



Informatica®

10.5.9

# Guia de Segurança

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, o logotipo Informatica, Informatica Cloud, PowerCenter e PowerExchange 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.

Consulte as patentes em <https://www.informatica.com/legal/patents.html>.

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

Sujeito aos seus direitos de descadastramento descritos abaixo, o Software transmitirá automaticamente para a Informatica nos EUA informações sobre o ambiente de rede e computação no qual o Software é implantado, bem como sobre o uso de dados e as estatísticas do sistema da implantação. Essa transmissão é considerada parte dos Serviços conforme a política de privacidade da Informatica, e a Informatica usará e processará essas informações de acordo com a política de privacidade da Informatica, disponível em <https://www.informatica.com/in/privacy-policy.html>. Você pode desativar a coleção de uso na ferramenta Administrator.

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](mailto: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: 2025-10-21

# Conteúdo

<b>Prefácio.....</b>	<b>11</b>
Recursos da Informatica. . . . .	11
Informatica Network. . . . .	11
Base de Dados de Conhecimento da Informatica. . . . .	11
Documentação da Informatica. . . . .	11
Matrizes de Disponibilidade de Produto da Informatica. . . . .	12
Informatica Velocity. . . . .	12
Informatica Marketplace. . . . .	12
Suporte Global a Clientes da Informatica. . . . .	12
 <b>Capítulo 1: Introdução à Segurança do Informatica.....</b>	 <b>13</b>
Visão Geral da Segurança da Informatica. . . . .	13
Segurança de Infraestrutura. . . . .	14
Autenticação. . . . .	14
Comunicação Segura no Domínio. . . . .	15
Armazenamento de Dados Seguro. . . . .	16
Segurança Operacional. . . . .	16
Repositório de Configuração de Domínio. . . . .	16
Domínio de segurança. . . . .	17
 <b>Capítulo 2: Autenticação de Usuário.....</b>	 <b>18</b>
