitos, muitos-para-muitos e assim por diante)- que caminho de correspondência leva à tabela filho (a lista de caminhos de correspondência é preenchida com base na seleção do tipo de relacionamento)- As colunas da tabela filho que devem ser exibidas.

Propriedades do Grupo de Áreas de Assunto

A caixa de diálogo usada para adicionar e editar um grupo de áreas de assunto é usada para configurar:

- Nome e nome de exibição. O nome é o identificador interno para essa área de assunto e deve consistir apenas em caracteres alfanuméricos: caracteres especiais não são permitidos.
- ORS lógico ao qual o grupo de áreas de assunto está associado
- Tabela primária para as áreas de assunto no grupo:

Recurso	Descrição
Nome e Nome de Exibição	São usados para identificar o grupo de áreas de assunto. O nome é o identificador interno para esse grupo de áreas de assunto e deve consistir apenas em caracteres alfanuméricos: caracteres especiais não são permitidos.
ORS Lógico	Configura de qual ORS Lógico os objetos nesse grupo de áreas de assunto são provenientes.
Tabela Primária	Configura qual objeto base é a tabela primária ou raiz para as áreas de assunto no grupo de áreas de assunto.
Somente Pesquisa	Esse recurso é selecionado para um grupo de áreas de assunto que possui dados criados e mantidos fora de um aplicativo do IDD. As áreas de assunto definidas nesse grupo são visíveis dentro de um aplicativo do IDD somente durante a criação de uma chave externa a partir de outra área de assunto (a pesquisa é usada para localizar o registro a ser relacionado).

Propriedades da Área de Assunto

A caixa de diálogo usada para adicionar e editar uma área de assunto é usada para configurar as seguintes propriedades:

- Nome e nome de exibição: o nome é o identificador interno para essa área de assunto e deve consistir apenas em caracteres alfanuméricos: caracteres especiais não são permitidos. Um nome de área de assunto não pode começar com um número.
- Tipo de entidade do HM: Essa propriedade define os tipos de objetos que podem ser relacionados, se houver.
- Pacote de exibição de resultados de pesquisa: Essa propriedade é usada para exibir resultados de pesquisa para essa área de assunto. O pacote deve ter a tabela primária do grupo de áreas de assunto como sua tabela primária.
- Colunas de link de Possíveis Correspondências: Essa propriedade define qual coluna de um layout deve ser exibida como um hiperlink que abre uma entidade de Possível Correspondência em uma nova guia Exibição de Dados.
- Coluna de subtipo: Essa propriedade especifica a coluna usada para o filtro de subtipo: O código de tipo (categoria) para essa área de assunto. Definido automaticamente quando um Tipo de Entidade do HM é selecionado.
- Valor de subtipo: Essa propriedade especifica o valor usado para o filtro de subtipo. Definido automaticamente quando um Tipo de Entidade do HM é selecionado.
- Número de Colunas Congeladas: Essa propriedade mostra o número de colunas congeladas nos resultados de pesquisa da área de assunto.
- Mostrar XREF: Se selecionada, o aplicativo do IDD exibirá uma guia filho para a área de assunto que exibe as referências cruzadas do objeto primário.

- Guias para definir as seguintes configurações:

Recurso	Descrição
Layout	Configura quais colunas do objeto base estão disponíveis no aplicativo IDD para exibição e edição, que tipo de componente de interface do usuário deve ser usado e, se for uma pesquisa, se os dados da pesquisa estão localizados.
Configurações de Correspondência	Configura o conjunto de regras de correspondência e o tipo de correspondência a serem usados para verificações de duplicatas.
Pesquisar	Configura propriedades de pesquisa.
Segurança de Dados	Configura a segurança em nível de linha baseada em função para a área de assunto.
Mascaramento de dados	Configura o mascaramento de dados baseado em função para colunas que estão selecionadas na guia Layout.
Limpar	Configura a função de limpeza a ser usada para limpeza e validação.
Rótulo	Configura como um rótulo é gerado para a área de assunto. Esse rótulo é usado, por exemplo, como o título de uma guia Exibição de Dados.
Atribuição de Tarefas	Configura como as tarefas são atribuídas. Especifica a lista de funções e o usuário para cada tipo de tarefa.
Ordem de Filhos	Configura a ordem das guias filho para a área de assunto.

Propriedades de Filhos e Netos da Área de Assunto

A caixa de diálogo usada para adicionar e editar uma área de assunto é usada para configurar as seguintes propriedades:

- Nome e nome de exibição. O nome é o identificador interno para um filho ou neto de área de assunto e deve consistir apenas em caracteres alfanuméricos: caracteres especiais não são permitidos.
- Tipo de filho - o tipo de relacionamento com o pai
- Caminho de Correspondência para Filho - o componente de caminho de correspondência que leva até esse objeto filho
- Guias para definir as seguintes configurações:

Recurso	Descrição
Layout	Configura quais colunas do objeto base estão disponíveis no aplicativo IDD para exibição e edição, que tipo de componente de interface do usuário deve ser usado e, se for uma pesquisa, se os dados da pesquisa estão localizados. Nota: Essa configuração não é aplicada aos filtros de registros filho. Todas as colunas estão disponíveis para filtros.
Mascaramento de dados	Configura o mascaramento de dados baseado em função para colunas que estão selecionadas na guia Layout.
Limpar	Configura funções de limpeza a serem usadas para limpeza e validação.

TÓPICOS RELACIONADOS:

- [“Localização de Pesquisas” na página 49](#)
- [“Etapa 4. Configurar a Limpeza e a Validação” na página 33](#)

Localização de Pesquisas

Um aplicativo do Informatica Data Director preenche uma lista de valores aceitáveis para colunas que você configura no Gerenciador de Esquema como pesquisas. Uma tabela de localização é necessária para a criação de pesquisas localizadas. Ao criar uma pesquisa, use um nome de exibição exclusivo. O Informatica Data Director não consegue distinguir pesquisas com códigos diferentes que compartilham o mesmo nome de exibição.

O Informatica Data Director também oferece suporte à localização dos valores de exibição de pesquisas. É possível configurar valores de exibição de pesquisas na guia Layout do Gerenciador de Configuração do Informatica Data Director para áreas de assunto e filhos de áreas de assunto.

Por exemplo, um Armazenamento de Referências Operacionais tem as seguintes tabelas:

- C_PARTY
- C_LU_SALUTATION
- C_LCL_SALUTATION

A tabela C_PARTY tem o código de pesquisa de saudação configurado na tabela C_LU_SALUTATION. Para cada código de saudação, o nome de exibição pode ter um valor localizado configurado na tabela C_LCL_SALUTATION.

Para gerar a lista de valores referentes à localidade de um determinado usuário, o Informatica Data Director primeiro procura um nome da pesquisa em C_LCL_SALUTATION com base nessa localidade. Se o Informatica Data Director não encontrar um nome de pesquisa em C_LCL_SALUTATION, ele usará o nome de pesquisa da tabela de pesquisas SALUTATION_DISP.

Nota: O código de idioma e o código de país determinam a localidade. Os valores para o código de idioma e o código de país são códigos ISO de duas letras.

A configuração do cenário anterior especifica que a coluna tem valores de pesquisa localizados e identifica quais tabelas e colunas são usadas. O seguinte XML de amostra exibe a configuração do exemplo anterior:

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

TÓPICOS RELACIONADOS:

- [“Tabelas de Pesquisa” na página 24](#)
- [“Códigos de Localidade” na página 159](#)
- [“Configuração Manual do IDD” na página 58](#)

Importar um modelo de importação de dados

Um desenvolvedor de aplicativos do Informatica Data Director (IDD) pode configurar um aplicativo IDD para permitir que usuários autorizados importem dados de um arquivo de origem. O administrador de dados cria um modelo de importação de dados, que você importa para a configuração do aplicativo IDD.

Nota: A importação de dados está disponível para aplicativos IDD que implementam o modelo de dados de área de assunto e as exibições legadas do IDD.

Para obter mais informações sobre como importar dados, consulte o *Guia do Usuário do Multidomain MDM Data Director*.

Importando o Modelo de Importação de Dados

No Gerenciador de Configuração IDD, um administrador do MDM importa o modelo de importação de dados para o aplicativo Data Director (IDD). O processo de importação valida o modelo.

1. Faça logon no Gerenciador de Configuração IDD.
2. Selecione o aplicativo.
3. Clique em **Importar** > **Importar para aplicativo do IDD existente**.
A janela **Importar para aplicativo do IDD existente** é exibida.
4. Na lista **Tipo de configuração**, selecione **Modelo de Importação de Dados**.
5. Clique em **Procurar** e selecione o arquivo XML que contém o modelo de importação de dados.
6. Clique em **Importar**.
O processo de importação valida o modelo. A janela **Resultados da Validação** é aberta, exibindo os erros, se houver.
7. Se houver erros de validação, resolva-os no modelo e depois volte a importar o modelo.
8. Na janela **Resultado da Validação**, clique em **OK**.

Pacote de provedor de logon personalizado

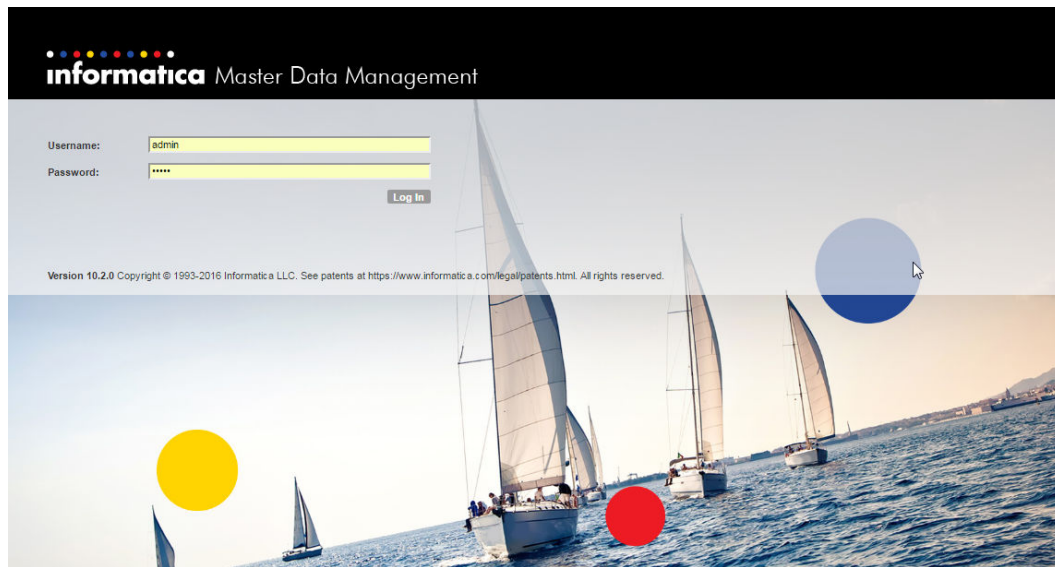
O pacote de provedor de logon personalizado é um arquivamento que contém classes Java. Você pode usar o Gerenciador de Configuração do Informatica Data Director para carregar esse arquivamento. O pacote de provedor de logon personalizado deve estar em um arquivo ZIP.

Na estrutura do Entity 360, o pacote de Provedor de Logon Personalizado deve estar em um arquivo ZIP que contém o seguinte:

- Pasta META-INF. Essa pasta contém um arquivo MANIFEST.MF que tem uma entrada Login-Provider-Class-Name contendo um nome de uma classe que implementa a interface LoginProvider.
- Arquivo JAR com a implementação de Provedor de Logon Personalizado.
- Outros arquivos JAR que contém dependências para a implementação do Provedor de Logon Personalizado, incluindo classes de utilitários, registro em log e bibliotecas de terceiros.

Você pode configurar o pacote de provedor de logon personalizado para usar o formulário de logon do Informatica Data Director ou o formulário de logon de um provedor de identidade externa, como o Google ou o Salesforce.

A imagem a seguir mostra o formulário de login do Informatica Data Director:



Se você não carregar um pacote de provedor de login personalizado, a implementação do Informatica Data Director padrão autenticará os usuários com as credenciais armazenadas no banco de dados principais do MDM Hub.

Pacotes de provedores de login personalizados no Kit de Recursos

O Kit de Recursos contém pacotes de provedores de login de amostra que você pode usar com o aplicativo Informatica Data Director. Esses pacotes de login único são armazenados tanto como arquivos JAR quanto como arquivos ZIP. Administradores de banco de dados e outros membros técnicos de uma equipe de implementação do MDM podem usar esses arquivos para criarem seus próprios pacotes de provedor de login personalizados.

Os arquivos de pacote de login único de amostra estão no seguinte diretório:

`<diretório de instalação infamdm>/hub/resourcekit/samples/sso`

Carregando o pacote de provedor de login personalizado

Para carregar o pacote de provedor de login personalizado, use o Gerenciador de Configuração do Informatica Data Director.

1. No painel de navegação do Gerenciador de Configuração do Informatica Data Director, clique em **Configurações do Provedor de Logon**.
2. No painel **Configurações do Provedor de Logon**, clique em **Editar**.
3. Na caixa de diálogo **Editar Configurações do Provedor de Logon**, clique em **Procurar**.
4. Selecione o arquivo morto do provedor de login personalizado e clique em **OK**.
5. Insira o nome do arquivo ZIP com a implementação da classe do Provedor de Logon no campo **Arquivamento de Implementação do Provedor de Logon**.
Você deve aguardar a conclusão do carregamento do arquivo ZIP no servidor.
6. Insira o nome da classe que implementa `com.siperian.bdd.security.LoginProvider` no campo **Nome da Classe do Provedor de Logon**.
Esse é o nome totalmente qualificado da classe que implementa `LoginProvider`.

7. Clique em **OK**.

O IDD valida o arquivo ZIP carregado e cria uma instância da classe de Provedor de Logon especificada.

Bibliotecas de terceiros

No IDD, você pode usar um provedor de logon personalizado com bibliotecas de terceiros. Porém, na estrutura do Entity 360, todas as bibliotecas de terceiros devem estar empacotadas no mesmo arquivo ZIP do pacote de provedor de logon personalizado.

Implementar o Provedor de Logon Personalizado

O Provedor de Logon Personalizado é uma classe Java que implementa a interface `LoginProvider` (`com.siperian.bdd.security.LoginProvider`) definida no IDD. Ele oferece suporte para o mecanismo de autenticação de Logon Único (SSO).

O Provedor de Logon do funciona em conjunto com Módulo de Logon do Hub. Todos os dados necessários no Módulo de Logon do Hub para a verificação do usuário autenticado devem ser transmitidos do Provedor de Logon como um campo de matriz de bytes `securityPayload` da classe `com.siperian.bdd.security.LoginCredentials`. Esse campo é transmitido do Provedor de Logon para o Módulo de Logon do Hub no estado em que se encontra e contém informações codificadas específicas da implementação sobre os usuários.

Provedor de Logon Personalizado com Formulário de Logon Externo

Se um determinado mecanismo de autenticação exigir uma página de logon que não seja do IDD, a implementação do Provedor de Logon Personalizado deverá usar os métodos de interface listados e descritos na seguinte tabela:

Nome do método de interface	Descrição
<code>initialize</code>	O IDD chama esse método antes de qualquer outro método da implementação do Provedor de Logon e transmite um conjunto de propriedades que descrevem o contexto de execução. No IDD, essas propriedades contêm uma entrada, que pode ser referenciada como <code>LoginProvider</code> . A propriedade <code>SSO_POST_REDIRECT_PAGE_PROPERTY</code> contém a URL da página jsf que pode publicar (POST) dados no provedor de logon externo. Uma implementação do Provedor de Logon pode usar essa página para redirecionar o IDD à Página de Logon Externa usando o método POST.
<code>isUseIDDLoginForm</code>	Esse método deve retornar <code>FALSE</code> .
<code>redirectToProviderLoginPage</code>	Esse método deve formar a URL para o formulário de logon externo e chamar o redirecionamento para essa página. Também é possível redirecionar a página de logon externo usando o método POST.
<code>extractLoginCredentials</code>	O IDD invoca esse método quando uma nova solicitação de autenticação de usuário é recebida. Se a solicitação contiver informações do provedor de identidade externo, como parâmetros de solicitação e cookies, esse método deverá extraí-los e retornar a instância <code>LoginCredentials</code> (<code>com.siperian.bdd.security.LoginCredentials</code>) com campos corretamente preenchidos. Se a solicitação não contiver informações de autenticação, o método deverá retornar <code>NULL</code> .

Nome do método de interface	Descrição
encodeComponentUrl	Esse método não é implementado, pois o nome de usuário e a senha são solicitados por um formulário de login externo que o IDD não reconhece.
onLogout	Esse método é chamado quando um usuário faz logout. Ele pode executar um logout no provedor de identidade externo e em parâmetros de limpeza definidos pelo método requestLoginCredentials.
getLogImageBody	Esse método deve retornar NULL.

Após o login bem-sucedido, você será direcionado à página principal do IDD ou à página de componentes do IDC (Informatica Data Controls), dependendo da sua solicitação inicial.

Além disso, você pode ignorar a autenticação externa usando o parâmetro `internal_login_form=true` na URL do IDD que exibe o login no IDD.

Por exemplo,

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

Nesse caso, o nome de usuário e a senha são verificados na lista de usuários do MDM Hub.

Transmitir Credenciais ao Link Externo

Se você precisar incorporar links externos ao IDD e esses links usarem o mesmo provedor de SSO (por exemplo, Salesforce.com) que o Provedor de Login Personalizado instalado, use esse método para adicionar informações de autenticação à URL do link. Se nenhuma informação for adicionada, o método deverá retornar um valor nulo ou a mesma string de URL transmitida para ele como um parâmetro.

Exemplo:

Suponha que você implemente LoginProvider para trabalhar com Salesforce.com.

Você também define o link externo com a URL `https://na7.salesforce.com/home/home.jsp` para ver a página inicial da conta do Salesforce.com incorporada na tela do IDD.

O método `encodeComponentUrl` recebe essa URL e a converte no seguinte:

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

Após essa transformação, o `Iframe` na página do IDD exibe a página inicial solicitada, sem redirecionamento para o formulário de login do Salesforce.

Usando uma página POST

O IDD usa a página POST para redirecionar usuários para uma página de login externa. Essa página é enviada depois de ser carregada no cliente.

A origem da página usa a variável JSF predefinida `requestScope` para acessar os parâmetros descritos na seguinte tabela:

Nome do Parâmetro	Uso
<code>providerGateURL</code>	Deve ser um valor de cadeia. Ele define a URL na qual o formulário será enviado (ação de formulário).
<code>authParameters</code>	Um mapa de pares de chave/valor. Cada par de valores é usado para criar uma entrada oculta. A chave de entrada de mapa é usada como o nome da entrada, e o valor é usado como o valor do campo de entrada.

No seguinte exemplo, a variável `postRedirectPageUrl` é configurada durante uma chamada para o método `initialize`:

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

Para enviar um redirecionamento para a nova página no logout, você pode adicionar o seguinte código ao método `redirectToProviderLoginPage()`:

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

O método `onLogout()` grava o código na resposta, conforme mostrado no exemplo a seguir:

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

Configurando o E360 para enviar solicitações POST ao serviço da Web

Às vezes, um provedor de logon personalizado usa serviços da Web que esperam uma solicitação POST. O Entity 360 inclui um servlet que envia solicitações POST. Para configurar o servlet de forma a enviar uma solicitação POST para um serviço da Web de terceiros, insira a URL de onde enviar essa solicitação no método `redirectToProviderLoginPage`.

1. Use um editor de texto para modificar a implementação do Provedor de Logon Personalizado.
2. Nas propriedades transmitidas ao método `initialize` do Provedor de Logon Personalizado, copie a URL do servlet.
3. No método `redirectToProviderLoginPage`, crie uma solicitação
 - a. No atributo `AuthParameters`, defina os parâmetros com pares de nome/valor.
Os pares de nome/valor compreendem o corpo da solicitação POST.
 - b. No atributo `ProviderGateURL`, insira a URL de onde a solicitação POST é enviada.
Nota: Certifique-se de que a URL termine com "/" (barra). Caso contrário, o aplicativo E360 gerará uma exceção de ponteiro nulo.

O código a seguir mostra uma solicitação de amostra em uma implementação de Provedor de Logon Personalizado:

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

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

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

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

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

Provedor de Logon Personalizado com Formulário de Logon do IDD

Se o mecanismo de autenticação usar o formulário de Logon do IDD para solicitar o nome de usuário e a senha, a implementação do Provedor de Logon Personalizado deverá usar os métodos de interface listados e descritos na seguinte tabela:

Nome do Método de Interface	Descrição
initialize	O IDD chama esse método antes de qualquer outro método da implementação do Provedor de Logon e transmite um conjunto de propriedades que descrevem o contexto de execução. No IDD, as propriedades contêm a única entrada. Ele pode ser referenciado como LoginProvider. SSO_POST_REDIRECT_PAGE_PROPERTY contém a URL da página JSF que pode publicar (POST) dados no provedor de logon externo.
isUseIDDLoginForm	Esse método deve retornar TRUE.
redirectToProviderLoginPage	Esse método não é usado.
extractLoginCredentials	Esse método extrai as credenciais de usuário de uma solicitação HTTP. Se a solicitação contiver informações de autenticação, esse método deverá retornar uma instância LoginCredentials (com.siperian.bdd.security.LoginCredentials) com campos corretamente preenchidos. Se a solicitação não contiver informações de autenticação, o método deverá retornar NULL.
requestLoginCredentials	Esse método é chamado depois que um usuário envia o formulário de logon preenchido. Esse método é usado para enviar solicitações a um provedor de identidade externo para autenticar usuários. Instâncias devidamente preenchidas de LoginCredentials são retornadas após a autenticação bem-sucedida. Se a autenticação falhar, uma exceção com.siperian.bdd.security.LoginProviderException será lançada.
encodeComponentUrl	Esse método recebe a URL ExternalLink e pode adicionar parâmetros de autenticação.

Nome do Método de Interface	Descrição
onLogout	Esse método é chamado quando um usuário faz logout. Ele pode executar o logout no provedor de identidade externo e em parâmetros de limpeza definidos pelo método <code>requestLoginCredentials</code> .
getLogolmageBody	Esse método retorna <code>InputStream</code> com o corpo do arquivo de imagem. Você pode usá-lo para exibir o logotipo de um provedor de identidade externo no formulário de logon do IDD. O formato da imagem deve ser PNG, JPEG ou GIF. A imagem não deve exceder uma largura de 155 pixels e uma altura de 29 pixels. Se esse método retornar <code>NULL</code> , o IDD usará a imagem predefinida para indicar que o formulário de logon é manipulado pelo Provedor de Logon Personalizado.

Criar a Biblioteca do Provedores de Logon

A classe `LoginProvider` e todas as classes do IDD que são necessárias para a compilação da implementação do Provedor de Logon Personalizado estão compactadas no arquivo `siperian-bdd.jar`. Esse arquivo está incluído no Kit de Recursos do MDM, que também contém a implementação de amostra de `LoginProvider`. Para obter mais informações, consulte *Guia do Kit de Recursos do Multidomain MDM*.

Configurar a Autenticação SSO do Salesforce (WebLogic)

Se você precisar configurar a autenticação SSO do Salesforce para o IDD, a verificação do nome do host deverá estar desativada no WebLogic. É possível desativar a verificação do nome do host usando o seguinte procedimento:

1. Abra o Console de Administração do Servidor WebLogic e faça login.
2. Expanda **Ambiente** e selecione **Servidores**.
3. Clique no nome do servidor que executa o Hub (o padrão é `AdminServer`).
4. Na página Configurações, clique na guia **SSL**.
5. Clique em **Avançado**, na parte inferior da página.
6. Defina o campo Verificação de Nome do Host como **Nenhum**.
7. Clique em **Salvar**.
8. Reinicie o Servidor WebLogic.

Configurar a Autenticação SSO do Salesforce (WebSphere)

Se você precisar configurar a autenticação SSO do Salesforce para o IDD, o WebSphere deverá ser configurado para confiar no servidor Salesforce. É necessário recuperar os certificados do signatário do host do Salesforce ao qual você está tentando se conectar e adicioná-los ao armazenamento de confiança do WebSphere usando o seguinte procedimento:

1. Abra o Console de Administração do WebSphere e faça login.
2. Expanda **Segurança** e clique em **Gerenciamento de certificados SSL e chaves > Gerenciar configurações de segurança de ponto de extremidade**.
3. Expanda **Saída** e clique em **HTTP**.
4. Escolha **Armazenamentos de chaves SSL** na lista suspensa.
5. Clique em **NodeDefaultTrustStore > Certificados do signatário**.

6. Clique em **Recuperar da porta**.
7. Insira os seguintes valores nos campos **Host**, **Porta** e **Alias**:
 - Host: `www.salesforce.com`
 - Porta: 443
 - Alias: `www.salesforce.com`
8. Clique em **Recuperar informações sobre o signatário**.

Os dados do certificado são exibidos.
9. Clique em **Aplicar**.
10. Repita as etapas de 6 a 9 para os seguintes hosts:
 - `na10-api.salesforce.com`
 - `c.na10.visual.force.com`
11. Clique em **Salvar**.
12. Reinicie o servidor WebSphere.

CAPÍTULO 5

Configuração Manual do IDD

Este capítulo inclui os seguintes tópicos:

- [Visão Geral da Configuração Manual do IDD, 58](#)
- [Ferramentas de XML, 59](#)
- [Trabalhar com o Arquivo XML de Configuração do IDD, 59](#)
- [Área de Assunto, 61](#)
- [Configuração do Gerenciador de Hierarquia, 68](#)
- [Extensões da Interface do Usuário, 73](#)
- [Saídas de Usuário, 82](#)
- [Localização, 89](#)
- [Páginas de Erro Personalizadas, 91](#)
- [Ajuda Online, 91](#)

Visão Geral da Configuração Manual do IDD

O arquivo de configuração do IDD (IDDConfig.xml) é um documento XML que pode ser modificado no Gerenciador de Configuração IDD ou exportado e editado manualmente.

Para editar a configuração de um aplicativo existente:

1. Exporte o aplicativo do IDD para um arquivo ZIP.
2. Extraia o arquivo ZIP do aplicativo.
3. Edite o arquivo de configuração do IDD (IDDConfig.xml).
4. Importe o arquivo de configuração editado diretamente para substituir aquele que se encontra no banco de dados (Importar Somente a Configuração do IDD). Como alternativa, o aplicativo do IDD pode ser novamente compactado, e o aplicativo completo pode ser importado para substituir todos os arquivos correspondentes (Importar Aplicativo Completo do IDD).

Ferramentas de XML

O Kit de Recursos do Informatica MDM Hub inclui um esquema XML (arquivo XSD) para o arquivo de configuração do IDD.

Isso é muito útil ao se trabalhar com editores de XML. Ele pode orientar você pelo processo de edição do arquivo e, o mais importante, é usado pelo editor para verificar a adequação do XML em um arquivo de configuração do IDD. O arquivo de configuração do IDD deve passar nesse teste antes de ser importado para o Gerenciador de Configuração IDD.

Embora um editor de texto simples possa ser usado para modificar a configuração do IDD, existem várias ferramentas de edição de XML que facilitam muito mais o trabalho com XML, entre elas:

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

O amostra do IDD no Kit de Recursos contém os seguintes componentes que podem ajudar com a configuração manual.

Item do Kit de Recursos	Descrição
siperian-bdd-config-6.xsd	Esquema XML do arquivo de configuração do IDD. Esse arquivo está localizado em <Pasta de instalação>\hub\resourcekit\sdk\bddXsdDoc\siperian-bdd-config-6.xsd
Documentação HTML do esquema XML	Documentação ao estilo Javadoc. Fornece as mesmas informações encontradas no esquema XML, mas em um formato mais fácil de navegar. Nota: Consulte essa documentação para obter as informações mais detalhadas sobre os elementos e atributos XML no arquivo de configuração do IDD.
Configuração do IDD de amostra	Para ser usada com o esquema de amostra.
Saídas de usuário do IDD de amostra	Um exemplo de como para criar um código Java personalizado para integração com o IDD.
Javadocs da biblioteca do IDD	Javadocs para as interfaces em Siperian-bdd.jar. Usados para implementar saídas de usuário do IDD em Java.

Trabalhar com o Arquivo XML de Configuração do IDD

Um arquivo XML de configuração do IDD pode chegar facilmente a centenas de linhas.

Um arquivo completo não é mostrado aqui, somente o trecho relevante. Você pode encontrar um arquivo de configuração completo no Kit de Recursos ou exportando-o do Gerenciador de Configuração IDD.

O seguinte trecho de código é um exemplo de um grupo de área de assunto com uma única área de assunto:

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

```

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

```

Consulte a documentação HTML do esquema XML para obter detalhes sobre os elementos, os atributos e os valores permitidos.

Área de Assunto

Os itens descritos nesta seção podem exigir modificação manual diretamente no arquivo IDDConfig.xml.

Coluna de Pesquisa

Um aplicativo do IDD preenche automaticamente uma lista suspensa de valores aceitáveis para colunas que estão configuradas no Gerenciador de Esquemas como pesquisas.

Isso é manipulado no Gerenciador de Configuração IDD para colunas que possuem uma chave externa para a tabela de pesquisa. Se a chave externa não existir (por exemplo, por motivos de desempenho), as informações sobre a tabela de pesquisa poderão ser especificadas na configuração do XML.

Uma pesquisa explícita é definida com o uso do elemento `columnLookup`, como mostra o exemplo a seguir.

```

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

```

Neste exemplo, a coluna `C_PARTY|GENDER_CD` deve ser tratada como se tivesse uma chave externa para a coluna `C_LU_GENDER|GENDER_CODE`, enquanto a tabela `C_LU_GENDER` é tratada como uma tabela de pesquisa. O aplicativo do IDD cria uma lista suspensa para a coluna `GENDER_CD`, e essa lista é preenchida com valores da tabela `C_LU_GENDER` (os valores de exibição são recuperados da coluna `GENDER_DISP`).

O elemento `columnI18NLookup` poderá ser especificado junto com o subelemento `columnLookup` se a localização dos valores de exibição for necessária.

```

<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
    <columnLookup lookupFKUid="C_LU_GENDER|GENDER_CODE"
        lookupNameUid="C_LU_GENDER|GENDER_DISP"/>
    <columnI18NLookup languageCdUid="C_LU_GENDER_LCL|LANGUAGE_CODE"
        countryCdUid="C_LU_GENDER_LCL|COUNTRY_CODE"
        lookupFKUid="C_LU_GENDER_LCL|GENDER_CODE"

```

```

        localizedNameUid="C_LU_GENDER_LCL|LOCALIZED_STRING"/>
    </column>

```

TÓPICOS RELACIONADOS:

- [“Tabelas de Pesquisa” na página 24](#)

Tabelas de Pesquisa com Coluna de Subtipo

Uma única tabela de pesquisa pode ser usada para armazenar valores de pesquisa para vários tipos de código diferentes.

Nesse caso, a tabela de pesquisa tem uma coluna de subtipo que identifica o tipo de código.

O uso de uma tabela de pesquisa com vários tipos de pesquisa é configurado conforme mostrado no exemplo a seguir.

```

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

```

Neste exemplo, a coluna C_AUTOMOBILE|DOORS_CODE é uma coluna de pesquisa. Somente os valores na tabela de pesquisa com ATTR_TYPE="Doors" são usados para essa pesquisa.

A localização da pesquisa também pode ser combinada com subtipos de pesquisa, conforme mostrado no exemplo a seguir.

```

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

```

TÓPICOS RELACIONADOS:

- [“Códigos de Idioma” na página 159](#)

Valores de Pesquisa Estáticos

Os valores de uma coluna de pesquisa também podem ser definidos diretamente no arquivo de configuração do IDD - nenhuma tabela de pesquisa é usada.

O elemento `columnStaticLookups` é usado para definir isso, conforme mostrado no exemplo a seguir.

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

Esse exemplo especifica que somente os valores 'M' e 'F' podem ser armazenados na coluna C_PARTY|GENDER_CD. Para essa coluna, o aplicativo do IDD cria uma lista suspensa preenchida com os valores 'MALE' e 'FEMALE'.

Valores de pesquisa estáticos também podem ser localizados, conforme mostrado no exemplo a seguir.

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

Exibir os Campos Secundários de um Objeto Base na Guia Filho

Para exibir os campos secundários de um Objeto Base (OB) na guia filho do IDD, use o tipo filho **Parte do Objeto Primário** ao criar a área de assunto filho (AS) no Gerenciador de Configuração IDD.

Você deve configurar o arquivo de configuração do IDD (`IDDConfig.xml`) para exibir os campos secundários de um OB na guia filho.

Para o exemplo a seguir, no Console do Hub, você deve criar um OB C_EMPLOYEE com quatro colunas: EMP_ID, EMP_NAME, STATE e COUNTRY, bem como a AS pai Employee e a AS filho EmpDetails.

O trecho de código a seguir mostra EMP_NAME (que é um campo secundário) na guia filho EmpDetails.

```
primaryObjectUid="C_EMPLOYEE" searchOnly="false">
<subjectArea displayName="Employee" name="Employee" showXREF="false">
  <primaryObject>
    <layout columnsNum="3">
      <column columnUid="C_EMPLOYEE|EMP_ID"
        editStyle="FIELD" editable="true"
        hidden="false" horizontalStyle="MEDIUM"
        lineBreak="false"
        ns1:showInHMCompactView="false"
        required="false" xmlns:ns1="urn:siperian.dsapp.config"/>
      <column columnUid="C_EMPLOYEE|STATE"
        editStyle="FIELD" editable="true"
        hidden="false" horizontalStyle="MEDIUM"
        lineBreak="false"
        ns2:showInHMCompactView="false"
        required="false" xmlns:ns2="urn:siperian.dsapp.config"/>
      <column columnUid="C_EMPLOYEE|COUNTRY"
        editStyle="FIELD" editable="true"
        hidden="false" horizontalStyle="MEDIUM"
        lineBreak="false"
        ns3:showInHMCompactView="false"
```

```

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

```

Exibindo um Pai de um Objeto Primário em uma Guia Filho

Quando um objeto primário tem um pai, é possível exibir os atributos do objeto base pai em uma guia filho. Para configurar a exibição, você deve editar o arquivo XML de configuração do IDD. É possível configurar várias guias filho, uma para cada objeto base pai que você deseja exibir.

No MDM Hub, o relacionamento entre os objetos base deve ser do tipo 1:1 ou 1:muitos. Por exemplo, você cria os objetos base C_ADDRESS e C_PARTY e depois cria um relacionamento entre eles.

1. No Gerenciador de Configuração do IDD, crie uma área de assunto para o objeto primário. Por exemplo, crie um área de assunto para C_ADDRESS.
2. Salve a configuração.
3. Abra o arquivo XML de configuração do IDD.
4. Após o elemento `primaryObject`, adicione o elemento `poParent` e defina os campos que você deseja exibir.

Por exemplo, a seguinte amostra de código indica como configurar o elemento `poParent` para mostrar três campos de C_PARTY na guia filho.

```

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

```

5. Salve o arquivo.

Expandir uma Área de Assunto Filho na Exibição de Dados por Padrão

É possível configurar uma área de assunto filho para que ela seja expandida por padrão quando você abrir um registro em uma exibição de dados.

Defina o atributo `expanded` como `true` em `BDDConfig.xml` para a área de assunto filho. Quando você abrir o registro primário, a área de assunto filho aparecerá expandida. As outras áreas de assunto filho aparecem reduzidas.

O seguinte exemplo de código define a área de assunto `C_PARTY_NAME` de forma que ela seja expandida por padrão quando você abrir o registro primário na exibição de dados:

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

Criar Referência Irmã

Você pode criar uma referência irmã para criar um relacionamento de um registro em uma área de assunto com um registro filho dentro dessa área de assunto. Por exemplo, um cliente pode incluir os registros filho de endereço e de número de telefone, com o número de telefone possuindo uma chave externa a ser associada a um endereço específico.

Você deve configurar o arquivo de configuração do IDD (`IDDConfig.xml`) para criar a referência irmã.

O trecho de código a seguir cria uma referência irmã para o campo `ADDRESS_ID` da coluna na área de assunto filho `PERSON DETAILS`.

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

Nota: Você deve especificar o atributo `ChildName` na marca `siblingReference` com o nome de referência da área de assunto filho disponível.

Netos

Quando netos são mostrados em uma exibição de tabela, todos os registros neto são exibidos, e não apenas aqueles que estão relacionados ao registro filho selecionado. O IDD tem uma opção de configuração que ajuda os usuários a compreender o relacionamento desses netos com o filho.

É possível definir um `parentReference` para a coluna que é a chave externa para o registro filho. Isso define um rótulo a ser exibido no registro neto que contém dados do filho.

No exemplo a seguir, a coluna de chave externa do neto para o filho está configurada como uma referência pai. Isso configura um elemento label com o conjunto de colunas a ser usado para rótulos e o existsFormat. Neste exemplo, o rótulo do registro filho será "<Phone Number>, (<Extension Number>".

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

Links de Área de Assunto

Uma área de assunto pode conter filhos de referência de muito-para-muitos.

Esses filhos mostram uma área de assunto como um filho de outra área de assunto. A área de assunto filho não pode ser editada diretamente. Para editá-la, o usuário de aplicativo do IDD deve navegar até uma exibição de dados separada para essa área. O elemento `subjectAreaLinkColumn` é usado para definir uma coluna a ser usada como um link de acesso.

Os dados na coluna identificada como o link da área de assunto são sublinhados. Quando o usuário de aplicativo do IDD clica nessa coluna, a área de assunto associada é aberta em uma nova guia.

Independentemente de uma coluna de link de área de assunto estar ou não configurada, o usuário de aplicativo do IDD pode clicar com o botão direito do mouse no registro e selecionar "Abrir em uma Nova Guia" para abrir a área de assunto.

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

Agrupamento Lógico de Menus

Se você tiver vários grupos de áreas de assunto, poderá organizá-los ou combiná-los para criar uma estrutura lógica de menus de nível superior no aplicativo do IDD.

Você deve editar o arquivo de configuração do IDD (`IDDConfig.xml`) para criar grupos lógicos de grupos de áreas de assunto.

O trecho de código a seguir cria um agrupamento lógico de grupos de áreas de assunto.

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

Adicionando grupos na janela Novo

Se você tiver muitas áreas de assunto, defina os grupos a serem usados na janela **Novo** do IDD. Defina a propriedade global `enableCreateBeMenuGrouping=true` e defina os grupos no arquivo `IDDConfig.xml`.

1. Defina a propriedade `enableCreateBeMenuGrouping` usando o seguinte comando:

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

2. No Configuration Manager do IDD, exporte o arquivo `IDDConfig.xml` e adicione os grupos ao arquivo, conforme mostrado no exemplo a seguir:

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

3. Reinicie o servidor de aplicativos.
4. Implante o arquivo `IDDConfig.xml` modificado.
5. Faça login no aplicativo do IDD e verifique se a janela **Novo** contém os grupos.

Personalizando Rótulos de Coluna

É possível personalizar rótulos de coluna no IDD no nível da área de assunto para diferenciar rótulos de coluna idênticos que são usados em várias áreas de assunto ou para modificar qualquer rótulo de coluna. Você deve editar o arquivo `MetadataBundle.properties` para personalizar o rótulo de coluna da área de assunto. Por exemplo, considere um objeto base, `Party`, com as áreas de assunto, `Person` e `Organization`. Se você tiver o rótulo de coluna `Tax ID` em ambas as áreas de assunto, poderá personalizá-lo para diferenciar entre as áreas de assunto.

Para personalizar rótulos de coluna de uma área de assunto, realize as etapas a seguir:

1. Se você tiver alterado os metadados no Armazenamento de Referências Operacionais, clique em **Limpar Cache**.
2. Exporte o aplicativo IDD para um arquivo ZIP.
3. Extraia o arquivo ZIP do aplicativo.
4. Edite o arquivo `MetadataBundle.properties`.
Por exemplo: Para modificar o rótulo de coluna `Tax ID` para `Customer Tax ID`, em `MetadataBundle.properties`, edite `Test.Person.COLUMN.C_PARTY|TAX_ID=Customer Tax ID`.
5. No Gerenciador de Configuração IDD, selecione o aplicativo IDD para substituir o arquivo `MetadataBundle.properties` editado.
6. Clique no botão **Importar** e selecione **Importar para aplicativo IDD existente**.
7. Na janela **Importar para aplicativo IDD existente**, para **Tipo de configuração** selecione **Pacote de Metadados**.
8. Clique em **Procurar** para localizar e selecionar o arquivo `MetadataBundle.properties` apropriado.
9. Clique em **Importar**.

Faça logon no aplicativo IDD para exibir os rótulos de coluna personalizados.

Configurar o Estilo de Edição de Caixa de Seleção

O Mapeamento de Valores permite definir valores que devem ser armazenados no MDM Hub para colunas com o estilo de edição de caixas de seleção.

A tabela a seguir fornece informações sobre estilos de edição que você pode configurar para o tipo de dados com suporte.

Tipo de Dados	Estilo de Edição
DATE	Calendário e Calendário longo
INT e CHAR(1)	Campo, Área de texto e Caixa de seleção
Outros	Campo e Área de texto

Nota:

- Para uma coluna do tipo de dados CHAR(1), você pode definir três pares de valores a serem configurados para uma Caixa de Seleção: Valor 1/0, valor Y/N ou valor T/F. Com base no par de valores atribuído, o valor correspondente será salvo no objeto base.
- Para uma coluna do tipo de dados INT, é possível definir somente pares de valores 0 e 1.

Para configuração manual, você deve garantir que o elemento `column` com `editStyle="CHECKBOX"` não tenha mais de um elemento `valueMapping` aninhado. O elemento `valueMapping` para `editStyle="CHECKBOX"` deve ter dois elementos `mappingItem`. Além disso, `mappingItem` deve incluir os valores `selected` de `true` e `false`.

No exemplo a seguir, o atributo `domainValue` é responsável pelo valor que é armazenado no MDM Hub, enquanto o atributo `selected` é responsável pela apresentação do controle de caixa de seleção. Os valores `true` ou `false` são definidos para os estados Marcado e Desmarcado da caixa de seleção, respectivamente.

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

Configuração do Gerenciador de Hierarquia

As configurações descritas aqui se aplicam à Exibição de Hierarquia do IDD para todos os tipos de entidade do HM (Gerenciador de Hierarquia).

A listagem de XML a seguir tem exemplos de todos os itens descritos mais adiante nesta seção.

```
<hmConfiguration hmConfigurationUid="Default|Master" enableAddRel="false"
simpleNodeLimit="100">
<hmOneHopLimits totalRels="1000"/>
<hmManyHopLimits hops="20" relsPerEntity="50" totalRels="1000"/>
<hmRelationshipTypes>
<hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.employs">
<layout columnsNum="2">
<column columnUid="C_RL_PARTY|REL_NAME" editStyle="FIELD"
horizontalStyle="LARGE" required="true"/>
<column columnUid="C_RL_PARTY|REL_DESC" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
<column columnUid="C_RL_PARTY|NOTE" editStyle="FIELD"
```

```

        horizontalStyle="SMALL"/>
    </layout>
</hmRelationshipType>
<hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.contains member">
    <layout columnsNum="2">
        <column columnUid="C_RL_PARTY_GROUP|HUB_STATE_IND" editStyle="FIELD"
            horizontalStyle="MEDIUM"/>
    </layout>
</hmRelationshipType>
</hmRelationshipTypes>
<hmFilter name="filter1" displayName="Filter 1">
    <showActiveRelOnly>false</showActiveRelOnly>
    <hideUnconnectedEntities>false</hideUnconnectedEntities>
    <getParents>true</getParents>
    <getChildren>true</getChildren>
    <getUndirected>true</getUndirected>
    <getBidirectional>true</getBidirectional>
    <getUnknown>true</getUnknown>
</hmFilter>
<hmFilter name="filter2" displayName="Filter 2">
    <showActiveRelOnly>false</showActiveRelOnly>
    <hideUnconnectedEntities>false</hideUnconnectedEntities>
    <getParents>true</getParents>
    <getChildren>true</getChildren>
    <getUndirected>true</getUndirected>
    <getBidirectional>true</getBidirectional>
    <getUnknown>true</getUnknown>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.member of account group
    </enabledRelationshipsUids>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.employs</
enabledRelationshipsUids>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.contains member 2
    </enabledRelationshipsUids>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.customer
    </enabledRelationshipsUids>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.contains member
    </enabledRelationshipsUids>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.associate
    </enabledRelationshipsUids>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.organization has
    </enabledRelationshipsUids>
    <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.is DNB parent of
    </enabledRelationshipsUids>
    <enabledHierarchiesUids>HM_HIERARCHY.Product</enabledHierarchiesUids>
    <enabledHierarchiesUids>HM_HIERARCHY.Customer</enabledHierarchiesUids>
    <enabledHierarchiesUids>HM_HIERARCHY.DNB</enabledHierarchiesUids>
</hmFilter>
<externalLinkAction callback="false" displayName="Graph Google Search"
    name="hm_google_search_action">
    <externalLink name="hm_google_search_link" type="IFRAME"
        url="http://www.google.com/search">
        <param bddParamName="SELECTED_GRAPH_OBJECTS" name="q" />
        <param name="hl" staticValue="en" />
    </externalLink>
</externalLinkAction>
<externalLinkAction callback="true" displayName="Test graph callback"
    name="hm_test_callback_action">
    <externalLink name="hm_test_callback" type="IFRAME"
url="test_external_hm.html">
        <param bddParamName="USERNAME" name="username" />
        <param bddParamName="SELECTED_GRAPH_OBJECTS" name="selectedHmObjects" />
        <param bddParamName="ALL_GRAPH_OBJECTS" name="allHmObjects" />
    </externalLink>
</externalLinkAction>
</hmConfiguration>

```

Adicionar Relacionamentos

A Exibição de Hierarquia pode ser configurada para ser uma exibição somente leitura.

O usuário de aplicativo do IDD pode navegar pelos relacionamentos, mas estes últimos não podem ser adicionados ou editados. O atributo `enableAddRel` que controla isso usa o valor "true" como padrão. O exemplo acima mostra como desativar adições e edições de relacionamentos.

Otimização de Renderização

O IDD fornece uma visualização sofisticada para entidades e relacionamentos na Exibição de Hierarquia.

Como o tamanho de um gráfico nessa exibição cresce até centenas de itens, o tempo de renderização da exibição pode ser um problema. O IDD define um limite acima do qual os nós são renderizados de maneira simplificada, diminuindo assim o tempo de renderização. Esse limite é de 300 por padrão, mas pode ser manualmente configurado com o uso do atributo `simpleNodeLimit`.

Tipos de relacionamento do Gerenciador de Hierarquia

Use o elemento `hmRelationshipType` para configurar os tipos de relacionamentos. Você pode configurar layouts, funções de limpeza e saídas de usuários para relacionamentos que são adicionados ou editados na Exibição de Hierarquia.

A configuração é feita por tipo de relacionamento. Há colunas padrão para cada relacionamento que são automaticamente gerenciadas pelo Data Director: tipo de relacionamento e hierarquia, data de início e de término e referências a entidades relacionadas. O elemento `hmRelationshipTypes` especifica quaisquer atributos adicionais em um registro de relacionamento.

Nota: Um relacionamento do Gerenciador de Hierarquia que é definido como um relacionamento de chave estrangeira no Console do Hub não pode ter campos personalizados e definição de layout no Data Director. Essa restrição é baseada na natureza do relacionamento de chave estrangeira. Para obter mais informações, consulte a seção sobre como configurar relacionamentos de chave estrangeira entre objetos base no *Guia de Configuração do Multidomain MDM*.

Filtro do Gerenciador de Hierarquia

A Exibição de Hierarquia tem filtros que controlam quais tipos de relacionamento e de hierarquia, direções de relacionamento e outros itens são exibidos.

Use o elemento `hmFilter` para definir configurações de filtro que podem ser atribuídas como as configurações de filtro padrão para uma área de assunto. Essa configuração é usada desde que um usuário de aplicativo do IDD não tenha criado um Filtro Salvo e o transformado no padrão para essa área de assunto.

Por exemplo, o código a seguir define `filter2` como o filtro padrão para a área de assunto A1:

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

Ativando Relacionamentos Inativos

Para permitir que o usuário exiba relacionamentos inativos no Gerenciador de Hierarquia, defina `hmInactiveRelationshipsAvailable` como `true`.

Para adicionar esse parâmetro ao banco de dados Oracle e definir o parâmetro como "true", execute o seguinte script:

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

Registros de Tabela de Relacionamento de Exibição de Hierarquia

Defina a contagem máxima de registros para limitar o número de registros de relacionamento exibidos pela tabela de relacionamentos da Exibição de Hierarquia.

O arquivo `cmxserver.properties` contém o parâmetro `sif.api.hm.flyover.max.record.count`. O valor padrão é 10.000.

Quando você não especifica uma data efetiva na Exibição de Hierarquia, a tabela de relacionamentos mostra os registros de relacionamento efetivos e não efetivos. Muitos registros de relacionamento efetivos e não efetivos podem existir para uma entidade específica. Se o número total de registros de relacionamento exceder o limite de contagem máxima de registros, o Informatica Data Director exibirá os registros de relacionamento mais altos na ordem de classificação. O Informatica Data Director não exibirá os registros de relacionamento que excederem a contagem máxima de registros.

Quando você especifica a data efetiva na Exibição de Hierarquia, a tabela de relacionamentos mostra todos os relacionamentos efetivos para essa data efetiva, independentemente do limite de contagem máxima de registros.

Exibição de Hierarquia

Na Exibição de Hierarquia, um usuário pode usar o comando Exibir Detalhes de uma entidade selecionada para ativar uma caixa de diálogo que oferece uma exibição compacta da entidade e alguns de seus registros filho.

Esse atributo `compactViewChildrenNumber` controla quantos registros filho de cada tipo devem ser mostrados (o padrão é 5).

As colunas e tipos de filho que são mostrados nessa exibição são controlados pelo atributo `showInHMCompactView` em colunas e objetos filho. Para o objeto primário, `showInHMCompactView="true"` deve ser definido para qualquer colunas a ser exibida. Para objetos filho, `showInHMCompactView="true"` deve ser definido para todos os objetos a serem exibidos. Se esse atributo não estiver definido para quaisquer colunas do objeto primário ou filhos, somente o rótulo da área de assunto será exibido nessa caixa de diálogo.

```
<subjectArea name="Person">
  <primaryObject hmEntityTypeUid="Person">
    ...
    <layout columnsNum="3">
      <column columnUid="C_PARTY|NAME_PREFIX_CD" editStyle="FIELD"
        horizontalStyle="SMALL"/>
      <column columnUid="C_PARTY|FIRST_NAME" editStyle="FIELD"
        showInHMCompactView="true"
        horizontalStyle="MEDIUM" required="true"/>
      <column columnUid="C_PARTY|MIDDLE_NAME" editStyle="FIELD"
        showInHMCompactView="true"
        horizontalStyle="MEDIUM"/>
      <column columnUid="C_PARTY|LAST_NAME" editStyle="FIELD"
```

```

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

```

As configurações de objetos primários descritas aqui controlam o comportamento padrão ao abrir uma Exibição de Hierarquia com uma entidade desse tipo como âncora. Os seguintes atributos podem ser configurados.

Atributo	Descrição
hmManyHopLimits	Controla o gráfico que é buscado. O padrão é um salto.
hmFilterName	Filtro inicial a ser aplicado ao exibir o gráfico. O nome deve ser um dos filtros definidos no atributo hmFilters descrito acima.
hmDefaultLayout	Layout a ser usado para exibir o gráfico. Um dos valores a seguir: hierarchy, taxonomy, tree, network, circular, explorerView.

```

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

```

Personalizações

A Exibição de Hierarquia pode ser personalizada das seguintes maneiras:

- Saídas de usuário que são executadas ao adicionar ou modificar relacionamentos
- Saídas de usuário que podem ser chamadas no menu Ações
- Ações personalizadas que podem ser chamadas no menu Mais Ações e que podem transmitir o contexto do gráfico que está sendo exibido

Extensões da Interface do Usuário

Extensões de interface de usuário são usadas para adicionar funcionalidade personalizada a um aplicativo IDD.

Elemento	Descrição
uiExtensions	Pode ser adicionado à configuração para adicionar guias de nível superior e extensões do Iniciar espaço de trabalho.
externalLinkChild	Pode ser configurado para adicionar guias filho a uma área de assunto.
externalLinkAction	Pode ser configurado para adicionar ações a uma área de assunto, filho de área de assunto ou resultados de pesquisa.

Essas extensões são chamadas por meio de uma URL para a qual é possível transmitir parâmetros. Esses parâmetros podem incluir o nome de usuário e a senha do usuário conectado. Eles podem ser transmitidos em texto simples ou criptografado usando a criptografia simétrica Blowfish. Use `encryptionKey` como elemento opcional no elemento `bddApplication`.

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

Guias de Espaço de Trabalho de Nível Superior

Por padrão, o Informatica Data Director exibe três guias do espaço de trabalho de nível superior: Início, Dados e Tarefas.

Nota: Não é possível desativar as guias Início, Dados e Tarefas padrão.

Podem ser configuradas guias adicionais que contêm uma página solicitada de uma URL externa.

Guias de Nível Superior Personalizadas

Você pode adicionar guias de Nível Superior personalizadas ao Informatica Data Director.

Você pode adicionar uma guia para exibir um link externo em um iFrame. Você não pode usar sites como o Google e o Facebook com o iFrame devido à política de privacidade dos sites. Certifique-se de que o link externo seja para um site que seja compatível com o iFrames.

A seguinte amostra de código de exemplo adiciona uma página de pesquisa do Bing:

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

```

        </topLevelTab>
    ...
</uiExtensions>
...
</bddApplication>

```

Espaço de Trabalho Início

O Informatica Data Director Iniciar espaço de trabalho é formado por três tipos de componentes: lista de tarefas (Minhas Tarefas), relatórios e componentes personalizados.

A lista de tarefas está sempre disponível. Esta seção descreve a configuração de componentes personalizados usando o elemento `externalLink`.

Por padrão, esses componentes estão ordenados como: lista de tarefas, relatórios e componentes personalizados. Eles podem ser reorganizados usando o elemento `dashboardLayout` descrito nesta seção. Os usuários de aplicativos do Informatica Data Director podem personalizar ainda mais o conjunto de componentes que eles verão, bem como a ordem na qual esses componentes são exibidos. Essas informações são salvas como parte das preferências do usuário.

Links Externos (Componentes Personalizados do Espaço de Trabalho Início)

Componentes personalizados são definidos usando o elemento `externalLink`.

Um `externalLink` permite a exibição de páginas solicitadas de uma URL externa ou de código HTML e JavaScript personalizado.

O trecho de código a seguir é um exemplo de um componente do Iniciar espaço de trabalho personalizado. Dois parâmetros são transmitidos como parte da URL, como:

```

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

```

Parâmetros de Link Externo (Estáticos e Dinâmicos)

Qualquer número de parâmetros pode ser configurado para a URL especificada em `externalLink`. Parâmetros podem ser estáticos ou dinâmicos.

Parâmetro	Descrição
Estático	Tem valores predefinidos especificados no arquivo de configuração do IDD. O seguinte exemplo mostra uma definição de parâmetro estático que usa o atributo <code>staticValue</code> : <pre><param name="hl" staticValue="en"/></pre>
Dinâmico	Substituído durante o tempo de execução. A definição de um parâmetro dinâmico contém o atributo <code>bddParamName</code> e o valor desse atributo é substituído por dados disponíveis durante o tempo de execução. Há suporte para os seguintes parâmetros dinâmicos: <ul style="list-style-type: none">- Nome de logon do usuário do aplicativo do IDD conectado (<code>bddParamName="USERNAME"</code>)- Nome de logon criptografado do usuário do aplicativo do IDD conectado (<code>bddParamName="USERNAME_ENCRYPTED"</code>)- Senha do usuário do aplicativo do IDD conectado (<code>bddParamName="PASSWORD"</code>)- Senha criptografada do usuário do aplicativo do IDD conectado (<code>bddParamName="PASSWORD_ENCRYPTED"</code>)

Componentes de Link Externo (IFRAME and IGOOGLE)

Há suporte para dois tipos de componentes `externalLink`: IFRAME e IGOOGLE.

IFRAME

Componentes IFRAME (`type= " IFRAME "`) exibem uma página solicitada de uma URL externa. Você não pode usar sites como o Google e o Facebook com o iFrame devido à política de privacidade dos sites. Certifique-se de que o link externo seja para um site que seja compatível com o iFrames.

A URL é construída a partir do valor especificado usando o atributo `url` e os parâmetros de URL especificados.

O trecho de XML anterior define um componente IFRAME, exibindo uma página solicitada de uma URL gerada dinamicamente. Essa URL é construída com base na cadeia " `http://www.bing.com/search`", no parâmetro estático com o nome "hl" e o valor "en", e no parâmetro dinâmico com o nome "q" e o valor substituído durante o tempo de execução pelo nome do usuário do aplicativo do IDD conectado atualmente.

Por exemplo, se o usuário do aplicativo do IDD conectado tiver o nome de logon "admin", esse componente exibirá uma página solicitada da seguinte URL:

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

IGOOGLE

Componentes IGOOGLE (`type= " IGOOGLE "`) são usados para incorporar o JavaScript importado de uma URL externa (construída a partir do valor especificado usando o atributo `url` e os parâmetros de URL especificados) e um código HTML personalizado.

Um componente definido como ' `<externalLink name="component_name" type="IGOOGLE" url="external URL"/>`' adiciona um componente do Iniciar espaço de trabalho construído a partir de uma única tag HTML `<script>`:

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

Layout do Espaço de Trabalho Início

Componentes no Iniciar espaço de trabalho são dispostos em uma grade, de cima para baixo e da esquerda para a direita.

Por padrão, esses componentes estão ordenados como: lista de tarefas, relatórios e componentes personalizados.

É possível especificar a ordem padrão usando o elemento `dashboardLayout`. Os usuários de aplicativos do IDD podem personalizar ainda mais o conjunto de componentes que eles verão, bem como a ordem desses componentes. Isso é salvo como parte das preferências do usuário.

Conceitualmente, o layout do Iniciar espaço de trabalho é uma grade com n colunas. Cada elemento pode ocupar uma linha e uma ou mais células nessa linha. Nem todas as células de uma linha devem ser preenchidas com elementos - nesse caso, o restante da linha estará em branco.

O trecho de código a seguir mostra um exemplo de um layout do Iniciar espaço de trabalho de duas colunas.

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

Cada elemento no layout é representado com o elemento `dashboardLayoutItem`, que apresenta os seguintes atributos possíveis:

Parâmetro	Tipo	Descrição
nome	string	ID de elemento exclusivo dentro do elemento <code>dashboardLayout</code> .
type	TASKS, REPORT ou EXTERNAL_LINK	Tipo do elemento.
Colunas	número ou "*"	Número de colunas ocupadas pelo elemento. O valor padrão é "1". Há um símbolo especial "*" para elementos que ocupam a linha inteira.

A ordem dos elementos no Iniciar espaço de trabalho é a ordem na qual eles são especificados no elemento `dashboardLayout`.

Guias Filho Personalizadas

Guias Filho Personalizadas podem ser adicionadas a uma área de assunto.

Elas são mostradas no mesmo painel de guias que as guias filho Um-para-Muitos e Muitos-para-Muitos. Além disso, são configuradas com o uso do elemento `externalLinkChild`.

Guias Filho Personalizadas com o tipo `externalLinkChild` são configuradas para exibir o conteúdo de uma página HTML solicitada de uma URL externa. Veja a seguir um exemplo de definição de `externalLinkChild`:

```
<subjectArea name="Organization" displayName="Organization">
  <primaryObject hmEntityTypeUid="Organization">
    <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
    <layout columnsNum="3">
      <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
    </layout>
  </primaryObject>
  <externalLinkChild name="org_name_bing_search_child" displayName="Bing Search">
    <externalLink name="org_name_bing_search_action_link" type="IFRAME"
url="http://www.bing.com/search">
```

```

        <param name="q" bddParamName="C_PARTY|ORGANIZATION_NAME"/>
        <param name="hl" staticValue="en"/>
    </externalLink>
</externalLinkChild>
</subjectArea>

```

Atributos de Guias Filho Personalizadas

Guias Filho Personalizadas são definidas usando o elemento `externalLinkChild` em uma área de assunto.

Esse elemento tem os seguintes atributos:

Atributo	Descrição
nome	Nome utilizado internamente desta guia filho personalizada. Deve ser exclusivo em todas as guias filho personalizadas. Use somente caracteres alfanuméricos - caracteres especiais não são permitidos.
displayName	Título da guia filho. O valor especificado no XML de configuração é usado por padrão, mas pode ser substituído no pacote de recursos.

Propriedades de Links Externos

O elemento `externalLinkChild` deve conter o elemento `externalLink`, que define a URL exibida na guia filho.

Esse elemento tem os seguintes atributos:

Atributo	Descrição
nome	Nome utilizado internamente deste link. Deve ser exclusivo entre todos os links externos. Use somente caracteres alfanuméricos - caracteres especiais não são permitidos.
tipo	Links externos definidos para guias filho personalizadas devem ser do tipo "IFRAME".
url	URL exibido na guia filho personalizada.

Parâmetros

Parâmetros podem ser anexados à URL usando o elemento `param`. Parâmetros de URL podem ser estáticos ou dinâmicos.

Parâmetros Estáticos

Parâmetros estáticos têm valores predefinidos especificados na configuração.

Veja a seguir um exemplo de uma definição de parâmetro estático (que usa o atributo `staticValue`):

```

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

```

Parâmetros Dinâmicos

Valores de parâmetros dinâmicos são substituídos em tempo de execução.

A definição de um parâmetro dinâmico contém o atributo `bddParamName`, e o valor desse atributo é substituído pelos seguintes dados disponíveis em tempo de execução:

- Nome de logon do usuário do aplicativo IDD conectado (`bddParamName=" USERNAME"`)

- Nome de logon criptografado do usuário do aplicativo IDD conectado (bddParamName="USERNAME_ENCRYPTED")
- Nome de logon criptografado do usuário do aplicativo IDD conectado (bddParamName="USERNAME_ENCRYPTED")
- Senha criptografada do usuário do aplicativo IDD conectado (bddParamName="PASSWORD_ENCRYPTED")
- Coluna do sistema 'ROWID_OBJECT' de PrimaryObject (bddParamName=" <primaryObject TableUID>| ROWID_OBJECT") da área de assunto
- Para PrimaryObjects ativados para linha do tempo, o formato longo em milissegundos da data efetiva de PrimaryObject (bddParamName="EffectiveDate") da área de assunto
- Dados de colunas de PrimaryObject (bddParamName=" <columnUid da coluna de PrimaryObject>") da área de assunto
- Dados de colunas dos filhos Lógicos do tipo Um:Um da área de assunto (bddParamName=" <columnUid da coluna filho do tipo Um:Um d PrimaryObject>")
- Você pode especificar os parâmetros @LOCALHOST@ e @LOCALPORT@ no arquivo de configuração do Informatica Data Director. Quando uma URL externalLinkAction de retorno de chamada aponta para um aplicativo implantado no mesmo servidor que o MDM Hub, você deve especificar dinamicamente o nome do host local na URL. Especifique dinamicamente o nome do host local na URL de forma que a janela externalLinkAction possa interoperar com a janela de navegador do Informatica Data Director sem restrições de navegador entre sites. O seguinte código mostra como definir o elemento externalLinkAction com o parâmetro @LOCALHOST@ na URL:

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

Para transmitir nomes de usuários e senhas criptografados, você deve definir a chave de criptografia. Você deve definir a chave de criptografia no arquivo de configuração do IDD (IDDConfig.xml) usando o elemento encryptionKey.

O seguinte exemplo de código mostra como definir o elemento encryptionKey:

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

Por exemplo, no arquivo de configuração, você pode definir a chave de criptografia do IDD da seguinte maneira:

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

Ações Personalizadas

Uma *ação personalizada* é uma solicitação HTTP chamada em uma janela de navegador pop-up.

Ações personalizadas podem ser configuradas para as seguintes áreas de aplicativo do IDD:

- SubjectArea (a definição da ação é colocada dentro da definição SubjectArea). Essas ações personalizadas são adicionadas ao menu Mais Ações da área de assunto (esse menu está disponível na Exibição de Dados e na Exibição de Hierarquia) e ao menu de contexto mostrado para nós na Exibição de Hierarquia.
- Pesquisa de SubjectArea (a definição da ação é colocada dentro da definição de Pesquisa de SubjectArea). Estas ações personalizadas são adicionadas ao menu de contexto dos resultados de pesquisa.
- Filhos de Um-para-Muitos e Muitos-para-Muitos (a definição da ação é colocada dentro da definição do filho). Estas ações personalizadas são adicionadas ao menu de contexto da tabela filho.
- Exibição de Hierarquia (a definição de ação é colocada dentro da definição hmConfiguration). Essas ações personalizadas são adicionadas ao menu Mais Ações da Exibição de Hierarquia.

Nota: Com base nas funções do usuário, não é possível configurar ações personalizadas.

Ações personalizadas são definidas usando o elemento externalLinkAction, que tem os seguintes atributos:

Atributo	Descrição
nome	Nome utilizado internamente dessa ação personalizada. Esse nome deve ser exclusivo em todas as ações personalizadas.
displayName	Texto para o item de menu criado para essa ação personalizada. O valor especificado no XML de configuração é usado por padrão, mas pode ser substituído no pacote de recursos.
callback	O atributo deve ter o valor "true" para a ação de retorno de chamada (consulte abaixo para ver uma descrição de ações de retorno de chamada).
windowWidth	Largura da janela modal exibindo o resultado de uma ação de retorno de chamada. O valor padrão é 700.
windowHeight	Altura da janela modal exibindo o resultado de uma ação de retorno de chamada. O valor padrão é 600.

O elemento externalLinkAction deve conter um elemento externalLink que define a URL de ação personalizada.

O elemento externalLink definido para externalLinkAction dá suporte às mesmas configurações que o externalLink definido para externalLinkChild. Para obter mais informações, consulte a descrição de externalLink fornecida em "Guias Filho Personalizadas" anteriormente neste documento.

Como para o elemento externalLink da guia filho personalizada, o externalLink definido para externalLinkAction dá suporte a parâmetros dinâmicos substituídos em tempo de execução. Quando a ação é executada para vários registros (por exemplo, o usuário do aplicativo do IDD seleciona vários registros nos resultados da pesquisa e executa uma ação no menu de contexto de pesquisa), e a URL da ação tem um parâmetro dinâmico substituídos por dados das colunas do registro. O valor do parâmetro é construído a partir dos valores das colunas de todos os registros selecionados, separados por vírgulas. Por exemplo, uma ação é definida para a Pesquisa da Organização com a seguinte definição de URL:

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

```

        <param name="hl" staticValue="en"/>
    </externalLink>

```

Quando o usuário do aplicativo do IDD selecionar três organizações nos resultados da pesquisa com os nomes 'name1', 'name2', 'name3' e executa a ação, a URL da ação será a seguinte:

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

Ação Personalizada Padrão

Uma ação personalizada padrão abre uma nova janela do navegador que exibe a página solicitada de uma URL externa.

Veja a seguir um exemplo de ação personalizada definida para SubjectArea:

```

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

```

Se o usuário do aplicativo do IDD abrir a Organização com o nome "Informatica" e selecionar o item "Pesquisa do Google" no menu "Mais Ações", o IDD abrirá uma janela que exibe a seguinte URL:

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

Ação Personalizada com Retorno de Chamada

Uma ação personalizada também pode incluir um retorno de chamada.

Isso é útil quando o processo externo invocado pela ação personalizada pode modificar dados na área de assunto. Após essa modificação, a ação personalizada pode invocar o retorno de chamada para instruir o aplicativo do IDD a atualizar a área de assunto.

O IDD define uma função JavaScript denominada `refreshObject` para atualizar a área de assunto. Essa função requer um parâmetro - o ID interno do IDD referente ao registro modificado. Para disponibilizar esse ID aos aplicativos externos, a solicitação HTTP da ação personalizada deve transmiti-lo como um parâmetro (nesse caso, o aplicativo externo pode obter esse ID de uma solicitação e transmiti-lo de volta ao aplicativo do IDD). Para adicionar um ID de registro interno à URL de uma ação, um parâmetro de URL dinâmico com `bddParamName='SiperianRowID'` deve ser adicionado à definição de URL (consulte o exemplo de definição de ação de retorno de chamada mais adiante nesta seção).

Quando uma ação personalizada de retorno de chamada é invocada, o IDD abre uma janela modal contendo o elemento `<iframe>`, que exibe a página HTML recebida como resultado da solicitação HTTP da ação. Essa página HTML é capaz de chamar a função `refreshObject` usando o seguinte código JavaScript:

```

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

```


A janela modal na qual o resultado da solicitação da ação é exibido pode ser acessada a partir do JavaScript como `window.parent`. Por exemplo, uma página HTML gerada como resposta a uma ação pode conter a seguinte função JavaScript, que fecha a janela modal da ação e atualiza as exibições do IDD:

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

Observação Importante: Devido a restrições de segurança do navegador, a página HTML apenas será capaz de chamar a função JavaScript definida no aplicativo do IDD se essa página estiver localizada no mesmo domínio que o aplicativo do IDD (essa página deve ser servida pelo mesmo servidor de aplicativos no qual o aplicativo do IDD está implantado).

Veja a seguir um exemplo de ação de retorno de chamada definida para `SubjectArea`:

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

Se um usuário de aplicativo do IDD abrir uma Organização com `ROWID_OBJECT=1222` e depois chamar essa ação personalizada, o IDD abrirá uma janela modal exibindo a página solicitada da seguinte URL:

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

Em seguida, essa página pode chamar a função JavaScript `refreshObject` do aplicativo do IDD com o parâmetro `"BASE_OBJECT.C_PARTY|1222"` (o ID interno do registro de Organização aberto), o que faz com que o aplicativo do IDD atualize todas as exibições abertas para esse registro.

Segurança para Extensões Personalizadas

O acesso a guias filho personalizadas e a ações personalizadas é controlado por meio do SAM.

Quando um aplicativo do IDD é implantado, são criados Recursos Personalizados para cada guia filho personalizada e ação personalizada definidas na configuração do IDD. Os privilégios para esses recursos devem ser configurados com o uso do Console do Hub.

Guias Filho Personalizadas

Para guias filho personalizadas, os recursos são nomeados da seguinte maneira:

```
CUSTOM_EXTENSION/CUSTOM_CHILD_TAB:<name>
```

em que `<name>` é o nome exclusivo da guia filho, conforme especificado na configuração.

Uma guia filho personalizada será visível se o usuário de aplicativo do IDD tiver privilégios `READ` para o recurso de guia correspondente.

Ações Personalizadas

Para ações personalizadas, os recursos são nomeados da seguinte maneira:

```
CUSTOM_EXTENSION/CUSTOM_ACTION:<name>
```

em que <name> é o nome exclusivo da ação, conforme especificado na configuração.

Uma ação personalizada será exibida e poderá ser executada se o usuário de aplicativo do IDD tiver o privilégio EXECUTE para o recurso de ação correspondente.

Saídas de Usuário

Saídas de usuário fornecem um meio de adicionar lógica comercial personalizada a operações padrão do Informatica Data Director. É possível usar saídas de usuário dentro do espaço de trabalho de Dados.

Saídas de usuário são implementadas em Java. Para obter detalhes sobre as interfaces usadas para implementar saídas de usuário, consulte o Javadoc para `siperian-bdd.jar` que está incluído no Kit de Recursos do MDM Hub. O Kit de Recursos também contém um conjunto de saídas de usuário de exemplo. Esse conjunto de saídas de usuário inclui um projeto ant que pode ser usado como modelo para a construção de um arquivo JAR de saída de usuário.

Saídas de Usuário e a Estrutura do Entity 360

Saídas de usuário não têm suporte para uso com espaços de trabalho desenvolvidos na estrutura do Entity 360, como o espaço de trabalho de **Início** e o espaço de trabalho de entidade.

Com a estrutura do Entity 360, você pode usar funções de limpeza e validação no lado do servidor para substituir algumas das funcionalidades de saídas de usuário. Para obter mais informações, consulte o *Guia da Ferramenta de Provisionamento do Multidomain MDM*.

Nota: Para compatibilidade com versões anteriores, é possível continuar a usar saídas de usuário com o espaço de trabalho de **Dados**. Para exibir o espaço de trabalho de **Dados**, ative a propriedade `cmx.dataview.enabled` no arquivo `cmxserver.properties`. Para obter mais informações, consulte o *Guia de Configuração do Multidomain MDM*.

Operações de Saída de Usuário

Saídas de usuário têm operações e pontos de entrada definidos.

Para cada área de assunto, é possível implementar saídas de usuário para adicionar funcionalidade personalizada para as seguintes operações:

- Salvar
- Enviar para Aprovação
- Operações de Tarefa
- Mesclar
- Marcar como Não é uma Correspondência
- Operações Personalizadas
- Salvar Relacionamento do HM
- Operações Personalizadas do HM

- Abrir

A tabela a seguir descreve os pontos de entrada de saídas de usuário disponíveis para cada operação. Salvar, Enviar para Aprovação e Operações de Tarefas são variações no processo de salvar alterações na exibição de dados da área de assunto e fornecem o mesmo conjunto de pontos de entrada.

Operação	Ponto de Entrada	Descrição
Salvar, Enviar para Aprovação, Operações de Tarefas	beforeValidation	Nota: Esse ponto de entrada não tem mais suporte. Em vez disso, use o ponto de entrada beforeEverything.
	afterValidation	Nota: Esse ponto de entrada não tem mais suporte. Em vez disso, use o ponto de entrada beforeEverything.
	beforeEverything	Chamada antes que qualquer processamento seja feito. Use-a para realizar a validação ou ampliação personalizada dos dados na área de assunto. O Informatica Data Director salva as alterações feitas pela saída de usuário nos dados da área de assunto. Pode relatar Erros e Avisos e Confirmações. Pode definir datas de início e término para um período. Executada fora da transação de salvamento.
	beforeSave	Chamada após a pesquisa em busca de duplicatas, logo antes da realização da transação de salvamento composta. Use-a para executar uma lógica comercial personalizada que amplia os dados na área de assunto. O Informatica Data Director salva as alterações feitas pela saída de usuário nos dados da área de assunto. Pode relatar Erros. Executada como parte da transação de salvamento composta. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.
	afterSave	Chamada depois que as alterações na área de assunto são salvas. Use-a para realizar a manutenção dos dados que não fazem parte da área de assunto. Pode relatar Erros que reverterem a transação. Executada como parte da transação de salvamento composta. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.
	afterEverything	Chamada depois que a transação de salvamento é confirmada. Use-a para fornecer notificações de usuário ou realizar a manutenção de dados que não fazem parte da área de assunto quando as alterações não podem ser executadas como parte da transação. Pode relatar Avisos. Executada fora da transação de salvamento.

Operação	Ponto de Entrada	Descrição
Mesclar	beforeEverything	<p>Chamada antes que qualquer processamento seja feito.</p> <p>Use-a para realizar a validação ou ampliação personalizada dos dados na área de assunto.</p> <p>Pode relatar Erros e Avisos e Confirmações.</p> <p>Pode definir datas de início e término para um período.</p> <p>Executada fora da transação de salvamento.</p>
	beforeMerge	<p>Chamada logo antes de a mesclagem ser realizada.</p> <p>Use-a para executar uma lógica comercial personalizada para fornecer mensagens de erro ou de confirmação.</p> <p>Pode relatar Erros.</p> <p>Executada como parte da transação de mesclagem. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.</p>
	afterMerge	<p>Chamada depois que a operação de mesclagem foi concluída.</p> <p>Use-a para realizar uma manutenção para dados que não fazem parte da área de assunto.</p> <p>Pode relatar Erros que reverterem a mesclagem.</p> <p>Executada como parte da transação de mesclagem. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.</p>
	afterEverything	<p>Chamada depois que a transação de mesclagem é confirmada.</p> <p>Use-a para fornecer notificações de usuário ou realizar a manutenção de dados que não fazem parte da área de assunto quando as alterações não podem ser executadas como parte da transação.</p> <p>Pode relatar Avisos.</p> <p>Executada fora da transação.</p>
Marcar como Não é uma Correspondência	beforeEverything	<p>Chamada antes que qualquer processamento seja feito.</p> <p>Use-a para realizar a validação ou ampliação personalizada dos dados na área de assunto.</p> <p>Pode relatar Erros e Avisos e Confirmações.</p> <p>Pode definir datas de início e término para um período.</p> <p>Executada fora da transação de salvamento.</p>
	beforeMarkNotAMatch	<p>Chamada logo antes de uma transação de não correspondência ser realizada.</p> <p>Use-a para executar uma lógica comercial personalizada para fornecer mensagens de erro ou de confirmação.</p> <p>Pode relatar Erros.</p> <p>Executada como parte da transação de não correspondência. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.</p>

Operação	Ponto de Entrada	Descrição
	afterMarkNotAMatch	<p>Chamada depois que a operação de não correspondência é concluída.</p> <p>Use-a para realizar uma manutenção para dados que não fazem parte da área de assunto.</p> <p>Pode relatar Erros que reverterão a mesclagem.</p> <p>Executada como parte da transação de não correspondência. Solicitações SIF para o Armazenamento de Referências Operacionais farão parte dessa transação.</p>
	afterEverything	<p>Chamada depois que uma transação de não correspondência foi confirmada.</p> <p>Use-a para fornecer notificações de usuário ou realizar a manutenção de dados que não fazem parte da área de assunto quando as alterações não podem ser executadas como parte da transação.</p> <p>Pode relatar Avisos.</p> <p>Executada fora da transação.</p>
Operação do Usuário	processOperation	<p>Chamada quando o usuário do Informatica Data Director invoca a saída de usuário de operação personalizada no menu Mais Ações da exibição de dados.</p> <p>Use-a para executar uma lógica comercial personalizada. A saída de usuário pode retornar mensagens de Erro ou Aviso. A exibição de dados será atualizada se a transação for concluída sem erros, de forma que qualquer alteração na área de assunto feita pela saída de usuário seja refletida no Informatica Data Director.</p>
Salvar Relacionamento do HM	beforeEverything	<p>Chamada antes que qualquer processamento seja feito.</p> <p>Use-a para realizar a validação ou ampliação personalizada do relacionamento.</p> <p>Pode relatar Erros e Avisos e Confirmações.</p> <p>Pode definir datas de início e término para um período.</p> <p>Executada fora da transação de salvamento.</p>
	afterValidation	<p>Chamada depois que a validação e a execução da função de limpeza são realizadas.</p> <p>Use-a para realizar a validação ou ampliação personalizada do relacionamento.</p> <p>Pode relatar Erros e Avisos e Confirmações.</p> <p>Executada fora da transação de salvamento.</p>
	beforeSave	<p>Chamada logo antes da realização do salvamento.</p> <p>Use-a para executar uma lógica comercial personalizada que amplia os dados associados ao relacionamento.</p> <p>Pode relatar Erros.</p> <p>Executada como parte da transação de salvamento. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.</p>

Operação	Ponto de Entrada	Descrição
	afterSave	Chamada depois que as alterações no relacionamento são salvas. Use-a para realizar a manutenção dos dados associados ao relacionamento. Pode relatar Erros que reverterem o salvamento. Executada como parte da transação de salvamento. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.
	afterEverything	Chamada depois que a transação de salvamento é confirmada. Use-a para fornecer notificações de usuário ou realizar a manutenção de dados ao relacionamento quando as alterações não podem ser executadas como parte da transação. Pode relatar Avisos. Executada fora da transação de salvamento.
Operação do Usuário do HM	processOperation	Chamada quando o usuário do Informatica Data Director invoca a saída de usuário de operação personalizada no menu Mais Ações da exibição de dados. Use-a para executar uma lógica comercial personalizada. A saída de usuário pode retornar mensagens de Erro ou Aviso. A saída de usuário indica quais partes do gráfico precisam ser atualizadas como resultado da operação de saída de usuário.
Abrir	beforeOpen	Chamada antes da realização de uma operação de abertura. Use-a para marcar colunas como somente leitura no modo de edição e para substituir valores de colunas. Pode relatar erros, avisos, confirmações e mensagens personalizadas. Executada fora da transação de abertura
	afterOpen	Chamada depois que a operação de abertura é concluída. Use-a para enviar várias notificações aos dados na área de assunto. Além disso, você pode usá-la para fazer uma verificação personalizada dos dados que são carregados no banco de dados. Pode relatar erros, avisos, confirmações e mensagens personalizadas. Executada como parte da transação de abertura. Solicitações SIF para o Armazenamento de Referências Operacionais fazem parte dessa transação.

Cada saída de usuário é fornecida com os seguintes dados, que estão descritos em detalhes no Javadoc:

- os dados da área de assunto que estão sendo usados para operação
- um objeto SiperianClient que pode ser usado para realizar operações SIF no banco de dados de Armazenamento de Referências Operacionais, além do ID do Armazenamento de Referências Operacionais e das credenciais de usuário para uso em solicitações SIF
- dados específicos de operações

Criando Saídas de Usuário

As etapas básicas para a criação de saídas de usuário para um aplicativo do IDD são:

1. Desenvolver o código Java da saída de usuário.
2. Compilar e criar um arquivo jar contendo as classes de saídas de usuário.
Usar `siperian-bdd.jar` no Kit de Recursos do MDM. Esse arquivamento contém todas as classes e definições de interface específicas do IDD que são necessárias para a criação da implementação de Saídas de Usuário. Para obter mais informações, consulte o *Guia do Kit de Recursos do Multidomain MDM*.
Nota: O arquivo jar deve se chamar `UserExitsImplementation.jar`.
3. Use o Gerenciador de Configuração IDD para importar o arquivo JAR no seu aplicativo do IDD. (Você também pode incluir o arquivo JAR em um arquivo ZIP de aplicativo do IDD importado.)
4. Registre as classes de saídas de usuário na área de assunto.
5. Implante o aplicativo do IDD.

Configurando uma Saída de Usuário

Saídas de usuário são configuradas pela área de assunto.

Uma área de assunto pode ter saídas de usuário definidas para cada uma das operações de saída de usuário descritas anteriormente nesta seção.

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

O seguinte trecho de código é um exemplo de configuração de `ClassName` para as saídas de usuário de salvar relacionamento do HM no arquivo `IDDConfig.xml`.

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

Nota: Com base nas funções do usuário, não é possível configurar saídas de usuário.

Configurando uma saída de usuário para definir a data de início e a data de término de um período

Para definir a data de início e de término de um período no Informatica Data Director, você pode usar a interface `IEffectivePeriodSetters` na saída de usuário `beforeEverything`.

Nota: A interface `IEffectivePeriodSetters` só funciona para o manipulador `Save`. Ela não funciona para o manipulador `Save` do relacionamento `HM`.

O trecho de código a seguir é um exemplo de como definir a data efetiva de início e término:

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

Mensagens de Saída de Usuário

Saídas de usuário podem retornar uma mensagem (como um erro, um aviso ou uma confirmação) a ser exibida para o usuário.

O IDD manipula essas mensagens da mesma maneira que costuma manipular suas próprias mensagens. Cada mensagem tem um código que é uma chave para o pacote de recursos `ErrorCodeBundle.properties`. O IDD localiza o nível de erro (erro, aviso ou confirmação) e o texto da mensagem nesse pacote de recursos.

Nota: Use códigos exclusivos para mensagens personalizadas.

Essas strings de mensagens podem ser localizadas da mesma maneira que outras strings.

Mensagens podem ter parâmetros que são substituídos por dados especificados na saída de usuário. Esses parâmetros são manipulados com o uso da classe Java `MessageFormat`.

O formato das mensagens em `ErrorCodeBundle.properties` é:

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

em que

Item	Descrição
Código de erro	Chave exclusiva da mensagem.
Nível de erro	Um dos valores a seguir: <code>ERROR</code> , <code>WARNING</code> ou <code>CONFIRMATION</code> .
Título	Título da caixa de diálogo. O título deve descrever a localização e o contexto em que o problema ocorreu. Se não for especificado, o título será "Informatica Data Director".
mensagem principal	Mensagem de erro principal. Esse texto deve descrever o problema sob a perspectiva do usuário de aplicativo do IDD, e não sob uma perspectiva técnica interna. Por exemplo, algo como "Problema ao salvar xxx", e não "Erro de inserção".
Mensagem secundária	Parte secundária da mensagem, instruindo o usuário de aplicativo do IDD sobre o que fazer com relação ao problema. Na caixa de diálogo, essa parte será separada da mensagem principal por pelo menos uma linha em branco. Essa mensagem não deve ser muito longa.

Solução de problemas

Ao tentar entender por que uma saída de usuário não está operando corretamente, use as seguintes ferramentas padrão.

Ferramenta	Descrição
Logs	Exceções geradas na saída de usuário podem ser encontradas nos logs do Informatica MDM Hub. A saída de usuário também pode criar entradas no log usando log4j, conforme mostrado nas saídas de usuário de amostra.
Depurador	O depurador Java pode ser usado para percorrer a execução do código. Isso é feito da mesma forma como você pode depurar qualquer aplicativo Java implantado em um ambiente de servidor de aplicativos.

Localização

Pacotes de recursos contêm as cadeias que são exibidas em um aplicativo do Informatica Data Director.

Há cinco conjuntos de pacotes de recursos:

- BDDBundle
- ErrorCodeBundle
- MessagesBundle
- MetadataBundle
- MigrateBundle

Cada conjunto inclui o arquivo padrão, um arquivo de espaço reservado no idioma inglês e versões traduzidas desse arquivo, se houver.

Por exemplo, para o conjunto MessagesBundle, há o arquivo padrão MessagesBundle.properties e o arquivo de espaço reservado no idioma inglês MessagesBundle_en.properties.

Cada arquivo de pacote de recursos é um arquivos de propriedades codificado em UTF-8. Cada entrada no arquivo é um par de nome/valor, como <name>=<value>.

- <name> é um valor fixo referenciado pelo aplicativo do Informatica Data Director. Esse valor não pode ser alterado.
- <value> é a parte que pode ser traduzida.

Alguns exemplos:

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

Para adicionar arquivos de pacote de mensagens ao aplicativo do Informatica Data Director, é possível incluí-los no arquivo .zip do aplicativo que você importa. Como alternativa, importe arquivos de pacote de mensagens diretamente para um aplicativo existente no Informatica Data Director.

Nota: No arquivo MetadataBundle.properties traduzido, evite espaços nos nomes de tipos de relacionamento do Gerenciador de Hierarquia e de Tipos de hierarquia. O Informatica Data Director substitui espaços por sublinhados ao exibir esses valores traduzidos.

Quando você cria um aplicativo do Informatica Data Director, o Gerenciador de Configuração do Informatica Data Director gera pacotes de recursos padrão de cada tipo. Esses pacotes de recursos têm entradas para todos os rótulos usados no aplicativo do Informatica Data Director.

Para alterar ou traduzir esses pacotes de recursos, realize as seguintes etapas:

1. Exporte o aplicativo do Informatica Data Director.
2. Extraia os arquivos do arquivo .zip do aplicativo.
3. Crie um pacote de recursos com o sufixo de código de idioma ISO apropriado do seu idioma escolhido.
4. No seu idioma escolhido, edite os rótulos no pacote de recursos.

Nota: Para localizar os rótulos de grupos de áreas de assunto, além de nomes de grupos de menus lógicos e áreas de assunto, use o arquivo `BDDBundle.properties` com o sufixo de código de idioma apropriado.

5. Repita as etapas 3 e 4 para cada pacote de recursos que você deseja traduzir.

Configurando a página de login e o idioma de exibição padrão do Gerenciador de Configuração

O idioma do navegador da Web determina o idioma de exibição da página de login do Informatica Data Director e do Gerenciador de Configuração. É possível executar um script para definir o idioma exibido na página de login e na interface do usuário do Gerenciador de Configuração.

Esse script não define o idioma de exibição padrão do aplicativo do Informatica Data Director. Você pode definir o idioma de exibição do aplicativo do Informatica Data Director na opção de menu Alterar Idioma, abaixo do seu nome de usuário. Quando você define o idioma de exibição padrão da página de login e do Gerenciador de Configuração, o Informatica Data Director ignora a configuração de idioma do seu navegador da Web.

1. Execute o seguinte script para definir o código de idioma do parâmetro `globalLocale`:

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

O código de idioma ISO é um código de duas letras que representa o idioma. Por exemplo, o código de país "ja" representa o idioma japonês. Se você não definir um código de idioma ISO válido, o idioma de exibição será o inglês.

2. Reinicie o servidor de aplicativos.

Páginas de Erro Personalizadas

Você pode configurar o Informatica Data Director (IDD) para exibir a página de erro personalizada em vez de mensagens de erro do servidor de aplicativos. Por exemplo, quando um usuário insere uma URL incorreta, é possível configurar o IDD para redirecionar esse usuário à página de login ou a uma página de erro mais simplificada.

Para criar páginas de erro personalizadas, edite o arquivo `web.xml` e configure a página de forma que ela apareça quando um usuário se deparar com um erro em uma sessão do IDD.

O arquivo `web.xml` está na seguinte localização:

```
<diretório de instalação do infamdm>/hub/server/siperian-mrm.ear/zds-gui.war
```

Configurando uma Página de Erro Personalizada

Para criar as páginas de erro personalizadas, edite o arquivo `web.xml` e configure a página de forma que ela apareça para um determinado código de erro.

1. Extraia os arquivos do diretório `zds-gui.war`.
O diretório contém vários arquivos, entre eles `web.xml`.
2. Use um editor de texto para editar o arquivo `web.xml`.
No exemplo a seguir, a resposta HTTP 404 do aplicativo redireciona o usuário para a página `error_custom.html`.

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

Nota: Para garantir que página personalizada seja exibida para os usuários, adicione a página `error_custom.html` ao diretório `zds-gui.war`.

3. Salve as alterações no arquivo `web.xml` e reimplante o aplicativo do IDD.

Ajuda Online

Por padrão, um aplicativo do Informatica Data Director (IDD) inclui a ajuda do Guia do Usuário. Também é possível adicionar uma ajuda personalizada.

Ajuda do Guia do Usuário

A ajuda do Guia do Usuário descreve as tarefas que você pode realizar com um aplicativo do IDD. Por exemplo, a ajuda indica como adicionar uma entidade comercial ou mesclar entidades comerciais. O desenvolvedor de aplicativos do IDD pode substituir o arquivo de ajuda enviado por um arquivo de ajuda revisado. Versões localizadas do arquivo de ajuda também estão disponíveis. Se você alterar a localidade de um aplicativo do IDD, esse aplicativo exibirá a ajuda no mesmo idioma.

Ajuda Personalizada

A ajuda personalizada descreve as entidades comerciais ou áreas de assunto que estão definidas no aplicativo. O desenvolvedor de aplicativos do IDD cria a ajuda personalizada e a adiciona ao aplicativo.

Guia do Usuário do Data Director

O Guia do Usuário descreve as tarefas que os usuários comerciais podem executar no Data Director (IDD). Por exemplo, ele descreve como adicionar uma entidade comercial ou mesclar entidades comerciais.

Por padrão, o Data Director inclui o Guia do Usuário como um arquivo de ajuda online. O desenvolvedor de aplicativos do IDD pode substituir o arquivo de ajuda enviado por um arquivo de ajuda revisado. Os arquivos de ajuda revisados estão disponíveis na Informatica Network.

Baixando um Arquivo de Ajuda do Guia do Usuário Revisado

Você pode encontrar e baixar arquivos de ajuda revisados do Guia do Usuário na Informatica Network.

1. Em um navegador, abra a Informatica Network.
2. Procure "**Ajuda do Guia do Usuário do Informatica Data Director**".
Se você vir **Ajuda do Guia do Usuário do Informatica Data Director** nos resultados, significa que um arquivo de ajuda revisado está disponível para a versão especificada.
3. Selecione o link.
4. Anote o Número de Revisão. Você pode usar esse número para verificar se a ajuda correta é exibida.
5. Baixe o arquivo de ajuda.

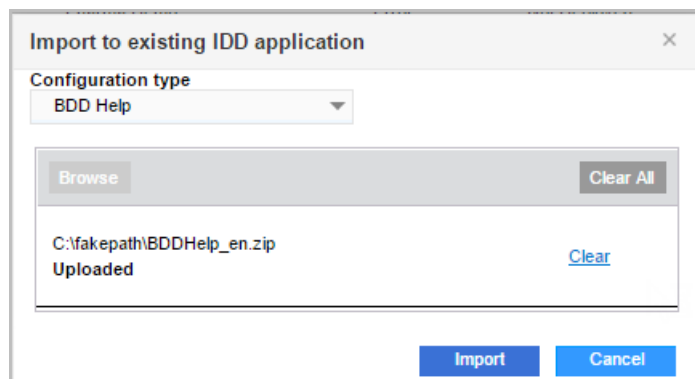
Importando um Arquivo de Ajuda do Guia do Usuário Revisado

Você pode importar um arquivo de ajuda revisado para os seus aplicativos do IDD.

O nome do arquivo de ajuda está no formato `BDDHelp_xx.zip`, em que `xx` é um código de idioma ISO. Se houver suporte para vários idiomas, importe os arquivos de ajuda localizados para cada idioma com suporte. A ajuda localizada é exibida quando um usuário seleciona a localidade correspondente no aplicativo do IDD.

1. Fazer login no Gerenciador de Configuração do IDD.
2. Selecione um aplicativo.
3. Clique em **Importar** > **Importar para aplicativo do IDD existente**.
4. Na caixa de diálogo **Importar para aplicativo do IDD existente**, selecione **Ajuda do BDD** na lista **Tipo de configuração**.
5. Clique em **Procurar**.
6. Na caixa de diálogo **Abrir**, selecione o arquivo de ajuda revisado e clique em **Abrir**.

A seguinte imagem mostra que a versão em inglês do arquivo de ajuda está pronta para ser importada:



7. Clique em **Importar**.

O processo de importação atualiza o aplicativo com a ajuda revisada do Guia do Usuário.

Testando a Ajuda Revisada

Depois de importar um arquivo de ajuda revisado, abra o aplicativo e verifique se a ajuda exibe o número de revisão correto.

1. Feche o aplicativo se ele estiver aberto.
2. Faça login no Informatica Data Director.
3. Se solicitado, selecione o aplicativo que contém a ajuda revisada.
4. No menu **Ajuda**, clique em **Ajuda**.
5. Verifique se o Número de Revisão na parte inferior do tópico Boas-vindas corresponde ao número associado ao arquivo de ajuda que você baixou.

Ajuda Personalizada

É possível criar uma ajuda personalizada que descreve as entidades comerciais ou áreas de assunto que você definiu no aplicativo do IDD. Depois de importar a ajuda personalizada e implantar o aplicativo, um item de menu **Ajuda Personalizada** é exibido no menu **Ajuda**.

Se houver suporte para vários idiomas, será possível criar arquivos de ajuda localizados para cada idioma com suporte. Quando um usuário seleciona a localidade no aplicativo do IDD, a ajuda personalizada localizada é utilizada.

Criando um Arquivo de Ajuda Personalizado

É possível criar um arquivo de ajuda personalizado para documentar seus aplicativos do IDD. Se houver suporte para vários idiomas, também será possível criar arquivos de ajuda localizados para cada idioma com suporte.

1. Em uma ferramenta de criação de HTML, crie os tópicos de ajuda personalizados e gere o projeto de ajuda.
2. Renomeie o arquivo `index.htm` como `bdd_help_CSH.htm`.
3. Crie um diretório denominado `bdd_help`.
4. Copie os arquivos e diretórios de ajuda gerados para o diretório `bdd_help`.
5. Selecione o diretório `bdd_help` e crie um arquivo `.zip` que preserve a estrutura de diretórios.
6. Use `CustomBDDHelp_xx.zip` como nome do arquivo `.zip`, em que `xx` é um código de idioma ISO de dois caracteres.
7. Verifique se o tamanho do arquivo `CustomBDDHelp_xx.zip` é 20 MB ou menos.

Importando um Arquivo de Ajuda Personalizado

É possível importar um arquivo de ajuda personalizado em aplicativos do IDD. Se você traduziu a ajuda personalizada, importe os arquivos de ajuda localizados também.

1. Fazer login no Gerenciador de Configuração do IDD.
2. Selecione um aplicativo.
3. Clique em **Editar**.
4. No painel Editar Aplicativo, marque a caixa de seleção **Ajuda Personalizada** e clique em **Salvar**.

No arquivo de configuração do aplicativo, a propriedade `help` é atualizada para definir `customBddHelp` como `true`:

```
<help bddHelp="true" customBddHelp="true"/>
```

5. Na árvore de navegação, clique em **Aplicativos**.
A lista de aplicativos é exibida.
6. Selecione o mesmo aplicativo.
7. Clique em **Importar > Importar para aplicativo do IDD existente**.
8. Na caixa de diálogo **Importar para aplicativo do IDD existente**, selecione **Ajuda Personalizada do BDD** na lista **Tipo de configuração**.
9. Clique em **Procurar**.
10. Na caixa de diálogo **Abrir**, navegue e selecione o arquivo `CustomBDDHelp_xx.zip` e clique em **Abrir**.
11. Clique em **Importar**.
O processo de importação atualiza o aplicativo com o arquivo de ajuda personalizado.
12. Clique em **Reimplantar**.

CAPÍTULO 6

Propriedades Globais do IDD

Este capítulo inclui os seguintes tópicos:

- [Referência a Propriedades Globais do Informatica Data Director, 95](#)
- [Atualizando as Propriedades Globais, 105](#)

Referência a Propriedades Globais do Informatica Data Director

A seguinte tabela lista as propriedades globais que controlam o comportamento em tempo de execução de todos os aplicativos do Informatica Data Director (IDD) em um único servidor de Hub.

Essa tabela descreve cada propriedade e seu valor padrão. Essas propriedades são armazenadas na tabela CMX_SYSTEM.C_REPOS_DS_PREF_DETAIL. Se as propriedades não estiverem definidas, os valores padrão especificados serão usados.

Importante: O servidor de aplicativos deve ser reiniciado para que as alterações nas propriedades globais a seguir entrem em vigor.

Propriedade	Valor padrão	Uso
allowDsEmptyChildren	false	Determina se os usuários poderão exibir registros filho quando você configurar um filtro de segurança em uma coluna neto, mas não houver registros neto. Se for <code>true</code> , os usuários poderão exibir os registros filho quando não houver registros neto. Se for <code>false</code> , os usuários não poderão exibir os registros filho quando não houver registros neto.
asyncChildLoading	false	Carrega os dados filho na Exibição de Dados quando você abre explicitamente o registro filho do objeto primário. Você pode definir o valor da propriedade como <code>true</code> para carregar os dados filho ao abrir o registro na Exibição de Dados.

Propriedade	Valor padrão	Uso
bulkexportloadsize	500	Tamanho máximo do carregamento para cada thread ao exportar dados para um arquivo do Microsoft Excel. O padrão é 500 registros. O máximo é de 1000 registros. Se definido como maior que 1000, o tamanho do carregamento padrão será usado.
CompositePagerTotalRecords	500	Número máximo de tarefas ActiveVOS que o IDD classifica de cada vez, sem distinção entre maiúsculas e minúsculas. Se as tarefas excederem o valor definido, o IDD classificará as tarefas ActiveVOS de acordo com o tipo de banco de dados. Se o banco de dados for Microsoft SQL Server, a classificação será sem distinção entre maiúsculas e minúsculas. Se o banco de dados for Oracle ou IBM DB2, a classificação fará distinção entre maiúsculas e minúsculas.
convert2DigitYearTo4Digit	false	Permite o ajuste de uma entrada de ano de dois dígitos para uma entrada de ano de quatro dígitos. Defina como <code>true</code> para permitir o ajuste das datas inseridas para 80 anos antes e 20 após a data atual. Por exemplo, se você inserir <code>1/Jan/30</code> como a data, o IDD interpretará a entrada como 1º de janeiro de 2030. Se você inserir <code>1/Jan/70</code> como a data, o IDD interpretará a entrada como 1º de janeiro de 1970.
credentialsAutofillDisabled	false	Por questões de segurança, se quiser controlar o navegador do usuário para impedir que ele salve credenciais de logon, como nome de usuário e senha, você poderá definir esse valor como <code>true</code> .
CSVColumnSeparator	Vírgula (,)	Determina o caractere a ser usado como separador de coluna quando você exportar os dados para um arquivo de valores separados por vírgula (CSV). Também é possível usar tabulação, ponto-e-vírgula e espaço como um delimitador.

Propriedade	Valor padrão	Uso
deleteMovedRelInExplorerView	true	Determina se é necessário excluir o relacionamento antigo quando você cria um novo relacionamento na exibição de explorador do Gerenciador de Hierarquia. Defina como false para definir uma data de término para o relacionamento antigo.
detectConcurrentUpdate	DISABLED	Determina se o registro que está sendo salvo é modificado simultaneamente por vários usuários. O padrão é DISABLED. Defina como SINGLE ou REPEATABLE para permitir que o Data Director detecte modificações simultâneas do registro. Quando você habilita essa propriedade, os usuários que editam o mesmo registro simultaneamente recebem uma notificação quando um deles tenta salvar o registro. Se o usuário continuar a salvar as alterações, as alterações feitas por outros usuários poderão ser substituídas.
enableCreateBEMenuGrouping	false	Especifica se você pode definir grupos lógicos para a janela Novo . Necessário se você tiver um grande número de áreas de assunto. Defina como true para definir grupos lógicos para a janela Novo . Defina como false se não quiser definir grupos lógicos para a janela Novo .
enableRememberCredentials	true	Quando "true", a caixa de seleção Memorizar Minhas Informações é exibida na página de logon. Os usuários permanecem conectados durante o período determinado por rememberCredentialsPeriod.
enableSaveForPeriodDialogForHmRel	true	Habilita a caixa de diálogo de período efetivo que aparece quando você atualiza um registro habilitado para o Gerenciador de Hierarquia no IDD. Defina como false para desabilitar a caixa de diálogo de período efetivo.

Propriedade	Valor padrão	Uso
enableTaskAttachments	false	<p>Especifica se os usuários podem anexar arquivos a tarefas ao usar as exibições herdadas com o Data Director.</p> <p>Defina como <code>false</code> para desativar anexos e ocultar a seção Anexos de Arquivo na caixa de diálogo Detalhes da Tarefa e na caixa de diálogo Criar Tarefa.</p> <p>Defina como <code>true</code> para ativar anexos.</p> <p>Importante: Para ver sua alteração no aplicativo do IDD, use o Configuration Manager do IDD para limpar o cache do aplicativo do IDD.</p>
expandDropDownListShowFullValue	false	<p>Permite a expansão da lista suspensa na guia Pesquisar para registros de pesquisa. Defina como <code>true</code> para permitir que a lista se ajuste para acomodar o item de lista maior.</p>
exportusingmultithread	false	<p>Ativa multithreading para exportar dados para um arquivo do Microsoft Excel. Defina como <code>true</code> para ativar multithreading para exportação de dados.</p>
handleUserExitBeforeShowingDialog	false	<p>Determina quando o IDD chama a saída de usuário <code>SendForApprovalHandler</code>.</p> <p>Defina como <code>true</code> para que o IDD chame a saída de usuário <code>SendForApprovalHandler</code> quando o usuário clicar em Enviar para Aprovação.</p> <p>Defina como <code>false</code> para que o IDD chame a saída de usuário <code>SendForApprovalHandler</code> quando o usuário clicar em OK na caixa de diálogo Enviar para Aprovação.</p>
HeaderBgColor	#000000	<p>Especifica o código de cores HTML da cor de plano de fundo da área de cabeçalho do IDD.</p>
hideSystemColumnsInResult	false	<p>Especifica se é necessário mostrar colunas do sistema nos resultados da pesquisa do IDD. Defina como <code>true</code> para ocultar as colunas do sistema nos resultados de pesquisa do IDD. Quando <code>true</code>, você ainda pode personalizar a exibição da tabela para selecionar manualmente as colunas do sistema a serem exibidas.</p>

Propriedade	Valor padrão	Uso
hmlInactiveRelationshipsAvailable	false	Defina como <code>true</code> para que o usuário possa ver relacionamentos inativos no Gerenciador de Hierarquia.
IDD2COCSCConverter.prefixCoNames	false	Quando a configuração do Informatica Data Director é convertida em uma configuração de entidade comercial, isso determina se um nome de área de assunto prefixado é usado para o nome da entidade comercial. Defina como <code>false</code> para usar o nome da área de assunto como o nome da entidade comercial. Defina como <code>true</code> para usar o nome da área de assunto prefixado com o nome do aplicativo do Informatica Data Director como o nome da entidade comercial.
isEffectiveDateIncluded	false	Especifica se você deseja incluir o campo Data Efetiva para consultas de pesquisa do Informatica Data Director. Defina como <code>true</code> para exibir a data atual no campo Data Efetiva. Defina como <code>false</code> para ocultar o campo Data Efetiva.
isFillOnGap	false	Especifica se você deseja ativar a propriedade Preencher a Lacuna para operações no Informatica Data Director. Defina como <code>true</code> para ativar a propriedade Preencher a Lacuna. Defina como <code>false</code> para desativar a propriedade Preencher a Lacuna.
lookupCacheUpdatePeriod	300000 (5 min)	O número de milissegundos que os dados de pesquisa podem estar no cache do IDD antes de serem recarregados.
minModalWidth	1100	Determina a largura mínima em pixels da janela Pesquisar .
maxCopiedChildrenNumber	10	Determina o número máximo de registros filho para cada tipo de filho que são copiados quando um usuário copia uma área de assunto.
maxCopiedGrandChildrenNumber	10	Determina o número máximo de registros neto para cada tipo de filho que são copiados quando um usuário copia uma área de assunto.

Propriedade	Valor padrão	Uso
maxImportThreads	5	Determina o número máximo de segmentos a serem usados durante a importação de dados.
maxParallelPromoteThreads	1	<p>Determina o número máximo de segmentos a serem usados quando você aprovar uma tarefa.</p> <p>Quando o <code>maxParallelPromoteThreads</code> for maior que 1 e você promover os registros de vários objetos base, o processo de promoção será executado em paralelo.</p> <p>O valor máximo do <code>maxParallelPromoteThreads</code> é igual ao número de núcleos de CPU do servidor.</p>
maxParallelSavedQueriesThreads	true	<p>Determina se as consultas são carregadas por meio de vários segmentos. Consultas com segmentos múltiplos são carregadas com mais rapidez.</p> <p>Defina como <code>true</code> para ativar a segmentação múltipla.</p> <p>Definir como <code>false</code> para desativar a segmentação múltipla.</p>
maxParallelBvtThreads	1	Determina o número máximo de segmentos a serem usados quando o IDD carregar uma tarefa para exibição.
maxSearchResultsExportedRows	5.000	Número máximo de linhas de dados de resultados de pesquisa que serão exportadas.
maxXrefSearchReturnCount	100	Especifica o número máximo de registros de referência cruzada que são retornados por uma solicitação de pesquisa.
needLoadChildOnOpen	false	<p>Defina como <code>true</code> para exibir inicialmente apenas os registros pai na exibição Correspondências. Os registros filho são exibidos à medida que você expande as guias de registros filho.</p> <p>Defina como <code>false</code> para exibir inicialmente os registros pai e todos os registros filho na exibição Correspondências.</p>

Propriedade	Valor padrão	Uso
openDashboardAfterTaskClose	false	Defina como <code>true</code> para que o Informatica Data Director abra o Iniciar espaço de trabalho depois que você concluir qualquer tarefa. Defina como <code>false</code> para que o Informatica Data Director abra a guia anterior na Exibição de Dados depois que você concluir qualquer tarefa.
overrideTextAreaColumnOrder	true	Por padrão, se você configurar uma coluna como uma área de texto em uma área de assunto, a coluna da área de texto sempre aparecerá na parte inferior do layout, independentemente da ordem das colunas. Defina como <code>true</code> para garantir que as colunas da área de texto em uma área de assunto apareçam na parte inferior do layout, independentemente da ordem das colunas. Defina como <code>false</code> para garantir que as colunas da área de texto apareçam em sua ordem especificada em um layout.
proactiveMatchResultSort	sortbyscorethenaction	Especifica a ordem de classificação na qual as correspondências potenciais aparecem. Defina como <code>sortbyscorethenaction</code> para classificar por corresponde a pontuações e, em seguida, por ação. Defina como <code>sortbyactionthenscore</code> para classificar por ação, como abrir e importar, e depois por corresponde a pontuações.
qrytaskidfromprocessidtotalretry	2	Número de tentativas que o IDD faz para recarregar uma tarefa ActiveVOS. Defina como um valor inteiro mais alto se você usa uma saída de usuário para administrar tarefas ActiveVOS e tarefas que não aparecem corretamente no IDD.
qrytaskidfromprocessidwaitintrvlmills	1.000	Número de milissegundos que o Informatica Data Director aguarda antes de tentar recarregar uma tarefa ActiveVOS. Defina como um valor inteiro mais baixo se você usa uma saída de usuário para administrar tarefas ActiveVOS e tarefas que não aparecem corretamente no IDD.

Propriedade	Valor padrão	Uso
rememberCredentialsPeriod	24 (horas)	Período de tempo (em horas) durante o qual as credenciais de usuário serão memorizadas se a caixa de seleção "Memorizar Minhas Informações" estiver marcada.
samCacheUpdatePeriod	600000 (10 min)	Determina por quanto tempo (em milissegundos) as funções do SAM (recursos com atribuições de privilégios) podem ficar no cache do IDD antes de serem recarregadas.
serverPageSize	100	Afeta a paginação dos resultados de pesquisas e dados filho. O IDD exibe ao usuário uma página de 10 registros. No entanto, o número de registros buscados do MDM Hub é determinado por essa propriedade. Com a configuração padrão, o IDD não solicitará dados adicionais até que o usuário acesse a 11ª página de dados.
search_empty_date	false	Determina se o campo de data efetiva na caixa de diálogo de pesquisa está vazio ou contém a data efetiva da Exibição de Dados quando você cria um registro filho. Defina como <code>true</code> para ter um campo de data efetiva vazio. Defina como <code>false</code> para fazer com que a data efetiva da Exibição de Dados preencha o campo de data efetiva.
searchForDuplicatesBeforeTaskDialog	false	Determina se a caixa de diálogo Possíveis Duplicatas é exibida antes ou depois de você enviar uma tarefa para aprovação. Defina como <code>true</code> para que a caixa de diálogo Possíveis Duplicatas seja exibida antes da caixa de diálogo Criar Tarefa . Defina como <code>False</code> para que a caixa de diálogo Possíveis Duplicatas seja exibida depois que você clicar em OK na caixa de diálogo Enviar para Aprovação .

Propriedade	Valor padrão	Uso
shouldDisableSearchFieldIfDependentFieldAbsence	false	Ativa ou desativa o campo de pesquisa dependente no formulário de pesquisa quando o campo de pesquisa pai não está presente nesse formulário ou não tem nenhum valor. Defina como <code>true</code> para ativar o campo de pesquisa dependente no formulário de pesquisa. Defina como <code>false</code> para desativar o campo de pesquisa dependente no formulário de pesquisa.
showMatchedColumns	#DBF5EC	Especifica o código de cor HTML da cor que identifica colunas correspondidas.
showShadowColumns	true	Especifica se mostrar as colunas de sombra na exibição de Referência cruzada. Defina como <code>true</code> para mostrar colunas de sombra. Defina como <code>false</code> para ocultar as colunas de sombra.
subjectAreaCopyDisabled	false	Determina se os usuários podem selecionar Copiar no menu Ações de uma área de assunto para copiar uma área de assunto. Defina como <code>true</code> para desativar a opção para copiar uma área de assunto. Defina como <code>false</code> para permitir a opção para copiar uma área de assunto.
table_default_width_key	-1	Determina a porcentagem de largura mínima de colunas de resultado da pesquisa.
tableMaxColumns	25	Determina o número de colunas que estão visíveis na exibição em tabela de registros filho e registros neto. O valor padrão permite 20 colunas visíveis e 5 colunas ocultas. Para garantir que você tenha colunas visíveis, especifique um inteiro maior que 5.

Propriedade	Valor padrão	Uso
tabsExpandByDefault	n/d	<p>Determina quais registros filho são expandidos por padrão na exibição de dados.</p> <p>Para expandir registros filho por padrão na exibição de dados, especifique o nome de cada área de assunto, separado por uma vírgula. Para expandir a guia XREF por padrão, especifique <code>xref</code>. Para expandir a guia Relacionamentos por padrão, especifique <code>hm_relationship</code>.</p> <p>Por exemplo, para expandir as guias XREF, Endereço de Entrega e Organização por padrão, especifique <code>xref, ShipAddress, Organização</code>.</p> <p>Se você não definir um valor para <code>tabsExpandedByDefault</code>, nenhum registro filho será expandido por padrão na exibição de dados.</p>
threadSchedulerIdleTime	5000 (segundos)	Determina o tempo ocioso máximo do agendador de segmentos.
transactionTimeout	30 (segundos)	O número de segundos que as transações têm para concluir a execução antes do tempo limite.
updateExistingPeriodByDefault	false	<p>Determina se a caixa de seleção Atualizar período existente está ativada por padrão.</p> <p>Defina como <code>true</code> para ativá-la por padrão.</p> <p>Defina como <code>false</code> para desativá-la por padrão.</p>
writeBOM	false	Exporta os resultados de pesquisa do Informatica Data Director como um arquivo CSV usando a codificação UTF-8 com uma marca de ordem de bytes. Se a pesquisa contiver caracteres ASCII estendidos, defina <code>writeBOM</code> como <code>true</code> para ver dados válidos quando você abrir o arquivo CSV.

TÓPICOS RELACIONADOS:

- [“Os Metadados do Informatica Data Director Não Foram Atualizados” na página 175](#)

Atualizando as Propriedades Globais

Para atualizar as propriedades globais, você pode executar o seguinte script SQL para o esquema CMX_SYSTEM.

O script SQL a seguir, quando usado para CMX_SYSTEM, inicializa as propriedades globais usando seus valores padrão. Atualize o campo VALUE neste script para modificar esses valores.

Nota: O script inclui a propriedade `enableTaskAttachment`. Você deve habilitar os anexos de tarefa na Ferramenta de Provisionamento para os tipos de tarefa que foram usados na área de assunto. Caso contrário, a propriedade `enableTaskAttachment` não entra em vigor.

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

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

insert into C_REPOS_DS_PREF_DETAIL
  (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
  'BDDGP.3', rowid_ds_pref, 'CompositePagerTotalRecords', '5000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
insert into C_REPOS_DS_PREF_DETAIL
  (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
  'BDDGP.4', rowid_ds_pref, 'convert2DigitYearTo4Digit', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
insert into C_REPOS_DS_PREF_DETAIL
  (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
  'BDDGP.5', rowid_ds_pref, 'credentialsAutofillDisabled', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

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

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

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

insert into C_REPOS_DS_PREF_DETAIL
```

```

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

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

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

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

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

insert into C_REPOS_DS_PREF_DETAIL
    (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
    'BDDGP.13', rowid_ds_pref, 'IDD2COCSCConverter.prefixCoNames', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

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

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

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

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

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

```

```

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

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

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

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

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

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

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

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

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

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

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

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

```

```

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

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

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

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

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

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

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

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

commit;
/

```

APÊNDICE A

Requisitos de Dimensionamento e Plataforma

Este apêndice inclui os seguintes tópicos:

- [Dimensionamento do Servidor de Banco de Dados, 109](#)
- [Dimensionamento do Servidor de Aplicativos, 109](#)
- [Dimensionamento do Cliente e da Rede, 109](#)
- [Requisitos de Configuração do Navegador, 110](#)

Dimensionamento do Servidor de Banco de Dados

As implantações do IDD não têm impacto direto sobre o dimensionamento do servidor de banco de dados.

Os requisitos de transação do IDD devem ser levados em consideração ao definir a seção de API do modelo de dimensionamento.

Dimensionamento do Servidor de Aplicativos

Um aplicativo do IDD é executado no servidor de aplicativos e está localizado em conjunto com os outros componentes do Servidor Informatica MDM Hub.

Os servidores de aplicativos devem ser dimensionados de forma a permitirem 1 núcleo de CPU/1 GB de memória para cada 10 sessões simultâneas de "usuário intenso" do IDD. O usuário intenso, para fins do modelo de dimensionamento, é definido como um usuário de um aplicativo do IDD que gera uma carga constante de 5 a 6 operações do IDD por minuto.

Dimensionamento do Cliente e da Rede

Estas são as configurações mínimas e recomendadas para máquinas cliente que acessam o Informatica Data Director:

Nota: A resolução de tela configurada para o Informatica Data Director é de 1280 x 1024.

Parâmetro	Valor
CPU	Mínimo: 1,6 GHz Recomendado: 2 GHz
Memória	Mínimo: 1 GB Recomendado: 2GB
A largura de banda da rede efetiva para o Servidor de Aplicativos	Mínimo: 10 Mbps Recomendado: 100 Mbps

Para obter mais informações sobre os requisitos de produto e as plataformas compatíveis, consulte a [Product Availability Matrix](#).

Requisitos de Configuração do Navegador

Você deve ativar o navegador nas máquinas cliente para permitir cookies.

Desative o bloqueador de pop-up se executar o Informatica Data Director no navegador Google Chrome.

APÊNDICE B

Componentes de Aplicativo

Este apêndice inclui os seguintes tópicos:

- [Referência a Componentes de Aplicativo, 111](#)

Referência a Componentes de Aplicativo

Um aplicativo do IDD é armazenado no banco de dados do sistema (CMX_SYSTEM.C_REPOS_DS_CONFIG) como um arquivo ZIP contendo arquivos de componente.

Esse arquivo ZIP pode ser exportado ou importado para o Gerenciador de Configuração IDD.

Nome do arquivo	Uso
IDDConfig.xml	Arquivo de configuração principal do aplicativo. Ele deve estar em conformidade com o esquema XML <code>siperian-bdd-config-6.xsd</code> .
BDDBundle.properties BDDBundle_XX.properties	Pacotes de recursos com rótulos para objetos definidos no aplicativo do IDD (como áreas de assunto e objetos filho).
MetadataBundle.properties MetadataBundle_XX.properties	Pacotes de recursos com rótulos para objetos definidos no ORS (como objetos base, colunas e assim por diante).
ErrorCodeBundle.properties ErrorCodeBundle_XX.properties	Pacotes de recursos com o texto para as mensagens de erro geradas por um aplicativo do IDD.
MessageBundle.properties MessageBundle_XX.properties	Pacotes de recursos com o texto exibido no aplicativo do IDD.
BDDHelp.zip BDDHelp_XX.zip	Arquivos de ajuda genéricos do IDD. Ajuda que descreve genericamente os recursos de um aplicativo do IDD.
CustomBDDHelp.zip CustomBDDHelp_XX.zip	Arquivos de ajuda do IDD personalizados. Ajuda que foi desenvolvida de forma a ser específica e exclusiva para um determinado aplicativo do IDD. Além de fornecer as instruções de uso específicas para implementação, esse arquivo de ajuda pode fornecer todas as informações relevantes, como procedimentos e diretivas de uma organização.
logo.gif, logo.png, logo.jpg ou logo.jpeg	Um substituto para o logotipo que o aplicativo do IDD exibe no canto superior esquerdo da tela. O tamanho do logotipo da Informatica é de 147 pixels de largura por 31 pixels de altura. Para obter melhores resultados, o logotipo de substituição deve ter dimensões semelhantes.

APÊNDICE C

Configuração de Segurança do IDD

Este apêndice inclui os seguintes tópicos:

- [Referência de Configuração de Segurança do IDD, 112](#)

Referência de Configuração de Segurança do IDD

As tabelas a seguir mostram as definições de configuração de segurança do IDD. Você define permissões no Console do Hub usando o Gerenciador de Acesso de Segurança.

Sugestão: O Gerenciador de Acesso de Segurança inclui os seguintes Grupos de Recurso: ALL_GLOBAL_RESOURCES, ALL_XREF e ALL_XREF_HISTORY. Use esses grupos quando quiser atribuir a mesma permissão a todos os recursos especificados. Por exemplo, você pode definir a permissão DELETE em todas as referências cruzadas selecionando a caixa de seleção DELETE na linha ALL_XREF.

Tabela 1. Geral

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Barra de Ferramentas Nova Área de Assunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		Y	Y	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	Y	-

Tabela 2. Exibição de Dados

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Criar Área de Assunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos	Y	-	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	Y	-	-	-	-
Ler Área de Assunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-
Atualizar Área de Assunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos	-	Y	Y	-	-	-
	BASE_OBJECT	NAME	-		-	Y	Y	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	Y	-
Excluir Área de Assunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	BO primário. O gerenciamento de Estado está ativado	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	-	-	Y	-	-
Copiar Área de Assunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		Y	Y	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	Y	-
Mostrar colunas do Sistema do BO	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO não é novo.	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-
Criar Objeto Filho	BASE_OBJECT	NAME	-	Para filhos um-para-muitos, apenas o próprio BO, para filhos muitos-para-muitos, o BO e seu BO de relação são marcados.	Y	Y	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	Y	-
Ler Objeto Filho	BASE_OBJECT	NAME	-	-	-	Y	-	-	-	-
Atualizar Objeto Filho	BASE_OBJECT	NAME	-	Para filhos um-para-muitos, apenas o próprio BO, para filhos muitos-para-muitos, o BO e seu BO de relação são marcados.	-	-	Y	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	Y	-

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Excluir Objeto Filho	BASE_OBJECT	NAME	-	O gerenciamento de estado está ativado. Para filhos um-para-muitos, apenas o próprio BO, para filhos muitos-para-muitos, o BO e seu BO de relação são marcados.	-	-	-	Y	-	-
	BASE_OBJECT	NAME	XREF	Referências cruzadas para o objeto filho devem ser selecionadas.	-	-	-	Y	-	-
	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Configuração necessária quando você usa a Exibição de Entidade.	-	Y	-	-	Y	-

Tabela 3. CM

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Exibir Xref	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO não é novo.	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-
	BASE_OBJECT	NAME	XREF	O BO primário e todos um-para-um Lógicos. Para filhos um-para-muitos, apenas o BO filho. Para filhos muitos-para-muitos, o BO filho e seu BO de relação.	-	Y	-	-	-	-
Localizar duplicatas	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-
Mesclar	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	Y

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
	BASE_OBJECT	NAME	-		-	-	-	-	-	Y
Desfazer Mesclagem	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	-	-	-	-	Y
Exibir Dados Brutos	BASE_OBJECT	NAME	RAW	-	-	Y	-	-	-	-

Tabela 4. Tarefas

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Enviar para aprovação (Novo Objeto Primário)	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos. O gerenciamento de Estado está ativado	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		Y	Y	-	-	-	-
	BASE_OBJECT	NAME	-	Filhos muitos-para-muitos. O gerenciamento de Estado está ativado	Y	Y	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	O Objeto Primário e todos os um-para-um lógicos	-	-	-	-	Y	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Padrão para aprovação	Y	-	-	-	-	-
Enviar para aprovação (Objeto Primário Existente)	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos. O gerenciamento de Estado está ativado	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	Y	-	-	-
	BASE_OBJECT	NAME	-	Filhos muitos-para-muitos. O gerenciamento de Estado está ativado	-	Y	Y	-	-	-

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	O Objeto Primário e todos os um-para-um lógicos	-	-	-	-	Y	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Padrão para aprovação	Y	-	-	-	-	-
Tarefa Enviar para Aprovação	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Os botões Enviar para Aprovação e Editar estão ativados para um novo registro criado. O botão Salvar está desativado.	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		Y	Y	Y	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ ReviewNoApprove		Y	-	-	-	-	-
Abrir tarefa do Iniciar espaço de trabalho	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA		-	-	-	-	Y	-
Criar Tarefa	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos os um-para-um Lógicos. O gerenciamento de Estado está ativado	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-
	BASE_OBJECT	NAME	-	Filhos muitos-para-muitos. O gerenciamento de Estado está ativado	-	-	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	O Objeto Primário e todos os um-para-um lógicos	-	-	-	-	Y	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Qualquer tipo de tarefa de criação	Y	-	-	-	-	-
Exibir Detalhes da Tarefa	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	-	-	-	-	-	Y	-

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Tarefa Mesclar	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Mesclar		Y	-	-	-	-	-
Tarefa Desfazer Mesclagem	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Desfazer Mesclagem		Y	-	-	-	-	-
Fila para mesclagem	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O botão Fila para Mesclagem está ativado.	-	Y	Y	-	-	Y
	BASE_OBJECT	NAME	-		-	Y	-	-	-	Y
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Mesclar		-	-	-	-	Y	-
Ação de Executar Tarefa	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA		-	-	-	-	Y	-

Tabela 5. Exibição de Histórico

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Exibir Histórico da Área de Assunto	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário persiste. O histórico foi ativado para o BO primário.	-	Y	-	-	-	-
Exibição de Histórico para Objeto Primário	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O BO primário e todos um-para-um Lógicos.	-	Y	-	-	-	-
	BASE_OBJECT	NAME	HISTORY		-	Y	-	-	-	-
	BASE_OBJECT	NAME	-	O histórico deve ser ativado para o BO.	-	Y	-	-	-	-
Exibição de Histórico para o BO Filho	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Para filhos muitos-para-muitos, os privilégios de relacionamento são levados em consideração.	-	Y	-	-	-	-
	BASE_OBJECT	NAME	HISTORY		-	Y	-	-	-	-

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
	BASE_OBJECT	NAME	-	O histórico deve ser ativado para o BO.	-	Y	-	-	-	-
Exibir Histórico de Xref do BO	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	O histórico deve ser ativado para o BO.	-	Y	-	-	-	-
	BASE_OBJECT	NAME	XREF_HISTORY		-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-
Exibir Histórico de Mesclagens do BO	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	Y	-	-	-	-
	BASE_OBJECT	NAME	-		-	Y	-	-	-	-

Tabela 6. Gráficos

Caso de uso	Grupo de Recursos	Nome	Subnome	Requisitos Especiais/ Comentários	C	R	U	D	E	M
Exibir Gráfico	CUSTOM_RESOURCE	BDD_NAME	CHART/ Exibir	-	-	Y	-	-	-	-

APÊNDICE D

Segurança de Dados

Este apêndice inclui os seguintes tópicos:

- [Visão Geral da Segurança de Dados, 119](#)
- [Aplicar a Segurança de Dados, 121](#)

Visão Geral da Segurança de Dados

Segurança de dados é a proteção dos dados contra tentativas acidentais ou não autorizadas de acesso, modificação, corrupção, destruição, duplicação ou divulgação durante operações como inserção, processamento, armazenamento, transmissão e saída, e esse acesso aos dados é devidamente controlado.

A segurança de dados do IDD assegura que os dados possam ser acessados pelos usuários com base nos seguintes critérios:

- Função de usuário
- Configuração da segurança de dados
- Dados armazenados no hub

Segurança de Dados Usando Filtros

A segurança de dados no Informatica Data Director é configurada usando a caixa de diálogo **Área de Assunto** no Gerenciador de Configuração do Informatica Data Director. Você pode definir filtros na coluna de área de assunto para restringir e proteger os dados de áreas de assunto que usuários individuais podem acessar. Filtros podem ser definidos na coluna do objeto primário, na coluna filho e na coluna neto. É possível configurar qualquer número de filtros para uma área de assunto e uma coluna de grupos de áreas de assunto.

A segurança de dados do Informatica Data Director dá suporte aos seguintes tipos de valores para filtros de segurança no tipo de coluna de tabela do banco de dados:

- Cadeia
- Número inteiro
- Flutuante

Nota: O valor de coluna de tabela do tipo Data não tem suporte por filtros de segurança de dados do Informatica Data Director.

Considere as seguintes regras e diretrizes ao trabalhar com filtros:

- Cada filtro de segurança é definido em colunas na área de assunto e consiste em um valor de filtro a ser aplicado a uma lista de funções.
- Filtros de segurança se baseiam em valores exatos e não em faixas ou comparações de curingas.
- Filtros devem ser definidos nas colunas de correspondência para aplicar filtros de segurança de maneira consistente entre pesquisas básicas, estendidas e avançadas.
- Filtros podem ser combinados. Um usuário com várias funções pode ter combinações de filtros aplicadas. O resultado é que um usuário tem acesso a todos os dados disponíveis em cada função atribuída por meio de uma união das atribuições de filtros.
- Filtros em diferentes colunas podem ser combinados para criar uma segurança de dados multidimensional.
- Vários filtros em uma única coluna para uma única função. Um usuário tem acesso a uma união de todos os dados que correspondem a cada filtro.
- Filtros em várias colunas para uma única função. Um usuário tem acesso à interseção de todos os dados que correspondem a cada filtro.
- Em ambientes IBM DB2, filtros em colunas com um tipo de dados flutuante não filtram além da escala da coluna. Por exemplo, se a escala da coluna for 1 e você definir o filtro como 1,2, os valores além dessa escala, como 1,21, também estão acessíveis.

Para obter mais informações, consulte a ajuda online do *Gerenciador de Configuração*.

Parâmetros de Segurança de Dados

Para restringir os dados que os usuários pertencentes a uma função específica podem acessar, você pode configurar os parâmetros de segurança de dados no arquivo `BDDConfig.xml`.

É possível configurar os seguintes parâmetros de segurança de dados:

securityFilter

Especifica a coluna que o Informatica Data Director (IDD) utiliza como base para filtragem. O atributo "columnUid" especifica o ID de coluna ou o caminho de correspondência.

securityValue

Especifica o valor que a coluna securityFilter deve ter para permitir que o usuário visualize os dados em um registro.

securityRole

Especifica a função à qual o filtro de segurança se aplica. O atributo "roleID" especifica o ID da função cujo acesso é restrito pelo filtro de segurança de dados.

Exemplo de Configuração de Objetos Pai de Segurança de Dados

Você precisa configurar a segurança no arquivo `BDDConfig.xml` para que os administradores de dados vejam o conteúdo que se aplica aos seus países. Os administradores de dados na França visualizam registros pai com um valor de país "FR", enquanto os administradores de dados no Japão visualizam registros pai com um valor de país "JA".

Para filtrar com base na localização de um administrador de dados, criar uma função no MDM Hub para cada região. Neste exemplo, você atribui aos administradores de dados na França a função "DSFrance" e atribui aos administrador de dados no Japão a função "DSJapan".

O seguinte trecho do arquivo `BDDConfig.xml` mostra como configurar a segurança de dados para esse exemplo:

```
<dataSecurity>
  <securityFilter columnUid="COUNTRY">
    <securityValue value="FR">
      <securityRole roleUid="DSFrance"/>
    </securityValue>
    <securityValue value="JA">
      <securityRole roleUid="DSJapan"/>
    </securityValue>
  </securityFilter>
</dataSecurity>
```

Exemplo de Configuração de Objetos Neto de Segurança de Dados

Você deseja que os administradores de dados na França visualizem registros filho e registros neto quando a coluna "Country" do registro neto `C_MT_ADDRESS` tiver o valor "FR".

Para filtrar com base na localização de um administrador de dados, criar uma função no MDM Hub para administradores de dados na França. Neste exemplo, você atribui aos administradores de dados na França a função "DSFrance". Use o componente de caminho de correspondência para o objeto neto quando especificar o valor "columnUid".

O seguinte trecho do arquivo `BDDConfig.xml` mostra como configurar a segurança de dados para esse exemplo:

```
<subjectArea name="Organization">
  <one2ManyChild name="Employee">
    <dataSecurity>
      <securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|COUNTRY">
        <securityValue value="RUS">
          <securityRole roleUid="DSFrance"/>
        </securityValue>
      </securityFilter>
    </dataSecurity>
  <one2ManyChild name="Address" mpcUid="C_MT_ADDRESS">
  </one2ManyChild>
</one2ManyChild>
</subjectArea>
```

Por padrão, os usuários não poderão exibir o registro filho se você configurar um filtro para uma coluna neto, mas o registro filho não tiver registros neto. Para permitir que os usuários exibam registros filho sem registros neto, defina a propriedade global "allowDsEmptyChildren" como `true`.

Aplicar a Segurança de Dados

A segurança de dados fornece a solução para proteger dados organizacionais, como dados transacionais, históricos, dinâmicos, hierárquicos e estáticos que as organizações obtêm, armazenam, criam, excluem e atualizam para a realização de processos comerciais.

Em um aplicativo do IDD, a segurança de dados definida em uma área de assunto é aplicada aos seguintes tipos de conteúdo:

- Dados de pesquisa
- Dados de entidade
- Dados hierárquicos
- Dados históricos

- Dados de tarefa.

Segurança de Dados em Dados de Pesquisa

A pesquisa do IDD permite que um usuário pesquise registros por área de assunto e grupo de áreas de assunto. Se uma área de assunto tiver filtros de segurança de dados para o usuário, os resultados da pesquisa deverão conter somente os registros que corresponderem à segurança de dados. A segurança de dados é aplicada a pesquisas básicas e difusas. Por exemplo, quando um usuário realiza uma pesquisa e tem acesso somente a pessoas na região CA, o resultado dessa pesquisa exibe somente os registros de pessoas na região CA.

Nota:

- Se um usuário com segurança de dados realizar uma pesquisa usando um termo de pesquisa, o resultado dessa pesquisa será uma interseção dos registros que correspondem à segurança de dados e daquilo que é retornado pela pesquisa.
- Se a eliminação de duplicatas da pesquisa para um registro filho não estiver ativada, e o usuário com segurança dos dados nos objetos primários tiver mais de um registro filho, o resultado da pesquisa terá todos os registros relacionados ao objeto primário.
- Quando a pesquisa é realizada por meio de um grupo de áreas de assunto, diferentes filtros de segurança de dados são usados.
- O IDD reduzirá todas as duplicatas se a quantidade de registros encontrados for menor que o tamanho da página do servidor configurado, por exemplo, se todos os resultados forem buscados após a primeira solicitação.

Segurança de Dados em Dados de Entidade

O IDD permite que um usuário acesse links de registro de Objeto Primário (OP), registro filho, registro neto e área de assunto por área de assunto e grupo de áreas de assunto. Se uma área de assunto tiver filtros de segurança de dados para um usuário, esse usuário poderá acessar apenas os registros que corresponderem à segurança de dados. As seguintes seções descrevem como a segurança de dados é aplicada a diferentes operações na exibição de dados.

Abrir um Registro

Filtros de segurança de dados garantem que somente os usuários autorizados possam abrir registros na exibição de dados.

Abrir um Registro Usando uma Única Função

Usuários com uma única função poderão abrir registros de objeto primário se as seguintes condições forem atendidas:

- O objeto primário deve corresponder a todos os filtros de segurança de dados existentes na coluna do objeto primário.
- O objeto primário deve ter pelo menos um registro aprovado nas restrições de segurança ativadas em cada guia filha com segurança de dados.

Por exemplo, considere um modelo de segurança de dados no qual um usuário tenha a função Gerente de Vendas - NY e os seguintes filtros de segurança configurados:

- Filtro 1: O código de estado é NY.

- Filtro 2: O tipo de telefone é Comercial e Residencial.
- Filtro 3: O código de saudação pessoal é MR.

Usando esse modelo de segurança de dados, considere um cenário no qual o banco de dados tem um registro de objeto primário, Mr. Steve Nash, com endereço de cobrança no estado de NY e tipo de telefone Comercial. Um usuário com a função Gerente de Vendas - NY pode abrir o registro Mr. Steve Nash na exibição de dados, pois o objeto primário corresponde ao filtro 3 e seus filhos correspondem aos filtros 1 e 2.

Usando o mesmo modelo de segurança de dados, considere outro cenário no qual o banco de dados tem um registro de objeto primário, Mr. Carlos Booser, com Endereço de Cobrança no estado de NY e tipo de telefone Celular. Um usuário com a função Gerente de Vendas - NY não pode abrir o registro Mr. Carlos Booser na exibição de dados porque esse registro não foi aprovado na restrição ativada na guia filho de Tipo de Telefone.

Filtrar Registros Usando uma Única Função

Usuários com uma única função poderão acessar os detalhes do objeto filho ou neto somente se este corresponder a todos os filtros de segurança de dados existentes na coluna filho ou neto do objeto primário.

Por exemplo, considere um modelo de segurança de dados no qual o usuário tenha a função SalesManager-NY e os seguintes filtros de segurança configurados:

- Filtro 1: O código de estado é NY.
- Filtro 2: O tipo de telefone é Comercial e Residencial.
- Filtro 3: O código de saudação pessoal é MR.

Usando o modelo de segurança de dados mencionado acima, considere um cenário no qual o banco de dados tem um registro de objeto primário: Mr. Robin Cameron, com endereço de Cobrança nos Estados CA, TX e NY e os tipos de telefone Comercial e Fax. Um usuário com a função Gerente de Vendas - NY pode ver apenas o Estado NY na guia Endereço de Cobrança e apenas o telefone Comercial na guia Telefones. Todos os outros registros em ambas as guias ficarão ocultos.

Filtrar Registros Usando Várias Funções

Por padrão, um usuário pertencente a várias funções pode acessar registros filho ou registros neto com base nos filtros de segurança de dados combinados.

Por exemplo, considere um modelo de segurança de dados no qual o usuário pertence às funções "Gerente de Vendas NY" e "Gerente de Vendas de Automóveis NJ".

A função "Gerente de Vendas NY" tem os seguintes filtros de segurança de dados:

- Filtro 1: O Código do Estado é "NY".
- Filtro 2: O Tipo de Telefone é "Comercial" ou "Residencial".

A função "Gerente de Vendas de Automóveis NJ" tem os seguintes filtros de segurança de dados:

- Filtro 1: O Código do Estado é "NJ".
- Filtro 2: O Ano do Carro é "2009".

Considere um cenário no qual o banco de dados tem um registro de objeto primário para John Smith. John tem endereços de faturamento com os valores de código de estado "NY", "NJ" e "TX". John tem números de telefone com os valores de tipo de telefone "Comercial" e "Fax". John tem um automóvel fabricado no ano de

2009 e outro fabricado no ano de 2001. O usuário com as funções "Gerente de Vendas NY" e "Gerente de Vendas de Automóveis NJ" visualiza as seguintes informações:

- O usuário vê os endereços de faturamento NY e NJ porque o filtro Código do Estado está configurado para ambas as funções.
- Se o atributo "affectFilter" para "securityValue" for `false`, o usuário verá números de telefone para todos os tipos de telefone e registros de automóvel para todos os anos. O Informatica Data Director (IDD) não aplica os filtros de segurança de dados para o tipo de telefone ou o ano do automóvel, pois esses filtros não estão configurados para ambas as funções.
- Se o atributo "affectFilter" para "securityValue" for `true`, o usuário verá os números de telefone para o tipo de telefone "Comercial" e dados de automóvel para o ano de 2009. O IDD aplica todos os filtros de segurança de dados que estão configurados para cada função. O padrão do atributo "affectFilter" é `true`.

Filtros de Segurança de Dados para Funções Herdadas

Você pode configurar filtros de segurança de dados para funções herdadas que são descendentes de uma função pai. Para configurar filtros de segurança de dados para funções herdadas, defina o atributo `affectFilter` para o parâmetro `securityFilter` no arquivo `BDDConfig.xml`.

Por exemplo, considere uma hierarquia de funções com uma função `DataSteward_NY` que seja descendente de uma função `DataSteward`. Um usuário pertencente à função `DataSteward_NY` também pertence à função `DataSteward`.

Você deseja configurar um filtro de segurança de dados que afeta somente os usuários pertencentes à função `DataSteward_NY`. Você deseja que os usuários pertencentes à função `DataSteward_NY` vejam registros contendo um valor `NY` para `STATE_CD`. É necessário definir o atributo `affectFilter` como `false` de forma a filtrar dados para a função `DataSteward_NY`. Quando o atributo `affectFilter` é `false`, o Informatica Data Director filtra os dados da função `DataSteward_NY` independentemente dos filtros de segurança de dados da função `DataSteward`.

O seguinte trecho do arquivo `BDDConfig.xml` mostra como configurar filtros de segurança de dados para esse exemplo:

```
<securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|STATE_CD">
  <securityValue value="NY">
    <securityRole roleUid="DataSteward_NY"/>
  </securityValue>
  <securityValue affectFilter="false">
    <securityRole roleUid="DataSteward"/>
  </securityValue>
</securityFilter>
```

Exibir Relacionamentos

No IDD, um relacionamento descreve a afiliação entre duas entidades específicas. Por exemplo, uma entidade de cliente pode ser logicamente vinculada a uma entidade de endereço.

A guia **Relacionamento** na Exibição de Dados contém informações sobre relações do Gerenciador de Hierarquia do objeto primário com outras entidades do Gerenciador de Hierarquia. Algumas das entidades do Gerenciador de Hierarquia podem ser transformadas em objetos primários que podem ser afetados pela segurança de dados.

Relacionamento deve conter apenas os relacionamentos que conectam entidades do Gerenciador de Hierarquia associadas aos objetos primários que correspondem às configurações de dados.

Mesclar Dados

Mesclagem é o processo de combinar dois ou mais registros porque eles são idênticos ou suficientemente semelhantes para serem considerados duplicatas. Mescle registros para consolidar dados duplicados em uma única entidade (entidade principal) que representa a melhor versão da verdade (BVT). Nos pontos em que os valores de atributos diferem, os valores retidos podem ser determinados por fatores diferenciados. Por exemplo, os valores retidos podem ser determinados com base na configuração de confiança desses registros ou com base em valores fornecidos por um usuário que preferiu editar o valor de substituição.

No aplicativo do IDD, a caixa de diálogo **Localizar Candidatos a Mesclagem** deve exibir somente os registros que são válidos de acordo com a segurança de dados da área de assunto do objeto primário.

Exportar Dados e Exportar Perfis

Todos os filtros de segurança de dados e o mascaramento de dados são aplicáveis tanto aos dados exportados quanto aos dados exibidos para o usuário.

Salvar um Registro

Um usuário pode salvar um registro somente depois do término da validação e da aplicação de todos os filtros de segurança de dados da área de assunto. Se um registro não corresponder aos requisitos dos filtros de segurança de dados, uma mensagem de aviso será exibido ao usuário.

Na caixa de diálogo com a mensagem de aviso, se você escolher **Sim**, objeto primário será salvo, e a guia será fechada. Se você escolher **Não**, o objeto primário não será salvo, mas o usuário poderá continuar a preender os detalhes desse objeto.

Localizar Duplicatas (Possíveis Correspondências)

Duplicatas são entidades em que os dados em determinadas colunas, como nome, endereço ou dados da organização, são idênticos ou suficientemente semelhantes para serem considerados quase idênticos. O IDD usa uma lógica de correspondência e atributos ativados para correspondência para determinar se duas entidades são suficientemente semelhantes para serem consideradas correspondências. Duplicatas são entidades que você leva em consideração para uma mesclagem.

Para pesquisar possíveis correspondências, clique em **Mais Ações** e escolha **Localizar Duplicatas**. Se uma área de assunto tiver filtros de segurança de dados para o usuário, os resultados de Localizar Duplicatas deverão conter somente os registros de OP que corresponderem à segurança de dados.

Por exemplo, considere um modelo de segurança de dados no qual o usuário tem uma única função, SalesManager- CA, e esse usuário executa uma pesquisa em busca de duplicatas para uma pessoa. O resultado da pesquisa terá indivíduos com pelo menos um endereço de cobrança no Estado de CA, e todas as outras duplicatas serão filtradas.

Nota: Se um usuário tiver mais de uma função e executar uma pesquisa em busca de duplicatas, ele poderá ver uma união de resultados que cada função é capaz de visualizar.

Segurança de Dados em Dados Hierárquicos

No IDD, uma hierarquia é um conjunto de tipos de relacionamento. Eles são apenas tipos de relacionamento agrupados para facilitar a classificação e a identificação. Quando a Exibição do Gerenciador de Hierarquia é aberta, primeiro ela verifica se a entidade âncora do Gerenciador de Hierarquia pode ser transformada em objeto primário e se essa entidade transformada em objeto primário está visível de acordo com a segurança de dados.

Adicionar Entidades do Gerenciador de Hierarquia

A entidade do Gerenciador de Hierarquia pode ser adicionada à tela usando operações Pesquisar e Criar.

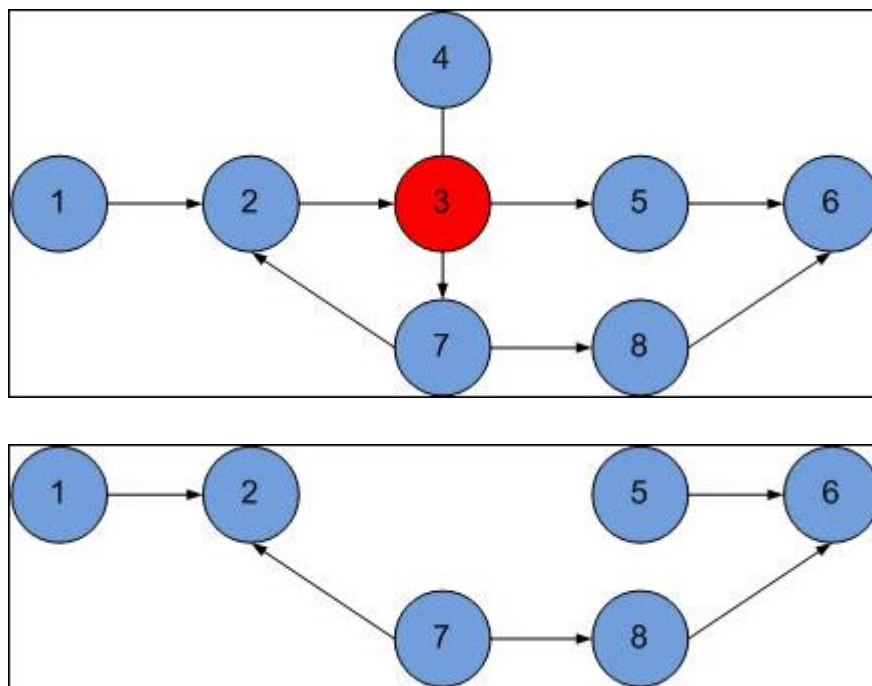
Nos resultados da pesquisa de dados, somente os registros permitidos pelo objeto primário da segurança de dados da área de assunto serão mostrados. Portanto, usando a opção Pesquisar, somente objetos podem ser adicionados.

Quando um usuário cria uma entidade do HM, ele pode salvar na exibição de dados um OP que não é válido de acordo com a Segurança de Dados. Se o usuário confirmar para salvar um OP que não ficará visível de acordo com a Segurança de Dados, essa entidade do HM não será adicionada à tela.

Representar Gráficos do Gerenciador de Hierarquia

As entidades do Gerenciador de Hierarquia podem ser transformadas em objetos primários. Objetos primários não visíveis como resultado da segurança de dados não são representados no gráfico do Gerenciador de Hierarquia como entidades do Gerenciador de Hierarquia. Se uma entidade do Gerenciador de Hierarquia não for visível para um usuário, o gráfico do Gerenciador de Hierarquia não deverá exigir essa entidade e sua subárvore.

Por exemplo, considere o seguinte gráfico o Gerenciador de Hierarquia, no qual um usuário não pode visualizar a entidade 3 devido à segurança de dados. Nesse caso, o gráfico deve estar visível para o usuário sem a entidade 3 e seu componente de subárvore, a entidade 4.



Nota: Usuários com várias funções podem acessar a união de todos os objetos que podem ser acessados por cada uma dessas várias funções.

Segurança de Dados em Dados Históricos

O IDD permite exibir o histórico de eventos de processamento de dados, como atualizações, exclusões e mesclagens, que ocorreram para a entidade selecionada. Se um objeto base corresponder aos requisitos de

segurança de dados, o histórico desse objeto base será mostrado, mesmo se no passado ele tenha ficado oculto devido à segurança de dados.

A Segurança de Dados no Histórico afeta as seguintes áreas:

- Histórico de objetos primários
- Eventos de histórico
- Histórico de Composição de objetos primários.

Abrir Detalhes de Histórico

Um usuário pode abrir o histórico de dados usando um link profundo ou como um componente no histórico no IDC. Nesse caso, a segurança de dados é aplicada pelo IDD para garantir que o objeto primário para o qual o histórico foi criado fique visível para usuários autorizados.

Exibir Eventos de Histórico

Eventos na exibição de Histórico fazem referência a objetos de área de assunto, objeto primário ou filhos de objeto primário. Se o objeto primário não está visível devido à segurança de dados, a exibição de Histórico não será mostrada. Se um registro filho não estiver visível devido à segurança de dados, a exibição de Histórico aparecerá para o objeto primário, mas os eventos de histórico do registro filho não serão adicionados à linha do tempo.

Segurança de Dados em Links Profundos

O recurso de vinculação profunda no aplicativo do IDD permite gerenciar o estado do aplicativo usando parâmetros de URL. Ele permite a definição de um determinado caminho de navegação interno na URL, que pode ser aberto no aplicativo do IDD.

Esse recurso também é usado para:

- Fornecer navegação entre o componente IDC e o aplicativo do IDD.
- Fornecer indicadores para partes específicas do aplicativo.

A segurança de dados do IDD afeta as seguintes áreas de links profundos:

- **Abrindo um registro:** o objeto primário e seus dados filho são verificados com base nas configurações de segurança de dados antes que uma nova guia mostre os dados do registro na exibição de dados.
- **Abrindo uma Tarefa:** Todas as configurações de segurança de dados mencionadas na seção [“Segurança de Dados em Dados de Tarefas” na página 156](#) são aplicáveis. Essas configurações de segurança de dados determinam se um usuário pode ou não abrir uma tarefa.

APÊNDICE E

Exemplo de Configuração de Segurança Baseada em Funções

Este apêndice inclui os seguintes tópicos:

- [Visão Geral do Exemplo de Configuração de Segurança Baseada em Funções, 128](#)
- [Principais Conceitos, 128](#)
- [Tarefas de Configuração de Segurança do IDD, 130](#)

Visão Geral do Exemplo de Configuração de Segurança Baseada em Funções

Este apêndice descreve um cenário simples para a configuração do acesso baseado em função a recursos seguros no Informatica Data Director (IDD).

Ele apresenta os principais conceitos e orienta ao longo das tarefas de configuração de segurança necessárias para implementar um cenário de amostra. O objetivo deste apêndice é fornecer aos implementadores do IDD alguns conhecimentos básicos sobre o que pode ser necessário para configurar a segurança em seus projetos de implementação do IDD.

Nota: Não se trata de um tutorial de laboratório para a criação de um aplicativo de amostra de trabalho. Ele é simplesmente uma orientação narrativa das ferramentas e tarefas envolvidas no suporte a um determinado cenário.

Principais Conceitos

Esta seção descreve os principais conceitos que você precisa compreender antes de implementar a segurança do IDD.

IDD, Gerenciador de Acesso de Segurança (SAM) e Estrutura de Integração de Serviços (SIF)

A maioria da funcionalidade IDD é implementada com o uso de chamadas SIF.

A SIF requer a configuração do SAM, que é altamente granular, para fornecer os direitos e os privilégios necessários para executar as chamadas SIF. A configuração do SAM envolve definir os usuários, as funções, os recursos seguros e os privilégios necessários no suporte para o acesso baseado em função a dados e operações.

Ferramentas para Configurar a Segurança do IDD

Você pode usar as seguintes ferramentas no Console do Informatica MDM Hub para configurar o SAM: Usuários, Usuários e Grupos, Funções e Recursos Seguros/Grupos de Recursos (incluindo pacotes e funções de limpeza).

Além disso, você pode usar o Gerenciador de Configuração IDD para associar sua configuração do SAM a objetos do IDD.

Leitura Relacionada

A documentação do Informatica a seguir fornece informações de referência importantes sobre o Gerenciador de Acesso de Segurança, a Estrutura de Integração de Serviços e a segurança do Data Director:

- *Guia de Segurança do Multidomain MDM*
- *Guia da Estrutura de Integração de Serviços do Multidomain MDM*, "Usando o Gerenciador de Acesso de Segurança com a API SIF"

TÓPICOS RELACIONADOS:

- ["Referência de Configuração de Segurança do IDD" na página 112](#)

Segurança de Objetos de Tarefas

É útil imaginar a segurança do IDD em duas categorias amplas:

- Segurança de objetos: Acesso a dados de áreas de assunto e a capacidade de realizar operações nesses dados (como exibir, criar, atualizar e mesclar) no IDD.
- Segurança de tarefas (fluxo de trabalho). Acesso a tarefas e ações com base em funções que são definidas no fluxo de trabalho.

Nota: Embora este cenário de exemplo enfatize apenas a segurança de objetos, muitas das ideias também são aplicáveis à segurança de tarefas no IDD, já que a segurança de tarefas depende do SAM também.

TÓPICOS RELACIONADOS:

- ["Fluxos de Trabalho e Tarefas" na página 22](#)

Dicas de Design de Segurança para Uso do IDD

A implementação da segurança do IDD é um processo repetitivo e contínuo.

Para começar, você precisa entender os vários tipos de acesso a recursos (objetos e operações) que os usuários do IDD precisarão ter no seu aplicativo do IDD.

No SAM, a *função* é o mecanismo central que determina o nível de acesso que um usuário possui a recursos do IDD. O SAM é altamente configurável e fornece controle granular sobre recursos. Considere criar uma função separada para cada combinação exclusiva de acesso a objetos/operações e atribua privilégios a essa função. Funções podem se basear em outras funções para criar camadas de privilégios em expansão. Uma vez configurada, você atribui usuários à função mais adequada para as responsabilidades de trabalho deles.

Este cenário de exemplo segue o princípio do *menor privilégio* - o acesso aos recursos é concedido apenas conforme necessário. Por padrão, os usuários não têm permissões. Você então concede seletivamente a esses usuários somente as permissões que são necessárias para concluir as operações pelas quais eles são responsáveis.

Importante: A configuração do SAM deve corresponder à configuração do IDD. Tudo o que é configurado no aplicativo do IDD também precisa ser configurado no SAM para fornecer privilégios suficientes para o suporte à funcionalidade do IDD configurada.

Outras Considerações

Ao planejar a segurança para o aplicativo do IDD, considere os seguintes pontos:

- Para o IDD acessar recursos do Informatica MDM Hub, esses recursos devem estar configurados como SECURE (não particulares) na ferramenta Recursos Seguros do Console do Hub.
- O SAM é configurada para cada ORS. Ao adicionar usuários do IDD, você precisa definir o esquema do IDD como o banco de dados padrão para esses usuários.
- No espaço de trabalho de Dados, os usuários do IDD normalmente não verão mensagens de erro explícitas referentes a privilégios insuficientes. Por exemplo, um determinado recurso pode simplesmente estar oculto do usuário, pois ele não está configurado para acessá-lo. Ao testar sua configuração de segurança, consulte o log do servidor para obter informações de depuração.
- Em um espaço de trabalho de entidade, o IDD exibe todos os recursos, independentemente da função do usuário. Quando os usuários realizam ações para as quais eles não têm a permissão de segurança necessária, o IDD exibe mensagens de erro.
- A configuração de segurança é armazenada em dois locais: No Servidor de Hub e no cache do IDD. Há um ligeiro atraso de tempo (1 minuto) para sincronizar as alterações. Em um ambiente de desenvolvimento, você pode reiniciar o servidor para atualizar o cache.

Tarefas de Configuração de Segurança do IDD

Esta seção discute a série de tarefas para implementar um cenário baseado em função de amostra: forneça aos usuários do IDD quatro níveis de privilégio diferentes (nenhuma permissão, somente leitura, criar e atualizar) para acessar um objeto base Party e os recursos afiliados.

Por exemplo, considere um cenário com duas áreas de assunto, como Party e Organization, no qual a área de assunto Party tem um relacionamento lógico de um-para-um com a área de assunto Organization. Na exibição de dados, para editar os atributos do registro, você deve ter o privilégio CREATE e UPDATE em ambas as áreas de assunto, que são C_PARTY e C_ORGANIZATION. Se alguns campos no objeto primário ou no objeto com um relacionamento lógico de um-para-um com esse objeto principal estiverem marcados como READ-ONLY, você ainda poderá editar o objeto primário. Os campos marcados como READ-ONLY são visíveis na exibição de Dados, mas não podem ser editados. Se todos os campos no objeto primário e no objeto com um relacionamento lógico de um-para-um com esse objeto primário tiverem permissões do tipo READ-ONLY, você não poderá editar o objeto primário na exibição de Dados.

Configurar Objetos de Design no Console do Hub

Antes de começar, você deve configurar todos os objetos de design no Console do Hub que serão usados pelo aplicativo do IDD.

Nesse cenário, os seguintes objetos são necessários:

- Objeto base Party (Gerenciador de Esquemas)
- Pacotes (ferramentas Consultas e Pacotes), que afetam a Pesquisa
- Regras de correspondência (Gerenciador de Esquemas), que afetam Localizar Duplicatas (possíveis correspondências)
- Funções de limpeza (ferramenta Funções de Limpeza), que afetam a entrada de dados (limpeza em linha dos dados após o salvamento)

Para obter mais informações sobre os objetos e as ferramentas do Console do Hub, consulte o *Guia de Configuração do Multidomain MDM*.

Nota: Embora este cenário descreva a configuração de apenas um objeto base, modelos de dados de clientes envolvem uma formação complexa de vários relacionamentos entre objetos base. O importante é que você configure a constelação inteira de objetos base e outros objetos de design que serão acessados por usuários do aplicativo do IDD.

Configurar os Usuários de Aplicativos IDD (Ferramenta Usuários)

Comece com a configuração do SAM, adicionando contas de usuário do IDD ao Banco de Dados Principais da sua implementação do Informatica MDM Hub.

Por exemplo, no Console do Hub, você pode executar a ferramenta Usuários e adicionar as seguintes contas de usuário:

Conta de Usuário	Atribuída com uma Função que Concede
user_1	Nenhuma permissão (padrão).
user_2	Permissão somente leitura no objeto base Party.
user_3	Permissão de criação no objeto base Party.
user_4	Permissão de atualização no objeto base Party.

Nota: Certifique-se de que cada usuário tenha acesso a todos os Armazenamentos de Registros Operacionais (ORS) associados ao aplicativo do IDD. Você também pode fazer isso na guia Usuários Atribuídos ao Banco de Dados da ferramenta Usuários e Grupos.

Configurar Recursos Seguros (Ferramenta Recursos Seguros)

Para que o IDD tenha acesso a um recurso, este deve estar sinalizado como SECURE na ferramenta Recursos Seguros.

Você deve garantir que todos os objetos de design configurados anteriormente estejam configurados como recursos SECURE.

- Objeto base Party, incluindo os seguintes itens associados:
 - conjuntos de regras de correspondência, que são usados no IDD para Procurar Duplicatas (possíveis correspondências)
 - metadados de conteúdo (HISTORY, RAW e XREF), que são usados no IDD para exibir o histórico de alterações, referências cruzadas e registros brutos
- funções de limpeza usadas para a entrada de dados
- pacotes usados para resultados de Pesquisa

Nota:

- Considere a criação de grupos de recursos para organizar recursos acessíveis pelo IDD e para agilizar a configuração da segurança.
- Se quiser impedir que todos os usuários do IDD tenham acesso a um determinado recurso, marque-o como PRIVATE. Por exemplo, você pode ocultar globalmente o acesso do IDD a registros RAW dessa maneira.

Criar e Configurar um Novo Aplicativo do IDD (Gerenciador de Configuração IDD)

No Gerenciador de Configuração IDD, crie um novo aplicativo do IDD e, em seguida, configure-o. Adicione um grupo de área de assunto (como Party Group) e, em seguida, a área de assunto Party.

Neste cenário, você deve especificar todas as colunas Party, o conjunto de regras de correspondência Party a ser usado para verificações de duplicatas (deve ser configurado como SECURE) e uma função de limpeza (deve ser configurada como SECURE). Quando terminar, salve as alterações e implante o aplicativo do IDD.

Nota: Uma maneira de restringir o acesso dos usuários às informações é especificar apenas um subconjunto de colunas para exibição na GUI do IDD. Mais tarde, você poderá configurar permissões para funções no nível da coluna, permitindo que alguns usuários vejam uma coluna, enquanto outros não.

Exibir Recursos Personalizados (ferramenta Recursos Seguros)

Quando você implanta um aplicativo do IDD no Gerenciador de Configuração IDD pela primeira vez, ele adiciona automaticamente um nó para o aplicativo no nó Recursos Personalizados.

Quando esse aplicativo é reimplantado, o Gerenciador de Configuração IDD adiciona/atualiza todos os objetos de design de suporte especiais como recursos SECURE. Esses objetos de suporte são necessários para a integração do IDD com o SAM. Depois de salvar as alterações na área de assunto e reimplantar o aplicativo, retorne à ferramenta Recursos Seguros e observe os recursos personalizados que foram automaticamente adicionados pelo arquivo de configuração do IDD.

Nota: Lembre-se que pode haver um ligeiro atraso entre o momento em que você salva a configuração do aplicativo e o momento em que ela é exibida na ferramenta Recursos Seguros.

Veja a seguir uma breve descrição desses recursos:

Recurso Personalizado	Expõe a Capacidade de
REPORT/View	Exibir relatórios no Iniciar espaço de trabalho.
SEARCH_QUERY/Create	Criar consultas particulares.
SEARCH_QUERY/CreatePublic	Criar consultas públicas.
SUBJECT_AREA/ BaseObject	Acessar a Área de Assunto no IDD. Você pode ver vários recursos SUBJECT_AREA recebendo seus dados do mesmo objeto base, mas representando diferentes exibições. Mesmo que a função tenha acesso ao objeto base, você também pode restringir privilégios sobre esses recursos para limitar quais recursos SUBJECT_AREA a função pode pesquisar, exibir e assim por diante.
TASK_TYPE/ SubjectArea:TaskType	Acessar a tarefa especificada para a área de assunto associada.

Configurar Funções e Privilégios de Recursos (Ferramenta Funções)

Funções fornecem um controle altamente granular sobre quais privilégios são atribuídos a quais recursos.

Para agilizar a sua configuração de segurança, você pode até mesmo criar uma hierarquia de funções, atribuindo funções a outras funções. No Console do Hub, use a ferramenta Funções para configurar as permissões necessárias para as operações do IDD realizadas por essa função.

Criar Funções

Comece criando as funções desejadas, como:

Nome da Função	Descrição
party_no_privileges_role	Padrão inicial. Nenhuma permissão para acessar algo (comparável a um usuário sem função atribuída). Este não é um cenário real - ele é fornecido para mostrar o que acontece à medida que privilégios são adicionados com outras funções.
party_read_only_role	Permissão somente leitura no objeto base Party.
party_create_role	Permissão de criação no objeto base Party.
party_update_role	Permissão de atualização no objeto base Party.

Configurar Privilégios de Recursos para Objetos Base e Objetos Afiliados

Em seguida, para cada função, você configura os privilégios de recursos para objetos base e objetos afiliados.

Para configurar permissões de objetos base na ferramenta Funções, selecione a função que você deseja configurar, expanda o nó Objetos Base, expanda o nó Party e configure os privilégios para o objeto base, os metadados de conteúdo e os conjuntos de regras de correspondência.

A seguinte tabela mostra os privilégios que você deve configurar para este cenário.

Nome da Função	Privilégios de Recursos
party_no_privileges_role	Nenhuma permissão.
party_read_only_role	<ul style="list-style-type: none"> - Privilégios READ a todas as colunas no objeto base PARTY - Privilégios READ a um conjunto de regras de correspondência aplicável - Privilégios READ a metadados de conteúdo (HISTORY, RAW e XREF).
party_create_role	<ul style="list-style-type: none"> - Privilégios READ a todas as colunas no objeto base PARTY. - Privilégios READ a um conjunto de regras de correspondência aplicável - Privilégios READ a metadados de conteúdo (HISTORY, RAW e XREF) - Privilégios CREATE a todas as colunas no objeto base PARTY (necessário para criar um novo registro) - Privilégios UPDATE a todas as colunas no objeto base PARTY (se você quiser permitir que essa função atualize um registro existente também)
party_update_role	<ul style="list-style-type: none"> - Privilégios READ a todas as colunas no objeto base PARTY. - Privilégios READ a um conjunto de regras de correspondência aplicável - Privilégios READ a metadados de conteúdo (HISTORY, RAW e XREF) - Privilégios UPDATE a todas as colunas no objeto base PARTY (necessário para salvar alterações em um registro)

Dicas:

- Se o seu objeto base tiver relacionamentos com outros objetos base (por exemplo, relacionamentos de pai-filho, pesquisas de chave externa ou relacionamentos de um-para-um), você precisará configurar o acesso a todos esses recursos também. Pesquisas exigem acesso READ, enquanto objetos base relacionados exigem permissões comparáveis às do objeto base principal).
- Você pode desativar seletivamente os privilégios READ em determinadas colunas para que os usuários não possam vê-las no aplicativo do IDD. Da mesma forma, você pode ativar privilégios READ e desativar privilégios UPDATE para que os usuários possam ver as colunas, mas não possam alterar dados.
- Você deve configurar o acesso READ a um conjunto de regras de correspondência para que a operação Localizar Duplicatas funcione.
- Você pode controlar se uma função pode exibir o histórico (requer privilégios READ em HISTORY), exibir referências cruzadas (requer privilégios READ em XREF) e exibir registros brutos (requer privilégios READ em RAW).
- Selecione (marque) **Mostrar Somente Recursos para essa Função** para ver rapidamente quais recursos estão atribuídos à função atual.

Configurar Privilégios de Recursos para Pacotes

Aplicativos do IDD usam pacotes para exibir resultados de pesquisa ao executar consultas na guia Pesquisar.

Funções devem ser configuradas para terem acesso READ a pacotes associados ao objeto base. Para configurar permissões de pacote na ferramenta Funções, selecione a função que você deseja configurar, expanda o nó Pacotes e configure privilégios para os pacotes aplicáveis.

Nome da Função	Privilégios de Recursos
party_no_privileges_role	Nenhum privilégio.
party_read_only_role	Privilégios READ no pacote Party.
party_create_role	Privilégios READ no pacote Party.
party_update_role	Privilégios READ no pacote Party.

Configurar Privilégios de Recursos para Funções de Limpeza

Se uma área de assunto estiver configurada para usar uma função de limpeza em linha (configurada no arquivo de configuração do IDD), a função deverá ter privilégios EXECUTE nessa função de limpeza para que esta última seja disparada após o salvamento.

Configurar Privilégios de Recursos para Recursos Personalizados

Em seguida, para cada função (exceto party_no_privileges_role), expanda o nó Recursos Personalizados, expanda o nó do aplicativo do IDD e atribua os seguintes privilégios:

Nome da Função	Privilégios de Recursos
party_no_privileges_role	Nenhuma permissão.
party_read_only_role	<ul style="list-style-type: none">- Privilégios READ ao recurso CHART/View, para que os usuários possam ver gráficos no Iniciar espaço de trabalho.- Privilégios CREATE para os recursos SEARCH_QUERY/Create e SEARCH_QUERY/CreatePublic (ou READ caso você queira que os usuários executem apenas consultas existentes, sem criarem novas consultas).- Privilégios READ para o recurso SUBJECT_AREA/Party.

Nome da Função	Privilégios de Recursos
party_create_role	<ul style="list-style-type: none"> - Privilégios READ ao recurso CHART/View, para que os usuários possam ver gráficos no Iniciar espaço de trabalho. - Privilégios READ e CREATE para os recursos SEARCH_QUERY/Create e SEARCH_QUERY/CreatePublic. - Privilégios READ e UPDATE em SUBJECT_AREA/Party (apenas se você quiser permitir que a função ignore o fluxo de trabalho completamente). Normalmente, os usuários têm privilégios READ e CREATE em TASK_TYPE/Party: ReviewNoApprove, que dá aos usuários acesso ao botão Enviar para Aprovação. - Privilégios READ e UPDATE para o recurso SUBJECT_AREA/Party.
party_update_role	<ul style="list-style-type: none"> - Privilégios READ ao recurso CHART/View, para que os usuários possam ver gráficos no Iniciar espaço de trabalho. - Privilégios READ e CREATE para os recursos SEARCH_QUERY/Create e SEARCH_QUERY/CreatePublic. - Privilégios READ e UPDATE no recurso SUBJECT_AREA/Party (apenas se você quiser permitir que a função ignore o fluxo de trabalho completamente). Normalmente, os usuários têm privilégios READ e UPDATE em TASK_TYPE/Party:ReviewNoApprove, que lhes dá acesso ao botão Enviar para Aprovação.

A forma como você configura o acesso a esses recursos personalizados afeta o que os usuários visualizam no aplicativo do IDD. Por exemplo:

- Se um usuário não tiver privilégios CREATE para SEARCH_QUERY/Create, ele não terá a opção de criar ou salvar uma nova consulta no IDD.
- Se um usuário não tiver privilégios CREATE para SEARCH_QUERYCreatePublic, ele não verá a opção Consulta Pública na caixa de diálogo Salvar Consulta como.
- Em geral, os usuários precisam ter privilégios READ e EXECUTE em tarefas que serão atribuídas a eles. Se um usuário não tiver privilégios CREATE para um determinado TASK_TYPE, ele não será capaz de criar essa tarefa no IDD.

Dicas de Configuração Adicionais

- Se quiser permitir que uma função seja capaz de mesclar dados e/ou desfazer a mesclagem de dados, você precisa conceder a ela privilégios MERGE no objeto base.
- Se quiser permitir que uma função abra registros na guia Exibição de Hierarquia, você precisa conceder acesso READ no recurso HM_PROFILE (o perfil Padrão ou outro recurso HM_PROFILE aplicável).

Conceda também os privilégios READ, CREATE, UPDATE e/ou DELETE apropriados nos recursos HM_RELATIONSHIP_TYPE e HM_HIERARCHY_TYPE.

Para adicionar uma entidade (Adicionar Entidade), a função deve ter privilégios CREATE na área de assunto. Para adicionar um relacionamento (Adicionar Relacionamento), a função deve ter privilégios CREATE na tabela REL, privilégios READ e CREATE em HM_PROFILE e privilégios READ e CREAT em HM_RELATIONSHIP_TYPE e HM_HIERARCHY_TYPE.

Atribuir Funções a Usuários (Ferramenta Usuários e Grupos)

No Console do Hub, use a ferramenta Usuários e Grupos para atribuir aos usuários do IDD as funções que você definiu.

Conta de Usuário	Atribuir à Função
user_1	party_no_privileges_role
user_2	party_read_only_role
user_3	party_create_role
user_4	party_update_role

Que IDD de Amostra os Usuários Podem Ver e Realizar

Depois que as funções tiverem recebido privilégios de recursos para recursos SECURE e os usuários tiverem sido atribuídos a funções, esses usuários poderão fazer login no aplicativo do IDD e ver o que está disponível para eles.

Neste exemplo, os usuários podem ver e realizar o seguinte:

Nome da Função	O Que o Usuário Pode Ver e Realizar
user_1 (nenhum privilégio)	<ul style="list-style-type: none">- No Iniciar espaço de trabalho, o usuário não pode exibir gráficos.- Na guia Dados, o usuário pode ver a guia Pesquisar, mas não pode exibir consultas públicas ou criar consultas.- Na guia Dados, o usuário pode ver as várias áreas de assunto nessa guia, mas não pode fazer nada com elas.
user_2 (privilégios somente leitura)	<ul style="list-style-type: none">- No Iniciar espaço de trabalho, o usuário pode exibir gráficos.- Na guia Dados (guia Pesquisar), o usuário pode executar uma consulta, exibir consultas públicas e exibir os resultados de pesquisa (incluindo todos os campos para registros individuais), mas não pode criar ou atualizar uma consulta.- Na guia Dados (área de assunto Party), o usuário não pode criar um novo registro.
user_3 (privilégios de criação)	<ul style="list-style-type: none">- No Iniciar espaço de trabalho, o usuário pode exibir gráficos.- Na guia Dados (guia Pesquisar), o usuário pode executar, criar e atualizar uma consulta.- Na guia Dados (área de assunto Party), o usuário pode criar um novo registro Party, adicionar dados e salvar alterações.
user_4 (privilégios de atualização)	<ul style="list-style-type: none">- No Iniciar espaço de trabalho, o usuário pode exibir gráficos.- Na guia Dados (guia Pesquisar), o usuário pode executar, criar e atualizar uma consulta.- Na guia Dados (área de assunto Party), o usuário pode editar um registro Party existente e salvar alterações, mas não pode criar um novo registro Party.

APÊNDICE F

Mascaramento de dados

Este apêndice inclui os seguintes tópicos:

- [Visão Geral do Mascaramento de Dados, 138](#)
- [Expressões, 138](#)
- [Padrões de Amostra, 139](#)
- [Definição de Máscara de Amostra, 139](#)

TÓPICOS RELACIONADOS:

- [“Mascaramento de dados” na página 24](#)

Visão Geral do Mascaramento de Dados

Este apêndice descreve o mecanismo de Mascaramento de Dados.

Esse mecanismo é usado para ocultar informações crítico de usuários do IDD que não têm autorização para acessar essas informações. Para campos mascarados, o IDD substitui parte dos caracteres (ou todos os valores de campos) por um asterisco (*).

O padrão de máscara é descrito em termos de expressões regulares. As partes da expressão que devem ser mascaradas estão entre parênteses.

Expressões

O padrão de máscara é descrito em termos de expressões regulares.

As partes da expressão que devem ser mascaradas estão entre parênteses.

.

Um ponto significa qualquer caractere.

.*

Um ponto seguido de um asterisco significa uma sequência de caracteres ou uma sequência vazia.

.+

Um ponto seguido de um sinal de adição significa um ou mais caracteres. Uma sequência vazia não é correspondida por essa expressão.

.{n}

Um ponto seguido de um número inteiro em chaves significa até n caracteres.

[.]

Um ponto entre colchetes significa um caractere de ponto.

Padrões de Amostra

Os exemplos a seguir mostram padrões de amostra.

Mascarar o valo do campo inteiro:

`(. +)`

Mascarar tudo, menos os três últimos caracteres:

`(. +) ...`

Deixar os quatro primeiros caracteres sem máscara:

`... (. +)`

Padrão que oculta os cinco primeiros caracteres, deixa três sem máscara e depois oculta o restante do valor, com exceção dos quatro últimos caracteres:

`(. {5}) ... (. +) ...`

Se o padrão especificado não corresponder o valor do campo, o valor inteiro será mascarado. Por exemplo, a string "ABS" não corresponde ao padrão `(. +) ...` porque este espera pelo menos quatro caracteres (um no início a ser mascarado e três no final a ser deixados sem máscara). Nesse caso, "ABS" é substituído por "****".

Definição de Máscara de Amostra

Definições de máscara podem aparecer no arquivo de configuração XML em qualquer seção Layout.

```
<layout columnsNum="3">
  <column columnUid="C_PRODUCT|PRODUCT_NUMBER" editStyle="FIELD"
    horizontalStyle="MEDIUM"
      required="true" showInHMCompactView="true">
    <dataMask value="... (. +)">
      <securityRole roleUid="Customer-CA"/>
    </dataMask>
  </column>
  <column lcolumnUid="C_PRODUCT|PRODUCT_NAME" editStyle="FIELD" horizontalStyle="MEDIUM"
    Requilred="true" showInHMCompactView="true"/>
  <column columnUid="C_PRODUCT|PRODUCT_DESC" editStyle="TEXT_AREA"
    horizontalStyle="MEDIUM"/>
  ...
</layout>
```

O exemplo anterior mostra a definição de máscara para a coluna Número do Produto. A máscara é aplicada aos usuários com a função de segurança Customer-CA.

Nota: Se nenhuma função de segurança estiver especificada para a definição de Máscara de Dados, a máscara será aplicada a todos os usuários não administradores.

APÊNDICE G

Mecanismo de Fluxo de Trabalho do Siperian BPM

Este apêndice inclui os seguintes tópicos:

- [O Siperian BPM está Obsoleto, 140](#)
- [Fluxos de Trabalho e Tarefas, 141](#)
- [Diagrama de Componentes de Configuração de Fluxo de Trabalho e Tarefas, 141](#)
- [Configuração de Tarefas, 142](#)
- [Tipos de Tarefa, 143](#)
- [Tipos de Tarefa - XML de Amostra, 143](#)
- [Atributos e Marcas TaskType, 144](#)
- [Personalização do Tipo de Tarefa, 147](#)
- [Tipos de Ação, 148](#)
- [Tipos de Ação - XML de Amostra, 148](#)
- [Atributos e Marcas ActionType, 149](#)
- [Configuração da Segurança de Tarefas, 150](#)
- [Atribuição de Tarefas, 151](#)
- [Notificação de Tarefas, 154](#)
- [Relatórios e métricas de gerenciamento de tarefas, 155](#)
- [Segurança de Dados em Dados de Tarefas, 156](#)

O Siperian BPM está Obsoleto

Na versão 10.0.0, mecanismo de fluxo de trabalho do Siperian BPM está obsoleto e será removido em uma versão futura. Anteriormente, o mecanismo de fluxo de trabalho do Siperian BPM era o mecanismo de fluxo de trabalho padrão no MDM Hub.

A Informatica recomenda atualizar os Data Director aplicativos (IDD) para usar ActiveVOS Server.

Para obter mais informações, consulte *Guia de Migração do Multidomain MDM Data Director*.

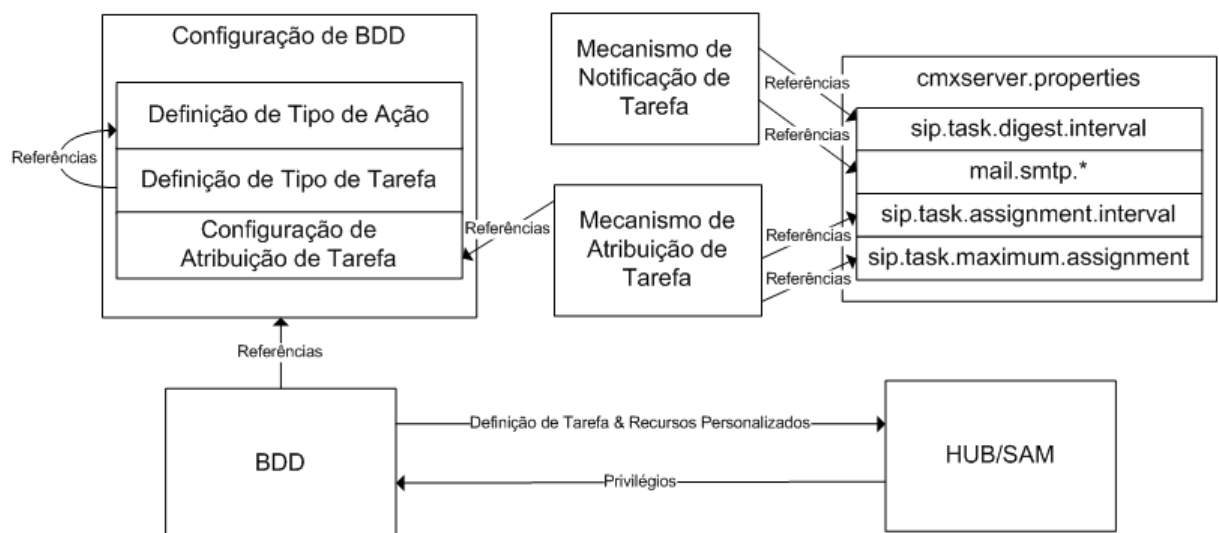
Fluxos de Trabalho e Tarefas

Ao usar a ferramenta Siperian BPM herdada ou as ferramentas BMP de terceiros, você precisa configurar as tarefas e o gerenciamento de tarefa do seu aplicativo do IDD.

Nota: Esta seção não se aplica ao Informatica ActiveVOS, seja autônomo ou incorporado. A versão incorporada usa tarefas predefinidas. A versão autônoma requer que você defina as tarefas em Informatica ActiveVOS.

Diagrama de Componentes de Configuração de Fluxo de Trabalho e Tarefas

O diagrama a seguir mostra os componentes da configuração de tarefas e fluxos de trabalho, bem como seus relacionamentos.



Descrições de Componentes de Configuração de Fluxo de Trabalho e Tarefas

Componente	Descrição
Definição do Tipo de Ação	<p><i>Tipos de ação</i> são os blocos fundamentais reutilizáveis para tarefas em um fluxo de trabalho. Eles definem o que uma tarefa fará quando uma ação for realizada no contexto dessa tarefa. Eles são reutilizáveis porque muitas tarefas fornecem subconjuntos semelhantes de ações que podem ser realizadas.</p> <p>Nota: Nesta versão, a Definição do Tipo de Ação pode ser personalizada apenas de uma maneira bastante limitada. No entanto, um nível de personalização adicional está planejado para as versões futuras.</p>
Definição de Tipo de Tarefa	<p><i>Tipos de tarefa</i> definem os tipos de tarefas que podem ser usados para criar fluxos de trabalho em um aplicativo do IDD. Essa seção da configuração permite a personalização de quais tarefas estão disponíveis, bem como o seu comportamento geral. Para obter mais informações, consulte "Tipos de Tarefa", mais adiante neste documento.</p>
Configuração de Atribuição de Tarefas	Usada para especificar o comportamento de mecanismos de atribuição de tarefas automáticos e manuais. Isso é configurado por meio do Gerenciador de Configuração IDD (consulte "Gerenciador de Configuração IDD", anteriormente neste documento).
Mecanismo de Notificação de Tarefas	É executado no Informatica MDM Hub e envia notificações por e-mail aos usuários em um intervalo configurado.
Mecanismo de Atribuição de Tarefas	É executado no Informatica MDM Hub e designa periodicamente tarefas não atribuídas a usuários configurados.
Arquivo cmxserver.properties	Especifica várias propriedades que podem ser definidas para configurar o comportamento de tarefas. Essas propriedades estão descritas em detalhes nas seções aplicáveis deste documento.
IDD	O aplicativo principal carrega a configuração na inicialização (e na implantação). O IDD também sincroniza a configuração de tarefas com o SAM, criando metadados de tarefas e recursos seguros personalizados no Informatica MDM Hub.
SAM	Fornecer informações ao IDD sobre quais privilégios são concedidos a usuários para tipos de tarefa.

Nota: Ao usar fluxos de trabalho e tarefas com um aplicativo do IDD, recursos de tarefas apenas estarão disponíveis se todos os objetos base envolvidos em uma área de assunto tiverem o gerenciamento de estado ativado no Gerenciador de Esquemas do Console do Hub. Isso é necessário porque certas tarefas usam registros pendentes, que estão disponíveis apenas quando o gerenciamento de estado está ativado.

Configuração de Tarefas

Cada aplicativo do IDD é inicializado com uma definição de fluxo de trabalho e tarefa padrão.

Atribuições de tarefas são configuradas no Gerenciador de Configuração IDD. Em muitos casos, a definição padrão será adequada. No entanto, a configuração da atribuição de tarefas sempre será necessária. Cada uma das subseções a seguir enfatiza uma parte dessa configuração.

Nota: Por padrão, a configuração de tarefas para o IDD é um processo de aprovação de duas etapas.

Tipos de Tarefa

Essa seção do arquivo de configuração do IDD especifica os tipos de tarefas que estão disponíveis para uso em um aplicativo do IDD.

Tipos de tarefa são o componente de tarefa mais configurável. Essa seção determina o comportamento de tarefas no Informatica MDM Hub, juntamente com o fluxo de uma tarefa para a seguinte.

A configuração padrão do IDD inclui sete tarefas predefinidas:

Tarefas Predefinidas	Descrição
UpdateWithApproval	Atualizar um registro, e a próxima etapa requer que o usuário passe por um processo de aprovação antes de concluir a tarefa.
UpdateWithOptionalApproval	Atualizar um registro, e a próxima etapa não requer que o usuário passe por um processo de aprovação antes de concluir a tarefa. A etapa de aprovação é opcional.
ReviewNoApprove	Revisar uma alteração e escalá-la ou rejeitá-la. Essa tarefa não fornece uma opção Aprovar e requer que pelo menos uma outra pessoa revise as alterações também.
FinalReview	Revisar uma alteração e aprovar, rejeitar ou escalar.
Mesclar	Mesclar registros.
Desfazer Mesclagem	Desfazer a mesclagem de um registro de XREF de um registro de Objeto Base.
UpdateRejectedRecord	Atualizar um registro que foi rejeitado em um processo de aprovação.

Tipos de Tarefa - XML de Amostra

O trecho de amostra a seguir do arquivo de configuração do IDD pertence a tipos de tarefa (e será referenciado mais adiante nesta subseção).

```
<!-- Task Definitions -->
  <taskType name="UpdateWithApproval" displayName="Update With Approval"
    creationType="create">
    <description>Update a record and require the user to go through
      an approval process before completing the task.
    </description>
    <action name="SubmitForApproval">
      <targetTask>ReviewNoApprove</targetTask>
    </action>
    <action name="Augment">
      <targetTask>UpdateWithApproval</targetTask>
    </action>
    <action name="CancelTask"/>
  </taskType>
  <taskType name="UpdateWithOptionalApproval" displayName="Update With Optional
Approval"
    creationType="create">
    <description>Update a record and do not require the user to go through
      an approval process before completing the task. The approval
step
      is optional.
    </description>
    <action name="CompleteUpdate"/>
    <action name="SubmitForApproval">
```

```

        <targetTask>ReviewNoApprove</targetTask>
    </action>
    <action name="Augment">
        <targetTask>UpdateWithOptionalApproval</targetTask>
    </action>
    <action name="CancelTask"/>
</taskType>
<taskType name="ReviewNoApprove" displayName="Review" defaultApproval="true"
    creationType="none" pendingBVT="true">
    <description>Review a change and either escalate or reject it. This task
        does not provide an Approve option and requires at least one
        other person to review the changes as well.
    </description>
    <action name="Reject">
        <targetTask>UpdateWithApproval</targetTask>
    </action>
    <action name="Escalate">
        <targetTask>FinalReview</targetTask>
    </action>
    <action name="Reassign">
        <targetTask>ReviewNoApprove</targetTask>
    </action>
    <action name="CancelTask"/>
</taskType>
<taskType name="FinalReview" displayName="Final Review" creationType="none"
    pendingBVT="true">
    <description>Review a change and approve, reject or escalate it.</
description>
    <action name="Approve"/>
    <action name="Reject">
        <targetTask>UpdateWithApproval</targetTask>
    </action>
    <action name="Escalate">
        <targetTask>FinalReview</targetTask>
    </action>
    <action name="Reassign">
        <targetTask>FinalReview</targetTask>
    </action>
    <action name="CancelTask"/>
</taskType>
<taskType name="Merge" displayName="Merge" creationType="merge"
displayType="merge">
    <description>Merge two records together.</description>
    <action name="Reassign">
        <targetTask>Merge</targetTask>
    </action>
    <action name="CancelTask"/>
</taskType>
<taskType name="Unmerge" displayName="Unmerge" creationType="unmerge"
    displayType="unmerge">
    <description>Unmerge an XREF record from a Base Object record.</description>
    <action name="Unmerge"/>
    <action name="Reassign">
        <targetTask>Unmerge</targetTask>
    </action>
    <action name="CancelTask"/>
</taskType>

```

É possível personalizar fluxos de trabalho e tarefas alterando as propriedades de tipos de tarefa. É necessário ter cuidado sempre que a definição de tarefa é modificada, pois erros aqui poderão fazer com que as tarefas se tornem inutilizáveis em um aplicativo do IDD. A definição de tarefa inclui as propriedades a seguir.

Atributos e Marcas TaskType

nome

O atributo name é o identificador do tipo de tarefa. Não use espaços e caracteres não ASCII no atributo name.

O atributo name é para uso interno por um aplicativo do IDD e pelo Informatica MDM Hub. Dessa forma, não é necessário alterar essas configurações. Se você introduzir um novo tipo de tarefa, especifique qualquer nome, pois ele não será significativo.

displayName

O atributo displayName especifica o nome da tarefa que deve aparecer em um aplicativo do IDD.

Porém, o nome real mostrado em um aplicativo do IDD é obtido de um pacote de recursos e, portanto, alterações no valor de displayName podem não resultar em alterações visíveis correspondentes no aplicativo do IDD implantado. O nome de exibição é usado como o valor padrão quando o IDD recupera o nome de exibição localizado de um pacote de recursos.

creationType

Esse atributo não deve ser modificado para tarefas existentes.

Ele é usado para determinar onde uma tarefa pode ser criada em um aplicativo do IDD. Os valores possíveis são:

creationType	Descrição
create	Tarefas são criadas quando o usuário de aplicativo do IDD escolhe Criar Tarefa em um menu de um aplicativo do IDD. Nota: Ao criar uma tarefa usando Mais Ações > Criar Tarefa , na janela Criar Tarefa , apenas as tarefas configuradas como CREATE para a opção Tipo de Criação serão listadas no campo suspenso Tipo .
mesclar	Uma tarefa é criada quando o usuário de aplicativo do IDD escolhe o comando para criar uma tarefa na exibição Possíveis Correspondências. Nota: Apenas um tipo de tarefa deve ter essa designação.
unmerge	Tarefas são criadas quando o usuário de aplicativo do IDD escolhe o comando para criar uma tarefa na caixa de diálogo Referências Cruzadas. Nota: Apenas um tipo de tarefa deve ter essa designação.
none	Tarefas não podem ser criadas por um usuário de aplicativo do IDD no aplicativo do IDD. Essa designação significa que esses tipos de tarefa só podem ser criados como resultado de um fluxo de trabalho.

Exemplo: O tipo de tarefa FinalReview tem essa designação no exemplo de código anterior porque ele só pode ser criado como parte de um fluxo (quando a ação Escalar é executada em uma tarefa ReviewNoApprove).

displayType

Esse atributo especifica como uma tarefa deve ser exibida quando ela é aberta na exibição de dados.

Os valores possíveis são:

displayType	Descrição
Normal	A tarefa é aberta na exibição de dados com o menu de ações de tarefa disponível. A exibição de dados apresentará o registro de dados associado à tarefa.
Mesclar	A tarefa é aberta na exibição de dados com o menu de ações de tarefa disponível. A guia filho Possíveis Correspondências está visível e selecionada na exibição de dados. A possível correspondência associada à tarefa é realçada e automaticamente selecionadas na guia filho Possíveis Correspondências.
desfazer mesclagem	A tarefa é aberta na exibição de dados com o menu de ações de tarefa disponível. A caixa de diálogo Referências Cruzadas é aberta sobre a exibição de dados. O registro de referência cruzada cuja mesclagem deve ser desfeita está selecionado nessa caixa de diálogo.

dataUpdateType

Um dos seguintes valores.

dataUpdateType	Descrição
ACTIVE	As modificações feitas no registro mostrado na exibição de tarefa antes da execução dessa ação são salvas no estado ACTIVE.
PENDING	As modificações feitas no registro mostrado na exibição de tarefa antes da execução dessa ação são salvas no estado PENDING. Esse valor é usado para todos os fluxos de aprovação, para salvar alterações como pendentes até que elas sejam aprovadas.
NONE	As modificações feitas no registro mostrado na exibição de tarefa antes da execução dessa ação serão perdidas. Nesse caso, o usuário de aplicativo do IDD vê uma caixa de diálogo de confirmação para garantir que ele deseja descartar as alterações feitas no registro. As alterações podem ser salvas com o botão Salvar na exibição de dados antes da execução da ação da tarefa.

pendingBVT

Esse atributo especifica se a exibição de dados deve incluir valores de referências cruzadas pendentes ao construir a exibição de BVT em um aplicativo do IDD.

Quando definido como "true", todas as referências cruzadas pendentes mencionadas pela tarefa serão incluídas na exibição de BVT e, como resultado, o usuário de aplicativo do IDD terá uma exibição "hipotética" do registro, exatamente como ela seria se as referências cruzadas pendentes se tornassem ativas. Isso é útil para a aprovação de alterações pendentes e para tentar decidir se o registro resultante seria correto.

defaultApproval

Esse atributo deve ser definido como "true" em exatamente um tipo de tarefa.

O tipo de tarefa com o valor "true" para esse atributo é o tipo de tarefa que será criado quando o botão **Enviar para Aprovação** for clicado na exibição de dados do IDD.

Nota: Se vários tipos de tarefa tiverem esse atributo definido como "true", resultados inesperados poderão ocorrer se o tipo de tarefa for criado quando o botão **Enviar para Aprovação** for clicado.

Marca de Descrição

Esse elemento fornece uma rápida descrição da finalidade do tipo de tarefa.

Marca de Ação

Esse elemento é uma referência a um tipo de ação descrito na seguinte seção.

Marca de Tarefa de Destino

Essa marca é opcional em cada ação de tarefa.

Quando definida, ela especifica o nome do tipo de tarefa que representa a próxima etapa do fluxo de trabalho quando a ação abrangente é executada.

Exemplo: Quando a ação Escalar é invocada no tipo de tarefa ReviewNoApprove, uma nova tarefa FinalReview é criada como a próxima etapa do fluxo de trabalho.

Omitir essa marca implica que a ação encerrará o processo do fluxo de trabalho depois de ser executada.

Exemplo: A ação da tarefa de cancelamento, presente em cada tipo de tarefa, encerrará o fluxo de trabalho.

Personalização do Tipo de Tarefa

Tipos de tarefa são altamente personalizáveis.

Novos tipos de tarefa podem ser criados desde que as regras anteriormente descritas sejam seguidas.

Fluxos existentes podem ser modificados por meio da alteração dos valores nas marcas de tarefa de destino para um determinado tipo de tarefa. O trecho de código a seguir é um exemplo de um processo de aprovação de duas etapas e de um processo de aprovação de uma única etapa.

```
<taskType creationType="NONE" dataUpdateType="ACTIVE"
  defaultApproval="false" displayName="Final Review"
  displayType="NORMAL" name="FinalReview" pendingBVT="true">
  <description>Review a change and approve, reject or escalate it.</
description>
  <action name="Approve"/>
  <action name="Reject">
    <targetTask>UpdateRejectedRecord</targetTask>
  </action>
  <action name="Escalate">
    <targetTask>FinalReview</targetTask>
  </action>
  <action name="Reassign">
    <targetTask>FinalReview</targetTask>
  </action>
  <action name="CancelTask"/>
</taskType>
```

Tipos de Ação

Essa seção do arquivo de configuração do IDD especifica os tipos de ações que estão disponíveis para uso por cada tarefa em um aplicativo do IDD.

Cada Tipo de Tarefa define um conjunto de ações possíveis que podem ser realizadas no contexto da tarefa. Como vários tipos de tarefa podem ter as mesmas ações ou ações semelhantes disponíveis, esses tipos são definidos fora do contexto de uma tarefa e são referenciados na definição de tipo de tarefa, conforme descrito anteriormente.

Quando você edita uma tarefa no Gerenciador de Configuração IDD, janela **Configuração de Tarefas**, é possível configurar os tipos de ação e a próxima etapa de cada tarefa. Ao trabalhar com uma tarefa no aplicativo do IDD, somente os tipos de ação selecionados serão exibidos como um botão para o usuário, e o tipo de tarefa selecionado na seção **Próxima Etapa** executará a próxima etapa do fluxo de trabalho para esse tipo de ação específico.

Nota: Para um tipo de ação selecionado, se o valor na seção **Próxima Etapa** for **<Empty>**, a ação encerrará o processo do fluxo de trabalho depois de ser executada.

A seguinte tabela fornece a lista de tipos de ação e suas descrições:

Tipos de Ação	Descrição
SubmitForApproval	Enviar uma alteração para aprovação.
Augment	Reatribuir a tarefa a outro usuário para assistência.
CompleteUpdate	Confirmar as alterações feitas em um registro de área de assunto.
Approve	Aprovar e confirmar as alterações feitas em um registro de área de assunto.
Reject	Rejeitar as alterações e reatribuir ao usuário que as efetuou.
Escalate	Reatribuir a tarefa a outro revisor para assistência. Isso pode fazer com que uma nova tarefa seja criada.
Reassign	Reatribuir a tarefa a outro usuário/função.
Desfazer Mesclagem	Executar a operação de desfazer mesclagem definida pela tarefa.
CancelTask	Cancelar a tarefa por meio da sua exclusão.

Tipos de Ação - XML de Amostra

O trecho a seguir de um arquivo de configuração do IDD pertence a tipos de tarefa e será referenciado mais adiante nesta subseção.

```
<!-- Action Definitions - MUST come before the task types definitions. -->
  <actionType name="SubmitForApproval" displayName="Submit For Approval">
    <description>Submit a change for approval.</description>
    <class>com.siperian.dsapp.domain.task.action.SubmitForApproval</class>
  </actionType>
  <actionType name="Augment" displayName="Augment" manualReassign="true">
    <description>Reassign the task to another user for assistance.</description>
```

```

        <class>com.siperian.dsapp.domain.task.action.Reassign</class>
    </actionType>
    <actionType name="CompleteUpdate" displayName="Complete Update">
        <description>Commit changes made to a subject area record.</description>
        <class>com.siperian.dsapp.domain.task.action.CompleteUpdate</class>
    </actionType>
    <actionType name="Approve" displayName="Approve">
        <description>Approve and commit changes made to a subject area record.</
description>
        <class>com.siperian.dsapp.domain.task.action.Approve</class>
    </actionType>
    <actionType name="Reject" displayName="Reject">
        <description>Reject changes and reassign to the user
            who made the changes.</description>
        <class>com.siperian.dsapp.domain.task.action.Reject</class>
    </actionType>
    <actionType name="Escalate" displayName="Escalate">
        <description>Reassign the task to another reviewer for assistance.
            This could result in a new task being created.</description>
        <class>com.siperian.dsapp.domain.task.action.Reassign</class>
    </actionType>
    <actionType name="Reassign" displayName="Reassign" manualReassign="true">
        <description>Reassign the task to another user/role.</description>
        <class>com.siperian.dsapp.domain.task.action.Reassign</class>
    </actionType>
    <actionType name="Unmerge" displayName="Unmerge">
        <description>Perform the unmerge operation defined by the task.</description>
        <class>com.siperian.dsapp.domain.task.action.Unmerge</class>
    </actionType>
    <actionType name="CancelTask" displayName="Cancel Task" cancelTask="true">
        <description>Cancel the task by deleting it.</description>
        <class>com.siperian.dsapp.domain.task.action.CancelTask</class>
    </actionType>

```

Atributos e Marcas ActionType

nome

O atributo name de um tipo de ação nunca deve ser alterado.

Ele é para uso interno por um aplicativo do IDD e pelo Informatica MDM Hub e, portanto, não é necessário alterar essas configurações. Se um novo tipo de ação for introduzido, qualquer nome poderá ser especificado, pois ele não será significativo.

displayName

Esse é o nome da ação exibido em um aplicativo do IDD.

Porém, o nome real mostrado em um aplicativo do IDD é obtido de um pacote de recursos e, portanto, alterações nesse valor podem não resultar em alterações visíveis correspondentes no aplicativo do IDD.

Marca de Descrição

Esse elemento fornece uma rápida descrição da finalidade do tipo de ação.

manualReassign

Quando esse atributo está definido como "true", o usuário de aplicativo do IDD é solicitado a selecionar um usuário específico para atribuição da tarefa antes que a ação seja executada.

Isso é usado, por exemplo, ao reatribuir uma tarefa manualmente a outro usuário. Se definido como "false", a atribuição de tarefa para esse tipo de ação será automática.

closeTaskView

Quando esse atributo está definido como "true", a guia na qual o usuário de aplicativo do IDD estava trabalhando durante a realização dessa ação será fechada, e o usuário voltará para a página do Iniciar espaço de trabalho.

O trecho de código a seguir é um exemplo de um tipo de ação.

```
<actionType cancelTask="true" closeTaskView="true"
  displayName="Cancel Task" manualReassign="false" name="CancelTask">
  <description>Cancel the task by deleting it.</description>
  <class>com.siperian.dsapp.domain.task.action.CancelTask</class>
</actionType>
```

Nota: Você pode configurar esse atributo para cada tipo de ação usando o arquivo de configuração do IDD (IDDConfig.xml). O valor padrão desse atributo é "true".

cancelTask

Quando esse atributo é definido como "true", a tarefa é cancelada quando a ação é executada.

Consequentemente, a tarefa é completamente excluída e não pode ser recuperada e quaisquer alterações pendentes associadas a ela serão permanentemente excluídas.

Marca de Classe

Esse atributo NÃO deve ser modificado nesta versão, pois especifica a classe Java que é usada para executar a ação.

Não é possível adicionar manipuladores de ação personalizados nesta versão, mas essa funcionalidade está planejada para uma versão futura.

Configuração da Segurança de Tarefas

Quando uma instância de aplicativo do IDD é implantado, ou quando o servidor de aplicativos é reiniciado, o aplicativo do IDD sincroniza um conjunto de recursos personalizados com o Informatica MDM Hub.

Esse conjunto de recursos personalizados inclui um recurso personalizado para cada área de assunto e cada tipo de tarefa por área de assunto (conforme definido no arquivo de configuração do IDD).

Use a ferramenta Funções no Console do Hub para configurar a segurança de tarefas por meio da especificação de privilégios sobre os recursos personalizados de tipos de tarefa.

Os seguintes privilégios para tipos de tarefa são aplicados em um aplicativo do IDD:

Privilégio	Descrição
Leitura	Não usado.
Criar	Esse privilégio é necessário para um usuário de aplicativo do IDD criar novas tarefas. Quando o usuário escolhe o comando Criar Tarefa na exibição de dados, o aplicativo do IDD exibe uma caixa de diálogo contendo uma lista dos possíveis tipos de tarefa a serem criados. Essa lista contém apenas os tipos de tarefa para os quais o usuário tem o privilégio Criar. Além disso, as tarefas exibidas nessa lista também devem ser configuradas corretamente no arquivo de configuração do IDD, por meio da definição do atributo creationType como "create".
Atualizar	Não usado.
Excluir	Não usado.
Mesclar	Não usado.
Executar	Esse privilégio é necessário para um usuário de aplicativo do IDD exibir detalhes sobre uma tarefa e fazer modificações nos detalhes dessa tarefa (o que inclui adicionar comentários, modificar a data de vencimento e até mesmo reatribuir a tarefa). Usuários de aplicativo do IDD que possuem privilégios Executar em um tipo de tarefa estão autorizados a executar todas as ações referentes a esse tipo de tarefa. Isso é válido independentemente do resultado da ação quando ela é executada. Por exemplo, se houver uma ação que cria uma nova tarefa, o usuário poderá executar essa ação mesmo não tendo privilégios Criar sobre o tipo de tarefa que é criado pela ação.

Importante: Os privilégios para tarefas, áreas de assunto e objetos base operam todos juntos no SAM. Uma configuração incorreta do SAM pode resultar em um comportamento inesperado em um aplicativo do IDD. A atribuição de tarefa (descrita a seguir e gerenciada no Gerenciador de Configuração IDD) é feita pelo usuário ou função. O IDD não verifica se a função ou o usuário tem a configuração de segurança para permitir operações nessa tarefa. Cabe ao implementador do aplicativo do IDD configurar isso corretamente. Além disso, para que um usuário de aplicativo do IDD possa cancelar uma tarefa, ele deve ter o privilégio DELETE na XREF para cada objeto base em uma área de assunto.

Atribuição de Tarefas

Configuração de Atribuição de Tarefas

Cada Área de Assunto do aplicativo do IDD pode ser configurada para usar um conjunto específico de tipos de tarefa.

Por sua vez, cada tipo de tarefa pode estar vinculado a uma ou mais funções de segurança ou a um único nome de usuário. Isso significa que a tarefa de um determinado Tipo de Tarefa pode ser atribuída somente aos usuários com as funções de segurança especificadas ou ao usuário que está especificado na definição de Atribuição de Tarefas.

No arquivo de configuração XML, a atribuição de tarefas pode ser definida com o uso da marca `taskAssignmentConfig`.

Exemplo:

```
<taskAssignmentConfig task="UpdateWithApproval">
    <securityRole roleUid="DataSteward"/>
</taskAssignmentConfig>
<taskAssignmentConfig task="UpdateWithOptionalApproval" >
    <securityRole roleUid="DataSteward"/>
    <securityRole roleUid="Customer-NY"/>
</taskAssignmentConfig>
<taskAssignmentConfig task="UpdateRejectedRecord" user="user1"/>
<taskAssignmentConfig task="ReviewNoApprove">
    <securityRole roleUid="Manager"/>
</taskAssignmentConfig>
<taskAssignmentConfig task="FinalReview" >
    <securityRole roleUid="SrManager"/>
</taskAssignmentConfig>
<taskAssignmentConfig task="Merge">
    <securityRole roleUid="DataSteward"/>
</taskAssignmentConfig>
<taskAssignmentConfig task="Unmerge">
    <securityRole roleUid="DataSteward"/>
</taskAssignmentConfig>
```

No exemplo anterior, as tarefas `UpdateWithOptionalApproval` podem ser atribuídas a usuários com uma função de Administrador de Dados ou Cliente-NY. Tarefas do tipo `UpdateRejectedRecord` podem ser atribuídas somente a um usuário (`user1`).

O elemento de atribuição de tarefas deve conter a tarefa `attribute` necessária, com o nome de um dos tipos de tarefa definido na configuração do IDD. Além disso, ele deve conter uma ou mais funções de segurança do elemento filho ou um atributo de usuário com o nome de um usuário ao qual a tarefa desse tipo específico pode ser atribuída.

Interface do Usuário de Configuração de Atribuição de Tarefas

É possível especificar a atribuição de tarefas usando a guia Atribuição de Tarefas na caixa de diálogo Área de Assunto do IDD.

Quando você clica na guia **Atribuição de Tarefas**, os tipos de tarefas que podem ser usados com a Área de Assunto são exibidos. É possível selecionar um tipo de tarefa e clicar em **Adicionar** para adicioná-lo à Área de Assunto.

Se todos os tipos de tarefa definidos na instância do aplicativo do IDD já estiverem adicionados à Área de Assunto, o botão Adicionar ficará desativado.

Você pode modificar um Tipo de tarefa selecionado usando o botão **Editar**. O botão **Excluir** permite que você remova um tipo de tarefa da Área de Assunto.

Você deve selecionar a opção **Atribuir à Função** para modificar ou adicionar funções. As funções de segurança definidas no MDM Hub (usando o MDM Hub) podem ser movidas para a lista Funções Selecionadas e vinculadas ao Tipo de Tarefa de uma Área de Assunto.

Atribuição Automática de Tarefas

A atribuição automática de tarefas é controlada por meio de um daemon de servidor que é executado como parte do Informatica MDM Hub.

A frequência com a qual esse daemon é executado é controlada pelo valor da propriedade `sip.task.assignment.interval` em `cmxserver.properties`. Por padrão, esse valor está definido como 0, o que significa que o daemon está desativado. Ele apenas deverá ser ativado se você estiver executando aplicativos do IDD e exigir a atribuição de tarefas. Para ativar o daemon, defina `sip.task.assignment.interval` como um valor em minutos. Um valor de 1 fará com que o daemon seja executado uma vez por minuto. Esse daemon tem dois trabalhos:

Ele atribuirá qualquer tarefa que não tenha um proprietário (rowid_user nulo), conforme definido na configuração da atribuição de tarefas do aplicativo do IDD.

Ele examinará todas as entradas da tabela de correspondências associadas à tabela primária de uma área de assunto configurada e criará tarefas a serem atribuídas a usuários de aplicativo do IDD disponíveis.

Um *usuário disponível* (a) tem menos do que o número máximo configurado de tarefas atualmente atribuídas a ele e (b) recebe a função especificada na configuração de atribuição de tarefas. É possível configurar o número máximo de tarefas que podem ser atribuídas automaticamente a um usuário de aplicativo do IDD especificando a propriedade sip.task.maximum.assignment no arquivo cmxserver.properties. O número máximo de tarefas a serem atribuídas por usuário é 25.

Quando tarefas são automaticamente atribuídas, usuários de aplicativo do IDD na função configurada são selecionados para a atribuição de tarefas de maneira circular, até que não haja mais usuários com um número de tarefas atribuídas menor que o máximo permitido. Sempre que o daemon de atribuição for executado, ele atribuirá todas as tarefas não atribuídas que puder. Se não houver usuários suficientes para receber todas as tarefas não atribuídas, talvez haja tarefas não atribuídas restantes após a execução do daemon (essas tarefas serão atribuídas assim que houver espaço disponível na fila de tarefas de um usuário de aplicativo do IDD de destino). Quando a atribuição de tarefas automática está ocorrendo, o usuário de aplicativo do IDD que recebe uma tarefa específica não pode ser previsto com precisão. Se uma tarefa precisa ser atribuída a um usuário específico, convém usar a atribuição manual.

Personalizando a Atribuição Automática de Tarefas

A atribuição automática de tarefas pode ser personalizada por meio da saída de usuário AssignTasks.

A saída de usuário AssignTasks funciona com o adaptador de fluxo de trabalho do Siperian BPM.

Atribuição Manual de Tarefas

A atribuição de tarefas manual é controlada pelo usuário de aplicativo do IDD no aplicativo do IDD.

Ao criarem tarefas, os usuários têm a opção de selecionar um usuário de destino para elas. Se especificado, o usuário selecionado se tornará o proprietário da tarefa recém-criada. Se deixado em branco, o daemon de atribuição automática designará a tarefa ao próximo usuário disponível.

Personalizando a Atribuição de Tarefas

A atribuição manual de tarefas pode ser personalizada por meio da saída de usuário GetAssignableUsersForTasks.

A saída de usuário GetAssignableUsersForTasks funciona com o adaptador de fluxo de trabalho do Siperian BPM.

Alterando Tarefas Atribuídas

Aplicativos do IDD podem administrar atribuições de tarefas na guia de administração de tarefas.

Se uma tarefa estiver atribuída a um usuário que não se encontra no escritório, um administrador poderá usar o aplicativo do IDD para atribuir essa tarefa a outro usuário.

Se um usuário for estar indisponível por um determinado período de tempo, você poderá evitar a atribuição de tarefas automática a esse usuário removendo-o da sua função.

Notificação de Tarefas

A notificação de tarefas é simples e direta.

Em um intervalo configurado, um e-mail resumido pode ser enviado a usuários que possuem tarefas. O daemon é executado como parte do Informatica MDM Hub. O intervalo no qual as notificações são enviadas pode ser configurado como um número especificado de horas no arquivo `cmxserver.properties` com a propriedade `sip.task.digest.interval`. O intervalo de notificação padrão é 0 horas, significando que resumos estão desativados. Para ativar resumos, altere isso para um valor em horas.

Veja a seguir um resumo de e-mail de amostra:

```
De: siperian_task_notification@siperian.com Para: null Assunto: Resumo de Tarefas do
Administrador de Dados para admin Mime-Version: 1.0 Content-Type: text/plain; charset=us-
ascii Content-Transfer-Encoding: 7bit Tarefas concluídas desde a última notificação: 0
Tarefas Totais Atribuídas: 17 Esta mensagem foi enviada pelo Daemon de Notificação de
Tarefa do Servidor de Hub Siperian.
```

Nota: Não é possível personalizar o corpo do resumo de e-mail.

Configurando o E-mail de Notificação de Tarefa

Para configurar o e-mail de notificação de tarefa, edite as propriedades no arquivo `cmxserver.properties`. É necessário configurar uma localização de servidor SMTP de saída.

A seguinte lista descreve as propriedades de e-mail de notificação de tarefa que você pode configurar no arquivo `cmxserver.properties`:

mail.smtp.sender

O endereço de e-mail do remetente. O padrão é `siperian_task_notification@siperian.com`.

mail.smtp.host

O nome do host do servidor de e-mail.

mail.smtp.port

O número da porta do servidor de e-mail.

mail.smtp.auth

Determina se o servidor de e-mail especificado requer autenticação para mensagens de saída. Será necessário definir `mail.smtp.auth` como "true" se você estiver usando o servidor de e-mail do Informatica MDM Hub.

mail.smtp.user

O nome de usuário do servidor de e-mail de saída. Será necessário especificar um valor para `mail.smtp.user` se `mail.smtp.auth` for "true".

mail.smtp.password

A senha para o `mail.smtp.user` especificado. Será necessário especificar um valor para `mail.smtp.password` se `mail.smtp.auth` for "true".

Configuração do Gerenciador de Usuários no Console do Hub

Além disso, para que os usuários de aplicativo do IDD possam receber e-mails, a conta de e-mail de entrada deve estar definida no Informatica MDM Hub.

Na ferramenta Usuários do Console do Hub, especifique o endereço de e-mail ao qual as notificações para o usuário do IDD devem ser enviadas. Um e-mail apenas será enviado se houver tarefas atribuídas a um usuário de aplicativo do IDD.

Relatórios e métricas de gerenciamento de tarefas

Métricas de gerenciamento de tarefas mostram a distribuição de tarefas do Data Director.

Os administradores podem usar métricas de gerenciamento de tarefas para mostrar a distribuição de tarefas do Informatica Data Director. Você pode gerar relatórios com base nas seguintes métricas de gerenciamento de tarefas:

Área de assunto da tarefa por data de criação

Os usuários podem exibir tendências de data de criação para uma área de assunto. Use `task_sa_by_create_date` como nome do relatório para configurar e preencher o datamart desse relatório.

Área de assunto da tarefa por data de vencimento

Os usuários podem exibir relatórios com base no número de registros com faixas de datas de vencimento que o administrador especifica quando o relatório é configurado. Use `task_sa_by_due_date` como nome do relatório para configurar e preencher o datamart desse relatório.

Área de assunto da tarefa por prioridade

Os usuários podem exibir relatórios com base no número de registros com prioridades como "Baixa", "Média" e "Alta". Use `task_sa_by_priority` como nome do relatório para configurar e preencher o datamart desse relatório.

Área de assunto da tarefa por status

Os usuários podem exibir relatórios com base no número de registros com status de data de vencimento, como "No Prazo" e "Vencido". Use `task_sa_by_status` como nome do relatório para configurar e preencher o datamart desse relatório.

Área de assunto da tarefa por tipo de tarefa

Os usuários podem exibir relatórios com base no número de registros com tipos de tarefa como "Atualizar com Aprovação", "Mesclar" e "Desfazer Mesclagem". Use `task_sa_by_task_type` como nome do relatório para configurar e preencher o datamart desse relatório.

Tarefa por área de assunto

Os usuários podem exibir relatórios com base no número de registros com áreas de assunto como "Pessoa", "Organização" e "Produto". Use `task_by_subject_area` como nome do relatório para configurar e preencher o datamart desse relatório.

Destinatário da tarefa por prioridade

Os usuários podem exibir relatórios com base no número de registros para um destinatário que possuem prioridades como "Baixa", "Média" e "Alta". Use `task_assignee_by_priority` como nome do relatório para configurar e preencher o datamart desse relatório.

Destinatário da tarefa por status

Os usuários podem exibir relatórios com base no número de registros para um destinatário que possuem prioridades status de data de vencimento, como "No Prazo" e "Vencido". Use `task_assignee_by_status` como nome do relatório para configurar e preencher o datamart desse relatório.

Segurança de Dados em Dados de Tarefas

O IDD permite que os usuários autorizados participem de fluxos de trabalho, que são modelos de computador de trabalhos reais envolvendo uma série de operações ou atividades. A segurança de dados do IDD afeta as seguintes áreas de tarefas:

- Verificação de permissões de exibição - se uma tarefa pode ou não ser aberta por um usuário. Se o usuário não tiver permissão para abrir uma tarefa, uma mensagem de aviso será exibida para ele.
- Filtragem de dados filho - quais registros filho são vistos pelo usuário na Exibição de Dados.

Nota:

- Filtros de segurança de dados não são aplicados a dados de XREF. Por exemplo, se um usuário tiver acesso a dados de objeto primário e seus dados filho, de acordo com a segurança de dados, ele poderá ver todas as XREFs contribuintes.
- A lógica de aplicar filtros de segurança de dados depende do tipo de tarefa.

Tarefa de Revisão

A principal diferença entre abrir os objetos primários regulares e revisar as tarefas na exibição de dados é que os filtros de segurança não são aplicados a um estado ativo do objeto primário e seus filhos. A segurança de dados é aplicada depois que a função BVT de visualização foi executada para os registros pendentes gerais associados à tarefa.

Abrir Tarefas de Revisão com uma Única Função

Um usuário com uma única função apenas poderá abrir uma tarefa se as seguintes condições forem atendidas:

- Todos os registros pendentes associados à tarefa devem corresponder aos filtros de segurança de dados.
- Se houver vários filtros em uma única coluna para uma única função, o usuário terá acesso a uma união de todos os dados que corresponderem a cada filtro.
- Se houver filtros em várias colunas para uma única função, o usuário terá acesso à interseção de todos os dados que corresponderem a cada filtro.
- Se houver filtros de segurança configurados por meio de registros filho ou neto, uma das seguintes condições deverá ser verdadeira:
 - O objeto primário deve ter pelo menos um registro aprovado nas restrições de segurança em cada guia filho com a segurança de dados ativada.
 - Deve haver um registro pendente associado à tarefa, pertencente à guia filho, com a segurança de dados ativada e correspondente às configurações de segurança de dados de acordo com a condição precedente.

Por exemplo, considere um modelo de segurança de dados no qual o usuário tenha a função SalesManager-NY e os seguintes filtros de segurança configurados:

- Filtro 1: O código de estado é NY.
- Filtro 2: O tipo de telefone é Comercial e Residencial.
- Filtro 3: O código de saudação pessoal é MR.

Usando o modelo de segurança de dados mencionado acima, considere um cenário no qual o banco de dados tem um registro de objeto primário, Mr. Florian Amadeu, com endereço de Cobrança no estado de NY

e o tipo de telefone Fax. Um usuário sem restrições de segurança de dados adiciona um novo telefone Comercial e cria a tarefa **Enviar para Aprovação**. Um usuário com a função Gerente de Vendas - NY poderá abrir o registro Mr. Florian Amadeu na exibição de dados, pois ele corresponde a todas as três condições acima e porque o próprio OP corresponde à Segurança de Dados (Filtro 3) e tem pelo menos um registro em cada filho em que a Segurança de Dados está ativada: endereço em NY (registro ativo) e telefone BUSINESS (registro pendente).

Usando o mesmo modelo de segurança de dados mencionado acima, considere um cenário no qual o banco de dados tem um registro de objeto primário, Mr. Dominic Wilkins, com Endereço de Cobrança no Estado de NY e sem um tipo de telefone. Um usuário sem restrições de segurança de dados adiciona um novo telefone Comercial e cria a tarefa **Enviar para Aprovação**. Um usuário com a função Gerente de Vendas - NY não poderá abrir a tarefa, pois o usuário não tem um telefone que corresponda ao Filtro 2.

Abrir Tarefas de Revisão com Várias Funções

Um usuário com várias funções apenas poderá abrir a tarefa se as condições a seguir forem atendidas.

- Todos os registros pendentes associados à tarefa devem corresponder aos filtros de segurança de dados para pelo menos uma função de usuário.
- Um usuário com várias funções pode ter combinações de filtros aplicadas. O resultado é que o usuário tem acesso a todos os dados disponíveis em cada função atribuída por meio de uma união das atribuições de filtros.
- Se filtros de segurança estiverem configurados por meio de filhos ou netos, uma das seguintes condições deverá ser verdadeira.
 - O objeto primário deve ter pelo menos um registro aprovado nas restrições de segurança em cada guia filho com a segurança de dados ativada.
 - O registro pendente associado à tarefa tem uma guia filho com a segurança de dados ativada e que corresponde às configurações de segurança de dados, conforme mencionada na condição precedente.

Por exemplo, considere um modelo de segurança de dados no qual o usuário tenha a função Gerente de Vendas - NY, os filtros de segurança de dados mencionados na seção [“Abrir Tarefas de Revisão com uma Única Função” na página 156](#) e também a função CarSalesManager-NJ, que possui os seguintes filtros de segurança configurados.

- Filtro 1: O código de estado é NJ.
- Filtro 2: O ano do Carro é 2009.

Além disso, o usuário tem outra função, CarSalesManager-CA, que tem o seguinte filtro de segurança configurado.

- Filtro 1: O código de Estado do Endereço é CA.
- Filtro 2: O ano do carro é 2008.

Usando o modelo de segurança de dados mencionado acima, considere um cenário no qual o banco de dados tem um registro de objeto primário, Mr. Derrick Rose, com endereço de Cobrança no estado de CA e o tipo de telefone Residencial. Um usuário sem restrições de segurança de dados adiciona um novo endereço de cobrança no Estado NY e cria a tarefa **Enviar para Aprovação**. Um usuário com a função Gerente de Vendas - NY será capaz de abrir o registro Mr. Derrick Rose na exibição de dados porque ele corresponde aos filtros de segurança da função SalesManager-NY.

Usando o mesmo modelo de segurança de dados mencionado acima, considere um cenário no qual o banco de dados tem um registro de objeto primário, Mr. Tyros Thomas, com Endereço de Cobrança no Estado de CA e com um carro produzido em 2008. Um usuário sem restrições de segurança de dados alterou o endereço de cobrança para NJ e criou a tarefa **Enviar para Aprovação**. Um usuário com ambas as funções, CarSalesManager-CA e CarSalesManager-NJ, não pode abrir a tarefa, pois Mr. Tyros Thomas não

corresponde aos filtros para CarSalesManager-CA e CarSalesManager-NJ, com um registro pendente para o novo endereço.

Filtrar Registro Filho na Exibição de Tarefas

O IDD aplica filtros de segurança ao recuperar dados para guias filho na exibição de dados. Por exemplo, considere um modelo de segurança de dados no qual o usuário tenha a função SalesManager-CA e o filtro de segurança de código de estado de endereço de cobrança – CA.

Usando o modelo de segurança de dados mencionado acima, considere um cenário no qual o banco de dados tem um registro de objeto primário, Mr. Blake Griffin, com dois endereços de cobrança nas cidades de Nova York e Bloomfield Hills, ambas no Estado de NY. Um usuário sem restrições de segurança de dados altera o valor do estado de Bloomfield Hills para CA e cria um endereço de cobrança adicional em LA (Estado de CA), criando em seguida a tarefa **Enviar para Aprovação**. Um usuário com a função Gerenciador de Vendas - NY poderá abrir o registro Mr. Blake Griffin na exibição de dados e ver dois endereços de CA na guia **Endereço de Cobrança**. Um deles é o endereço antigo de NY que foi alterado, e o segundo é o novo endereço que foi adicionado. O endereço de NY que não mudou é removido quando os filtros de segurança são aplicados à BVT de visualização.

Abrir Tarefas de Mesclagem/Desfazer Mesclagem

O IDD aplica as seguintes regras para determinar se a tarefa Mesclar ou Desfazer Mesclagem pode ser aberta pelo usuário.

- A tarefa Mesclar apenas poderá ser aberta se todos os Objetos Primários a serem mesclados corresponderem às configurações de segurança de dados.
- A tarefa Desfazer Mesclagem poderá ser aberta se o Objeto Primário puder ser aberto de acordo com as configurações de Segurança de Dados.

Por exemplo, considere um modelo de segurança de dados no qual o usuário tenha a função SalesManager-CA e o filtro de segurança de código de estado de endereço de cobrança – CA.

Usando o modelo de segurança de dados mencionado acima, considere um cenário no qual há duas pessoas no banco de dados com o mesmo nome, Kevin Durant. Um dos indivíduos tem um endereço de cobrança em LA (Estado de CA), enquanto o outro tem um endereço de cobrança em Nova York (Estado de NY). Um usuário sem restrições de segurança de dados cria a tarefa **Mesclar** para dois registros de pessoa. Usuários com a função SalesManager- CA não poderão abrir a tarefa, pois eles não têm a permissão necessária para abrir um registro de pessoa com endereço de cobrança no Estado de NY e, portanto, não poderão executar uma tarefa **Mesclar** inteira.

Atribuição de Tarefas com Reconhecimento de Dados

Ao atribuir uma tarefa na caixa de diálogo **Atribuir Tarefa**, o IDD remove revisores de tarefas sem privilégios para abrir essa tarefa. Além disso, para a atribuição de tarefas automática, um daemon atribui a tarefa apenas aos usuários com o devido privilégio para abri-la.

APÊNDICE H

Códigos de Localidade

Este apêndice inclui os seguintes tópicos:

- [Códigos de Idioma, 159](#)
- [Códigos de país A-L, 164](#)
- [Códigos de PaísM-Z, 169](#)

Códigos de Idioma

Código ISO	Idioma
aa	Afar
ab	Abkhazo
af	Africâner
am	Amárico
ar	Árabe
as	Assamês
ay	Aymara
az	Azerbaijano
ba	Bashkir
be	Bielorrusso
bg	Búlgaro
bh	Bihari
bi	Bislama
bn	Bengalês, Bangla

Código ISO	Idioma
bo	Tibetano
br	Bretão
ca	Catalão
co	Corso
cs	Tcheco
cy	Galês
da	Dinamarquês
de	Alemão
dz	Bhutani
el	Grego
ptb	Inglês
eo	Esperanto
Es	Espanhol
et	Estoniano
eu	Basco
fa	Persa
fi	Finlandês
fj	Fiji
fo	Faroês
fr	Francês
fy	Frísio
ga	Irlandês
gd	Gaélico Escocês
gl	Galego
gn	Guarani
gu	Gujarati
ha	Hausa

Código ISO	Idioma
he	Hebraico (anteriormente iw)
hi	Hindi
hr	Croata
hu	Húngaro
hy	Armênio
ia	Interlingua
id	Indonésio (anteriormente em)
ie	Interlingue
ik	Inupiak
is	Islandês
it	Italiano
iu	Inuktitut
ja	Japonês
jw	Javanês
ka	Georgiano
kk	Cazaque
kl	Groenlandês
km	Cambojano
kn	Kannada
ko	Coreano
ks	Kashmiri
ku	Curdo
ky	Quirguiz
la	Latino
ln	Lingala
lo	Laotiano
lt	Lituano

Código ISO	Idioma
lv	Letão, Lettish
mg	Malgaxe
mi	Maori
mk	Macedônio
ml	Malaiala
mn	Mongol
mo	Moldavo
mr	Marathi
ms	Malaio
mt	Maltês
my	Birmanês
na	Nauru
ne	Nepali
nl	Holandês
no	Norueguês
oc	Occitânico
om	(Afan) Oromo
ou	Oriá
pa	Punjabi
pl	Polonês
ps	Pashto, Pushto
pt	Português
qu	Quechua
rm	Reto-romance
rn	Kirundi
ro	Romeno
ru	Russo

Código ISO	Idioma
rw	Kinyarwanda
sa	Sânscrito
sd	Sindhi
sg	Sangho
sh	Servo-croata
si	Cingalês
sk	Eslovaco
sl	Esloveno
sm	Samoano
sn	Shona
so	Somali
sq	Albanês
sr	Sérvio
ss	Siswati
st	Sesotho
su	Sudanês
sv	Sueco
sw	Suaíle
ta	Tâmil
te	Telugu
tg	Tadjique
th	Tailandês
ti	Tigrínia
tk	Turcomeno
tl	Tagalog
tn	Setswana
para	Tonga

Código ISO	Idioma
tr	Turco
ts	Tsonga
tt	Tatar
tw	Twi
ug	Uigur
uk	Ucraniano
ur	Urdu
uz	Uzbeque
vi	Vietnamita
vo	Volapuque
wo	Uólofe
xh	Xhosa
yi	Lídiche (anteriormente ji)
yo	Yoruba
za	Zhuang
zh	Chinês
zu	Zulu

TÓPICOS RELACIONADOS:

- [“Tabelas de Pesquisa com Coluna de Subtipo” na página 62](#)

Códigos de país A-L

País	Código de Duas Letras	ISO #
ILHAS AALAND	AX	248
AFEGANISTÃO	AF	4
ALBÂNIA	AL	8

País	Código de Duas Letras	ISO #
ARGÉLIA	DZ	12
SAMOA AMERICANA	AS	16
ANDORRA	AD	20
ANGOLA	AO	24
ANGUILLA	AI	660
ANTÁRTICA	AQ	10
ANTÍGUA E BARBUDA	AG	28
ARGENTINA	AR	32
ARMÊNIA	AM	51
ARUBA	AW	533
AUSTRÁLIA	AU	36
ÁUSTRIA	AT	40
AZERBAIJÃO	AZ	31
BAHAMAS	BS	44
BAHRAIN	BH	48
BANGLADESH	BD	50
BARBADOS	BB	52
BIELORRÚSSIA	BY	112
BÉLGICA	BE	56
BELIZE	BZ	84
BENIN	BJ	204
BERMUDA	BM	60
BUTÃO	BT	64
BOLÍVIA	BO	68
BÓSNIA E HERZEGÓVINA	BA	70
BOTSUANA	BW	72
ILHA BOUVET	BV	74

País	Código de Duas Letras	ISO #
BRASIL	BR	76
TERRITÓRIO BRITÂNICO DO OCEANO ÍNDICO	IO	86
BRUNEI DARUSSALAM	BN	96
BULGÁRIA	BG	100
BURKINA FASO	BF	854
BURUNDI	BI	108
CAMBOJA	KH	116
CAMARÕES	CM	120
CANADA	CA	124
CABO VERDE	CV	132
ILHAS CAYMAN	KY	136
REPÚBLICA CENTRO-AFRICANA	CF	140
CHADE	TD	148
CHILE	CL	152
CHINA	CN	156
ILHA CHRISTMAS	CX	162
ILHAS COCOS (KEELING)	CC	166
COLÔMBIA	CO	170
COMORES	KM	174
CONGO, República Democrática do (antigo Zaire)	CD	180
CONGO, República do	CG	178
ILHAS COOK	CK	184
COSTA RICA	CR	188
COSTA DO MARFIM	CI	384
CROÁCIA (nome local: Hrvatska)	HR	191
CUBA	CU	192
CHIPRE	CY	196

País	Código de Duas Letras	ISO #
REPÚBLICA CHECA	CZ	203
DINAMARCA	DK	208
DJIBOUTI	DJ	262
DOMINICA	DM	212
REPÚBLICA DOMINICANA	DO	214
EQUADOR	EC	218
EGYPT	EG	818
EL SALVADOR	SV	222
GUINÉ EQUATORIAL	GQ	226
ERITREIA	ER	232
ESTÔNIA	EE	233
ETIÓPIA	ET	231
ILHAS FALKLAND (MALVINAS)	FK	238
ILHAS FAROE	FO	234
FIJI	FJ	242
FINLÂNDIA	FI	246
FRANÇA	SX	250
GUIANA FRANCESA	GF	254
POLINÉSIA FRANCESA	PF	258
TERRITÓRIOS FRANCESES DO SUL	TF	260
GABÃO	GA	266
GÂMBIA	GM	270
GEÓRGIA	GE	268
ALEMANHA	DE	276
GANÁ	GH	288
GIBRALTAR	GI	292
GRÉCIA	GR	300

País	Código de Duas Letras	ISO #
GROENLÂNDIA	GL	304
GRANADA	GD	308
GUADALUPE	GP	312
GUAM	GU	316
GUATEMALA	GT	320
GUINÉ	GN	324
GUINÉ-BISSAU	GW	624
GUIANA	GY	328
HAITI	HT	332
ILHAS HEARD E MC DONALD	HM	334
HONDURAS	HN	340
HONG KONG	HK	344
HUNGRIA	HU	348
ISLÂNDIA	IS	352
ÍNDIA	IN	356
INDONÉSIA	ID	360
IRÃ (REPÚBLICA ISLÂMICA DO)	IR	364
IRAQUE	IQ	368
IRLANDA	IE	372
ISRAEL	IL	376
ITÁLIA	IT	380
JAMAICA	JM	388
JAPÃO	JP	392
JORDÂNIA	JO	400
CAZAQUISTÃO	KZ	398
QUÊNIA	KE	404
QUIRIBATI	KI	296

País	Código de Duas Letras	ISO #
COREIA, REPÚBLICA POPULAR DEMOCRÁTICA DA	KP	408
COREIA, REPÚBLICA DA	KR	410
KUWAIT	KW	414
QUIRGUISTÃO	KG	417
LAO, REPÚBLICA DEMOCRÁTICA POPULAR	LA	418
LETÔNIA	LV	428
LÍBANO	LB	422
LESOTHO	LS	426
LIBÉRIA	LR	430
JAMAHIRIA ÁRABE DA LÍBIA	LY	434
LIECHTENSTEIN	LI	438
LITUÂNIA	LT	440
LUXEMBURGO	LU	442

Códigos de PaísM-Z

País	Código de Duas Letras	ISO #
MACAU	MO	446
MACEDÔNIA, ANTIGA REPÚBLICA JUGOSLAVA DA	MK	807
MADAGASCAR	MG	450
MALAWI	MW	454
MALÁSIA	MY	458
MALDIVAS	MV	462
MALI	ML	466
MALTA	MT	470
ILHAS MARSHALL	MH	584

País	Código de Duas Letras	ISO #
MARTINICA	MQ	474
MAURITÂNIA	MR	478
MAURÍCIO	MU	480
MAYOTTE	YT	175
MÉXICO	MX	484
MICRONÉSIA, ESTADOS FEDERADOS DA	FM	583
MOLDÁVIA, REPÚBLICA DA	MD	498
MÔNACO	MC	492
MONGÓLIA	MN	496
MONTSERRAT	MS	500
MARROCOS	MA	504
MOÇAMBIQUE	MZ	508
MIANMAR	MM	104
NAMÍBIA	NA	516
NAURU	NR	520
NEPAL	NP	524
HOLANDA	NL	528
ANTILHAS HOLANDESAS	AN	530
NOVA CALEDÔNIA	NC	540
NOVA ZELÂNDIA	NZ	554
NICARÁGUA	NI	558
NÍGER	NE	562
NIGÉRIA	NG	566
NIUE	NU	570
ILHA NORFOLK	NF	574
ILHAS MARIANAS DO NORTE	MP	580
NORUEGA	NÃO	578

País	Código de Duas Letras	ISO #
OMÃ	OM	512
PAQUISTÃO	PK	586
PALAU	PW	585
TERRITÓRIO PALESTINIANO, Ocupado	PS	275
PANAMÁ	PA	591
PAPUA NOVA GUINÉ	PG	598
PARAGUAI	PY	600
PERU	PE	604
FILIPINAS	PH	608
PITCAIRN	PN	612
POLÓNIA	PL	616
PORTUGAL	PT	620
PUERTO RICO	PR	630
CATAR	QA	634
REUNION	RE	638
ROMÉNIA	RO	642
FEDERAÇÃO RUSSA	RU	643
RUANDA	RW	646
SANTA HELENA	SH	654
SÃO CRISTÓVÃO E NEVIS	KN	659
SANTA LÚCIA	LC	662
SAINT PIERRE E MIQUELON	PM	666
SÃO VICENTE E GRANADINAS	VC	670
SAMOA	WS	882
SAN MARINO	SM	674
SÃO TOMÉ E PRÍNCIPE	ST	678
ARÁBIA SAUDITA	SA	682

País	Código de Duas Letras	ISO #
SENEGAL	SN	686
SÉRVIA E MONTENEGRO	CS	891
SEICHELES	SC	690
SERRA LEOA	SL	694
CINGAPURA	SG	702
ESLOVÁQUIA	SK	703
ESLOVÉNIA	SI	705
ILHAS SALOMÃO	SB	90
SOMÁLIA	SO	706
ÁFRICA DO SUL	ZA	710
GEÓRGIA DO SUL E ILHAS SANDWICH DO SUL	GS	239
ESPANHA	ES	724
SRI LANKA	LK	144
SUDÃO	SD	736
SURINAME	SR	740
ILHAS SVALBARD E JAN MAYEN	SJ	744
SUAZILÂNDIA	SZ	748
SUÉCIA	SE	752
SUIÇA	CH	756
REPÚBLICA ÁRABE DA SÍRIA	SY	760
TAIWAN	TW	158
TAJIKISTÃO	TJ	762
TANZÂNIA, REPÚBLICA UNIDA DA	TZ	834
TAILÂNDIA	QI	764
TIMOR-LESTE	TL	626
TOGO	TG	768
TOKELAU	TK	772

País	Código de Duas Letras	ISO #
TONGA	PARA	776
TRINIDAD E TOBAGO	TT	780
TUNÍSIA	TN	788
TURQUIA	TR	792
TURCOMENISTÃO	TM	795
ILHAS TURKS E CAICOS	TC	796
TUVALU	TV	798
UGANDA	UG	800
UCRÂNIA	UA	804
EMIRADOS ÁRABES UNIDOS	AE	784
UNITED KINGDOM	GB	826
ESTADOS UNIDOS	US	840
TERRITÓRIOS INSULARES DOS ESTADOS UNIDOS	UM	581
URUGUAI	UY	858
UZBEQUISTÃO	UZ	860
VANUATU	VU	548
CIDADE DO VATICANO (SANTA SÉ)	VA	336
VENEZUELA	VE	862
VIETNÃ	VN	704
ILHAS VIRGENS (BRITÂNICAS)	VG	92
ILHAS VIRGENS (EUA)	VI	850
ILHAS WALLIS E FUTUNA	WF	876
SAARA OCIDENTAL	EH	732
IÊMEN	YE	887
ZÂMBIA	ZM	894
ZIMBABWE	ZW	716

APÊNDICE I

Solução de problemas

Este apêndice inclui os seguintes tópicos:

- [Visão Geral de Solução de Problemas, 174](#)
- [Verificar a Configuração do SAM, 174](#)
- [Verificar a Configuração da Função de Limpeza, 175](#)
- [Os Metadados do Informatica Data Director Não Foram Atualizados, 175](#)
- [O Informatica Data Director Para de Responder quando Você Troca de Entidades, 175](#)
- [A Configuração do Informatica Data Director não é Válida, 176](#)
- [O Desempenho de Correspondência é Muito Lento, 176](#)

Visão Geral de Solução de Problemas

Este apêndice descreve algumas dicas sobre o que verificar quando você encontrar resultados inesperados na configuração do seu aplicativo do IDD.

Verificar a Configuração do SAM

Verifique se o SAM tem as permissões corretas atribuídas em todos os níveis necessários, de acordo com a documentação.

As áreas a serem verificadas em busca de CRUD incluem:

- Se referências cruzadas e históricos de alterações forem necessários, com botões ativados no aplicativo do IDD, os conteúdos de metadados apropriados (objetos XREF e HIST) será recursos SECURE e também serão configurados de acordo.
- Consultas/Pacotes - Certifique-se de que ps recursos sejam transformados em SECURE. Caso contrário, um aplicativo do IDD talvez não permita acesso à área de assunto inteira.

Verificar a Configuração da Função de Limpeza

Se funções de limpeza estiverem configuradas, certifique-se de que:

- Cada função de limpeza seja um recurso SECURE.
- As funções que precisam de acesso à função de limpeza tenham a permissão Executar.

Os Metadados do Informatica Data Director Não Foram Atualizados

O Informatica Data Director mantém um cache de metadados do MDM Hub que descreve objetos base, colunas, relacionamentos e outros detalhes. Para limpar o cache para o aplicativo IDD selecionado e forçar o IDD a recarregar os metadados, clique em **Limpar Cache** no Gerenciador de Configuração IDD.

Também é possível reiniciar o servidor de aplicativos para limpar o cache.

O Informatica Data Director Para de Responder quando Você Troca de Entidades

O Informatica Data Director para de responder quando você troca de entidades para relacionamentos do Gerenciador de Hierarquia em sistemas de origem que não estão ativados para a substituição do gerenciamento de estado.

O comportamento ocorre para ambientes JBoss em execução no Java 1.7. Para resolver esse problema, você deve configurar o arquivo `standalone-full.xml`.

1. Abra o arquivo `standalone-full.xml` para edição. O arquivo está no seguinte diretório:
 - No UNIX. <diretório de instalação do JBoss>/jboss-eap-6.1/standalone/configuration
 - No Windows. <diretório de instalação do JBoss>\jboss-eap-6.1\standalone\configuration
2. Adicione o seguinte código XML ao arquivo `standalone-full.xml` de forma a configurar a manipulação assíncrona para o agente de log:

```
<async-handler name="ASYNC">
  <level name="INFO"/>
  <queue-length value="1024"/>
  <overflow-action value="BLOCK"/>
  <subhandlers>
    <handler name="FILE"/>
    <handler name="CONSOLE"/>
  </subhandlers>
</async-handler>
```

3. Em <subsystem xmlns="urn:jboss:domain:logging:1.2"> no arquivo `standalone-full.xml`, adicione o seguinte código XML de forma a configurar a manipulação assíncrona para o agente de log raiz:

```
<root-logger>
  <level name="INFO"/>
  <handlers>
    <handler name="ASYNC"/>
```

```
</handlers>
</root-logger>
```

4. Reinicie o servidor de aplicativos.

A Configuração do Informatica Data Director não é Válida

Se você receber um erro informando que a configuração do Informatica Data Director não é válida, valide o arquivo `IDDConfig.xml` com base no esquema `siperian-bdd-config-6.xsd`.

O esquema `siperian-bdd-config-6.xsd` está localizado no kit de recursos, no seguinte diretório:

- No UNIX. <diretório de instalação infamdm>/hub/resourcekit/sdk/bddXsdDoc
- No Windows. <diretório de instalação infamdm>\hub\resourcekit\sdk\bddXsdDoc

O Desempenho de Correspondência é Muito Lento

Os usuários do aplicativo do IDD relatam que o desempenho de correspondência está muito lento.

Ative a propriedade `needLoadChildOnOpen` e reinicie o servidor de aplicativos.

Para ativar essa propriedade, execute as seguintes instruções SQL no banco de dados ORS:

```
insert into C_REPOS_DS_PREF_DETAIL (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE) select
'BDDGP.30', rowid_ds_pref, 'needLoadChildOnOpen', 'true' from C_REPOS_DS_PREF where name =
'__SYSTEM_PREFERENCES_ROOT__';

commit;
```


APÊNDICE J

Glossário

administrador

Usuário de aplicativo do IDD que tem a responsabilidade principal de configurar o aplicativo do IDD.

administrador de dados

Usuário de aplicativo do IDD que tem a responsabilidade principal pela qualidade dos dados.

Aplicativo do IDD

A unidade principal de configuração e implantação para implementação do IDD. Um aplicativo do IDD é o que os usuários comerciais visualizam quando iniciam o IDD e fazem login nele.

Área de assunto

O principal conceito organizacional para um aplicativo do IDD. Uma área de assunto representa uma coleção de dados que devem ser tratados como uma unidade sob uma perspectiva comercial.

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 esquema de banco de dados que armazena as regras para o processamento dos dados principais, as regras para o gerenciamento do conjunto de objetos de dados principais, juntamente com as regras de processamento e a lógica auxiliar usadas pelo Informatica MDM Hub na definição da melhor versão da verdade (BVT).

arquivos auxiliares

Arquivos auxiliares são arquivos temporários e que são criados em diferentes circunstâncias, ao editar ou exportar um projeto.

autenticação

Processo de verificar a identidade de um usuário para garantir que ele seja quem alega ser. No aplicativo do IDD, usuários são autenticados com base em suas credenciais fornecidas — nome de usuário/senha, carga de segurança ou uma combinação de ambos. O aplicativo do IDD fornece um mecanismo de autenticação interno e também dá suporte à autenticação do usuário usando provedores de autenticação de terceiros.

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).

Banco de Dados Principais

Banco de dados que contém as definições de configuração do ambiente do Informatica MDM Hub—contas de usuário, configuração de segurança, registro do ORS, configurações de fila de mensagens e assim por diante. Um determinado ambiente do Informatica MDM Hub pode ter apenas um Banco de Dados Principais. O nome padrão do Banco de Dados Principais é CMX_SYSTEM.

Caminho de Correspondência

Permite percorrer a hierarquia entre os registros—independentemente de essa hierarquia existir entre objetos base (caminhos inter-tabela) ou dentro de um único objeto base (caminhos intra-tabela). Caminhos de correspondência são usados para configurar regras de coluna de correspondências que envolvem registros relacionados em tabelas separadas ou na mesma tabela.

chave de correspondência

Strings codificadas que representam os dados na coluna de chave da correspondência difusa do objeto base. Chaves de correspondência consistem em valores de tamanho fixo, compactados e codificados criados a partir de uma combinação de palavras e números em um nome ou endereço, de forma que variações relevantes tenham o mesmo valor de chave de correspondência. Chaves de correspondência são uma parte dos tokens de correspondência que são gerados durante o processo de tokenização, armazenados na tabela de chaves de correspondência e, em seguida, usados durante o processo de correspondência para identificar candidatos para correspondência.

chave de correspondência difusa

Coluna especial no objeto base que o Gerenciador de Esquemas adicionará se uma coluna de correspondência usar a estratégia de correspondência/pesquisa difusa. Essa coluna é o campo principal usado durante pesquisas e correspondências de forma a gerar candidatos a correspondência para esse objeto base. Todos os objetos base difusos têm uma, e somente uma, Chave de Correspondência Difusa.

chave externa

Em um banco de dados relacional, uma coluna (ou conjunto de colunas) cujo valor corresponde a um valor de chave primária em outra tabela (ou, em casos raros, na mesma tabela). A chave externa atua como um ponteiro para a outra tabela. Por exemplo, a coluna Department_Number na tabela Employee seria uma chave externa que aponta para a chave primária da tabela Department.

coluna de correspondência

Uma coluna usada em uma regra de correspondência para fins de comparação. Cada coluna de correspondência é baseada em uma ou mais colunas do objeto base.

Confiança

Confiança é um mecanismo para medir o fator de segurança associado a cada célula, com base em seu sistema de origem, no histórico de alterações e em outras regras comerciais. A confiança leva em consideração a idade de dados, quanta confiabilidade decaiu ao longo do tempo e a validade dos dados.

conjunto de regras de correspondência

Uma coleção lógica de regras de correspondência que permitem aos usuários executar diferentes conjuntos de regras em diferentes estágios do processo de correspondência. Conjuntos de regras de correspondência incluem um nível de pesquisa que determina a estratégia de pesquisa, qualquer número de regras de correspondência automáticas e manuais e, opcionalmente, um filtro que permite incluir ou excluir registros seletivamente durante o processo de correspondência. Conjuntos de regras de correspondência são usados para executar regras de coluna de correspondência, mas não regras de correspondência da chave primária.

Console do Hub

Interface de usuário do Informatica MDM Hub que compreende um conjunto de ferramentas para 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, configurar o acesso de aplicativos externos a recursos do Informatica MDM Hub e outras tarefas de operação e configuração do sistema.

correspondência

O processo de determinar se dois registros devem ser automaticamente mesclados ou se devem ser candidatos a mesclagem manual por possuírem valores idênticos ou semelhantes nas colunas especificadas.

correspondência difusa

Uma estratégia de correspondência/pesquisa que usa a correspondência probabilística, que leva em conta variações ortográficas, possíveis erros ortográficos e outras diferenças que podem fazer com que registros correspondentes não sejam idênticos.

Dados em andamento

Dados em andamento são dados comerciais que podem passar por diferentes estados (ACTIVE, PENDING ou DELETED) ao progredirem por um fluxo de trabalho.

Dados principais

Uma coleção de entidades comuns principais — juntamente com seus atributos e valores — que são consideradas fundamentais para os negócios de uma empresa e que são necessárias para uso em dois ou mais sistemas ou processos comerciais. Os exemplos de dados principais incluem os dados de cliente, produto, funcionário, fornecedor e localização.

desfazer mesclagem

Processo de desfazer a mesclagem de registros anteriormente mesclados. Apenas para objetos base ao estilo de mesclagem.

duplicar

Um ou mais registros em que os dados em determinadas colunas (como nome, endereço ou dados da organização) são idênticos ou quase idênticos. Regras de correspondência executadas durante o processo de correspondência determinam se dois registros são suficientemente semelhantes para serem considerados duplicatas para fins de consolidação.

entidade

Uma entidade é qualquer objeto, pessoa, local ou coisa que tenha um significado e possa ser trabalhado no seu banco de dados.

entidade comercial

Uma estrutura aninhada de objetos base. Use a estrutura do Entity 360 no Informatica Data Director para exibir todas as informações relacionadas ao objeto base raiz de uma entidade comercial. Execute uma pesquisa no Informatica Data Director para localizar dados em uma entidade comercial.

esquema

O modelo de dados que é usado na implementação do Informatica MDM Hub de um cliente. O Informatica MDM Hub não impõe ou exige um determinado esquema. O esquema é independente dos sistemas de origem.

estado do sistema

Descreve como registros de objeto base são suportados pelo Informatica MDM Hub. Existe suporte para os seguintes estados: ACTIVE, PENDING e DELETED.

Estrutura de Integração de Serviços (SIF)

A parte do Informatica MDM Hub que faz interface com programas cliente. Logicamente, ela serve como uma camada intermediária no modelo de cliente/servidor. Ela permite que você implementar as interações de solicitação/resposta usando qualquer uma das seguintes variações arquitetônicas:

- Serviços da Web de conexão flexível usando o protocolo SOAP.
- As chamadas de procedimento remoto Java altamente acopladas com base em Enterprise JavaBeans (EJBs) ou XML.
- Mensagens assíncronas com base no Serviço de Mensagens Java (JMS).
- Documentos XML que vão e voltam via protocolo HTTP.

Filtro de segurança

Um filtro de segurança especifica uma condição aplicada pelo IDD para restringir e proteger dados de áreas de assunto que usuários individuais podem acessar. Filtros podem ser definidos na coluna do objeto primário, na coluna filho e na coluna neto. Você pode configurar qualquer número de filtros para uma área de assunto.

fluxo de trabalho

No Informatica MDM Multidomínio, um fluxo de trabalho representa um processo comercial em uma organização. Consulte [processo comercial na página 183](#).

fonte de dados

No ambiente do servidor de aplicativos, uma fonte de dados é um recurso JDBC que identifica informações sobre um banco de dados, como seu nome e localização, seu ID de usuário e senha e assim por diante. O Informatica MDM Hub precisa dessas informações para se comunicar com um ORS.

Gerenciador de Acesso de Segurança (SAM)

O Gerenciador de Acesso de Segurança (SAM) é a estrutura de segurança abrangente do Informatica MDM Hub para proteger os recursos do Informatica MDM Hub contra o acesso não autorizado. Em tempo de execução, o SAM impõe as decisões de diretivas de segurança da sua organização para a implementação do Informatica MDM Hub, o tratamento da autenticação dos usuários e a autorização de acesso, de acordo com a sua configuração de segurança.

Gerenciador de Configuração IDD

Um utilitário baseado na Web usado para adicionar, modificar e gerenciar aplicativos do IDD.

Gerenciador de Esquemas

O Gerenciador de Esquemas é um componente em tempo de design no Console do Hub usado para definir o esquema, bem como para definir as tabelas de preparação e aterrisagem. O Gerenciador de Esquemas também é usado para definir regras de correspondência e mesclagem, validação e filas de mensagens.

Gerenciador de Hierarquia

O Gerenciador de Hierarquia permite que os usuários gerenciem dados de hierarquia que estão associados aos registros gerenciados no MDM Hub . Para obter mais informações, consulte o *Guia de Configuração do Multidomain MDM* .

Gerenciamento de dados

Gerenciamento de dados é a prática de gerenciar dados como ativos corporativos em toda a empresa. Ele envolve processos, diretivas, padrões, tecnologias e pessoas em toda a organização para garantir a disponibilidade de dados precisos, consistentes e oportunos para melhorar a tomada de decisões e aprimorar os processos comerciais.

gerenciamento de estado

O processo de gerenciamento do estado do sistema do objeto base e dos registros de referência cruzada afeta a lógica de processamento em todo o fluxo de dados. Você pode atribuir um estado do sistema a registros de objeto base e referência cruzada em vários estágios do fluxo de dados, usando as ferramentas de Hub que trabalham com registros. Além disso, você pode usar as várias ferramentas de Hub para gerenciar seu esquema e ativar o gerenciamento de estado para um objeto de base ou para definir permissões de usuário que controlam quem pode alterar o estado de um registro.

O gerenciamento de estado é limitado aos seguintes estados: ACTIVE, PENDING e DELETED.

gerenciamento de processo comercial (BPM)

O gerenciamento de processo comercial se concentra na adaptação dos processos de uma organização. O Informatica MDM é enviado com um mecanismo de gerenciamento de processo comercial incorporado. Usando esse mecanismo, você pode automatizar os processos de revisão e aprovação para dados mestre.

Grupo de áreas de assunto

Um conjunto de uma ou mais áreas de assunto que têm o mesmo objeto base em sua raiz (também chamada de objeto primário).

grupo de recursos

Uma coleção de recursos seguros que simplificam a atribuição de privilégios, permitindo que você atribua privilégios a vários recursos de uma só vez, por exemplo, atribuindo grupos de recursos facilmente a uma função.

grupo de usuários

Uma coleção lógica de contas de usuário.

hierarquia

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

Kit de Recursos

O Kit de Recursos do Informatica MDM Hub é um conjunto de utilitários, exemplos e bibliotecas que fornecem exemplos de funcionalidades do Informatica MDM Hub que podem ser expandidos e implementados.

limpar função

O IDD permite que você use funções de limpeza já definidas no MDM para limpar, padronizar e validar dados de entrada. Você pode usar essa função para lidar com processos de validação e padronização e também para a ampliação de dados provenientes de outras origens.

limpeza de dados

O processo de padronizar o layout e o conteúdo de dados, decompor e analisar valores de texto em elementos identificáveis, verificar valores identificáveis (como CEPs) com base em bibliotecas de dados e substituir valores incorretos por valores corretos de bibliotecas de dados.

linhagem

Quais sistemas e quais registros desses sistemas contribuíram com registros consolidados no Armazenamento de Hub.

mapeamento

Define um conjunto de transformações que são aplicadas aos dados de origem. Mapeamentos são usados durante o processo de preparação (ou usando a solicitação de API SiperianClient CleansePut) para transferir dados de uma tabela de aterrisagem para uma tabela de preparação. Um mapeamento identifica a coluna de origem na tabela de aterrisagem e a coluna de destino a ser preenchida na tabela de preparação, juntamente com quaisquer funções de limpeza intermediárias usadas para limpar os dados.

Mascaramento de dados

Um mecanismo para ocultar informações com base em funções de segurança.

melhor versão da verdade (BVT)

Um registro que foi consolidado com as melhores células de dados dos registros de origem. Às vezes abreviado como BVT.

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.

metadados de conteúdo

Dados que descrevem os dados comerciais que foram processados pelo Informatica MDM Hub. Metadados de conteúdo são armazenados em tabelas de suporte para um objeto base, incluindo tabelas de referência

cruzada, tabelas de histórico e outras. Metadados de conteúdo são usados para ajudar a determinar de onde os dados no objeto base são provenientes e como eles mudaram ao longo do tempo.

Modelo de dados

O modelo de dados é um modelo abstrato que descreve como os dados são estruturados e organizados.

objeto base

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

objeto base de relacionamento

Um objeto base de relacionamento é um objeto base usado para armazenar informações sobre relacionamentos do Gerenciador de Hierarquia.

objeto de design

Partes dos metadados usados para definir o esquema e outras definições de configuração para uma implementação. Objetos de design incluem instâncias dos seguintes tipos de objetos do Informatica MDM Hub: objetos base e colunas, tabelas de aterrisagem e preparação, colunas, índices, relacionamentos, mapeamentos, funções de limpeza, consultas e pacotes, configurações de confiança, regras de validação e correspondência, definições do Gerenciador de Acesso de Segurança, definições do Gerenciador de Hierarquia e outras configurações.

objeto de hub

Um termo genérico para vários tipos de objetos definidos no Hub que contém informações sobre as suas entidades comerciais. Alguns exemplos incluem: objetos base, tabelas de referências cruzadas e qualquer objeto no hub que você possa associar a métricas de relatórios.

parentReference

Um parentReference pode ser definido no XML da coluna que é a chave externa para o registro filho. Isso define um rótulo a ser exibido no registro neto que contém dados provenientes do filho, para ajudar os usuários a entender o relacionamento dos netos com o filho

procedimento armazenado

Um conjunto nomeado de instruções SQL que são compiladas e armazenadas no servidor de banco de dados. Trabalhos em lote do Informatica MDM Hub são codificados em procedimentos armazenados para que possam ser executados usando scripts de execução de trabalho em um software de agendamento de trabalhos (como o Tivoli ou o CA Unicenter).

processo

Consulte [processo comercial na página 183](#).

processo comercial

Um processo comercial é um fluxo de trabalho que obtém o objetivo de uma organização e implementa uma função comercial. Um processo comercial contém as atividades que são necessárias para obter o objetivo e define os caminhos de execução por meio de atividades. O MDM Multidomínio é enviado com processos de negócios predefinidos Informatica ActiveVOS que são gerenciados pelo ActiveVOS Server. O objetivo organizacional desses processos é garantir que o pessoal autorizado, como o gerentes comerciais ou administradores de dados, revise todas as atualizações para dados mestre.

processo de validação

Processo de verificação da integridade e da precisão dos metadados que descreve um repositório. O processo de validação compara o modelo lógico de um repositório a seu esquema físico. Se qualquer problema ocorrer, o Repository Manager gerará uma lista de problemas que exigem atenção.

Provedor de Logon Externo

Um plug-in usado com o IDD para autenticar usuários com provedores de identidade externos.

Provedor de Logon Personalizado

Um módulo conectável que autentica usuários quando o aplicativo do IDD é iniciado.

referência irmã

Uma referência irmã é um relacionamento de um registro em uma área de assunto com um registro filho dentro dessa área de assunto. Por exemplo, um cliente pode incluir registros filho de endereço e de número de telefone, com o número de telefone possuindo uma chave externa a ser associada a um endereço específico.

regra de correspondência

Define os critérios com base nos quais o Informatica MDM Hub determina se os registros podem ou não ser duplicatas. Colunas de correspondência são combinadas em regras de correspondência para determinar em que condições dois registros são considerados como sendo suficientemente semelhantes para serem mesclados. Cada regra de correspondência informa ao Informatica MDM Hub a combinação de colunas de correspondência que ele precisa para examinar se há pontos de similaridade.

Relacionamentos de Área de Assunto

Relacionamentos de Área de Assunto definem como áreas de assunto estão relacionados umas com as outras. Uma área de assunto pode ter áreas de assunto filho, áreas neto e referências irmãs.

remover duplicação

Uma técnica para eliminar dados redundantes.

saída de usuário

Saídas de usuário fornecem um meio de adicionar lógica comercial personalizada a operações padrão do IDD.

Segurança de dados

A segurança dos dados impede que os usuários vejam determinados registros com base no conteúdo desses registros.

serviço de entidade comercial

Um serviço de entidade comercial é um conjunto de operações que executam o código do MDM Hub para criar, atualizar, excluir e pesquisar registros de objeto base em uma entidade comercial.

Servidor de Correspondência de Limpeza

O componente de tempo de execução Servidor de Correspondência de Limpeza é um servlet que lida com solicitações de limpeza. Esse servlet é implantado em um ambiente de servidor de aplicativos. O servlet contém dois componentes de servidor:

- um servidor de limpeza que gerencia operações de limpeza de dados
- um servidor de correspondência que lida com operações de correspondência

O Servidor de Correspondência de Limpeza é multissegmentado e, portanto, cada instância pode processar várias solicitações ao mesmo tempo. Ele pode ser implantado em uma variedade de servidores de aplicativos.

O Servidor de Correspondência de Limpeza faz interface com qualquer um dos mecanismos de limpeza com suporte, como o mecanismo de limpeza Trillium Director. O Servidor de Correspondência de Limpeza e o mecanismo de limpeza trabalham para padronizar os dados. Essa padronização funciona estreitamente com o Mecanismo de Consolidação Informatica (anteriormente conhecido como Mecanismo de Mesclagem) para otimizar os dados para consolidação.

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.

tabela de correspondências

Tipo de tabela do sistema, associada a um objeto base, que dá suporte ao processo de correspondência. Durante a execução de um trabalho de Correspondência para um objeto base, o Informatica MDM Hub preenche sua tabela de correspondência associada com os valores ROWID_OBJECT para cada par de registros correspondidos, além do identificador da regra de correspondência que resultou na correspondência e um indicador de mesclagem automática.

tabela de histórico

Um tipo de tabela em um ORS que contém informações históricas sobre alterações em uma tabela associada. Tabelas de histórico fornecem opções de controle de alterações detalhadas, incluindo o histórico de mesclagem e operações de desfazer mesclagem, o histórico dos dados previamente limpos, o histórico do objeto base e o histórico da referência cruzada.

tipo de correspondência

Cada coluna de correspondência tem um tipo de correspondência que determina como a coluna de correspondência será tokenizada em preparação para a comparação de correspondência.

tipo de dados

Define as características de valores permitidos em uma coluna de — caracteres, números, datas, dados binários e assim por diante.

valor nulo

A ausência de um valor em uma coluna de um registro. Nulo não é o mesmo que em branco ou zero.

ÍNDICE

A

Adicionar um Aplicativo do IDD [42](#)
Agrupamento Lógico de Menus [66](#)
ajuda
 arquivo de ajuda personalizado, criando [93](#)
 arquivo de ajuda personalizado, importando [93](#)
ajuda online
 arquivo de ajuda personalizado, criando [93](#)
 arquivo de ajuda personalizado, importando [93](#)
Arquivo XML de Configuração do IDD [59](#)
Associação do ORS [41](#)
Atribuição Automática de Tarefas [152](#)
Atribuição Manual de Tarefas [153](#)
Atributos de Guias Filho Personalizadas [77](#)
Atributos e Marcas ActionType [149](#)
Atributos e Marcas TaskType [144](#)
Atualizando as Propriedades Globais [105](#)
Autenticação do Usuário (SSO) [19](#)

C

Caminhos de Correspondência [20](#)
Códigos de Idioma [159](#)
Códigos de País [164](#), [169](#)
Coluna de Pesquisa [61](#)
Conceitos do IDD
 Aplicativo do IDD [14](#)
 Arquivos de Configuração do IDD [14](#)
 Gerenciador de Configuração IDD [14](#)
 Grupos de Áreas de Assunto [16](#)
Conceitos do Informatica Data Director
 Áreas de Assunto [15](#)
conexão única
 configurações do provedor de logon [50](#)
confiança
 sobre [22](#)
configuração da segurança de dados
 exemplo de objetos neto [121](#)
 exemplo de objetos pai [120](#)
Configuração da Segurança de Tarefas [150](#)
Configuração de Atribuição de Tarefas [151](#)
Configuração de Segurança [112](#)
Configuração do HM [68](#)
configuração do navegador
 requisitos [110](#)
Configurações do Provedor de Logon
 bibliotecas de terceiros [52](#)
 Criar a Biblioteca do Provedores de Logon [56](#)
 Implementar o Provedor de Logon Personalizado [52](#)
Configurando a Pesquisa
 Configurar a Pesquisa Básica [34](#)
 Configurar Consultas Públicas [35](#)
 Configure a Pesquisa Estendida [34](#)
Configurar a Autenticação SSO do Salesforce (WebLogic) [56](#)

Configurar a Autenticação SSO do Salesforce (WebSphere) [56](#)
Configurar a Limpeza e a Validação [33](#)
Configurar a Pesquisa [34](#)
Configurar a Segurança [37](#)
Configurar Áreas de Assunto [31](#)
Configurar Extensões da Interface do Usuário [37](#)
Configurar Grupos de Áreas de Assunto [31](#)
Configurar o Estilo de Edição de Caixa de Seleção [68](#)
Configurar o Fluxo de Trabalho [36](#)
Configurar Pesquisas de Correspondências e Duplicatas no IDD [35](#)
Criar o Aplicativo do IDD [30](#)
Criar Referência Irmã [65](#)

D

Descrições de Componentes de Configuração de Fluxo de Trabalho e Tarefas [142](#)
Diagrama de Componentes de Configuração de Fluxo de Trabalho e Tarefas [141](#)
Dimensionamento do Cliente e da Rede [109](#)
Dimensionamento do Servidor de Aplicativos [109](#)
Dimensionamento do Servidor de Banco de Dados [109](#)

E

Editar Aplicativo
 Áreas de Assunto [46](#)
 Bancos de Dados ORS Lógicos [45](#)
 Propriedades da Área de Assunto [47](#)
 Propriedades de Filhos e Netos da Área de Assunto [48](#)
 Propriedades do Grupo de Áreas de Assunto [47](#)
Estado do Aplicativo [44](#)
Estrutura de Integração de Serviços [18](#)
exibição de dados
 expandir um área de assunto filho por padrão [65](#)
Exibição de Dados [27](#)
Exibição de Hierarquia [27](#)
Exibir os Campos Secundários de um Objeto Base na Guia Filho [63](#)
Extensões da Interface do Usuário [73](#)

F

Ferramenta BPM
 configurar [36](#)
Ferramentas de XML [59](#)
Fluxo de Trabalho e Tarefas [22](#)
Funções de Limpeza
 Funções de Limpeza que Retornam NULL [22](#)
 Limpeza de e Padronização [21](#)
 Validação [21](#)

G

Gerenciador de Acesso à Segurança [23](#)
Gerenciador de Hierarquia [23](#)
Guia do Usuário
arquivo de ajuda revisado, importando [92](#), [93](#)
guias
guias personalizadas [73](#)
Guias de Nível Superior
guias [73](#)
Guias Filho Personalizadas (área de assunto) [76](#)

H

Histórico [24](#)

I

Implantação [44](#)
importação de dados
importando o modelo [50](#)
Importar uma Configuração de Aplicativo do IDD [42](#)
Indicadores [26](#)
Informatica Data Director [12](#)

L

Layout do Espaço de Trabalho Início
sobre [76](#)
Limpar Cache
sobre [19](#)
Linha do Tempo [25](#)
Links de Área de Assunto [66](#)
links externos
parâmetros [77](#)
Links Externos (Componentes Personalizados do Espaço de Trabalho Início) [74](#)
Localização de Pesquisas [49](#)
Localizar o Aplicativo [38](#)

M

Mascaramento de dados [138](#)
métricas
métricas de gerenciamento de tarefas [155](#)
métricas de gerenciamento de tarefas
sobre [155](#)
módulo de provedor de logon personalizado
logon único [50](#)
Módulo de Provedor de Logon Personalizado
Carregando [51](#)

N

Netos [65](#)
Notificação de Tarefas [154](#)

O

Objetos Base [19](#)

P

página de erro personalizada
configurando [91](#)
Página Inicial [40](#)
parâmetros
para links externos [77](#)
parâmetros dinâmicos
para links externos [77](#)
parâmetros estáticos
para links externos [77](#)
Personalizando a Atribuição Automática de Tarefas [153](#)
Personalizando Rótulos de Coluna [67](#)
Pesquisa sem Distinção entre Maiúsculas e Minúsculas [35](#)
Pesquisar
Básica - Pesquisa baseada em SQL [20](#)
Estendida - Pesquisa baseada em Correspondência [20](#)
Pesquisa Avançada [21](#)
Pesquisas Dependentes [25](#)
Pré-requisitos [13](#)
processo de configuração
sobre [30](#)
Propriedades de Links Externos [77](#)

R

Referência a Componentes de Aplicativo [111](#)
Referência a Propriedades Globais do IDD [95](#)
Regras de Linha do Tempo [26](#)
Relacionamentos em Áreas de Assunto
Referências Irmãs [18](#)
Relacionamentos Filho de Muitos-para-Muitos [16](#)
Relacionamentos Filho de Um-para-Muitos [16](#)
Relacionamentos Neto de Muitos-para-Muitos [17](#)
Relacionamentos Neto de Um-para-Muitos [17](#)

S

SAM e Segurança
Mascaramento de dados [24](#)
Segurança de Dados [24](#)
Segurança de Objetos e Colunas [23](#)
segurança de dados
usando filtros [119](#)
Segurança de Dados [119](#)
servidores Web
usando [19](#)
Siperian BPM
aviso de obsolescência [140](#)

T

Tabelas de Pesquisa [24](#)
Tabelas de Pesquisa com Coluna de Subtipo [62](#)
tempo limite da sessão [46](#)
Tipos de Ação [148](#)
Tipos de Ação - XML de Amostra [148](#)
Tipos de Tarefa [143](#)
Tipos de Tarefa - XML de Amostra [143](#)

V

Validação [43](#)
Valores de Pesquisa Estáticos [63](#)

visão geral [12](#)

Visão Geral da Configuração Manual do IDD [58](#)

Visão Geral do Gerenciador de Configuração IDD [39](#)

Visão Geral do Processo de Implementação [29](#)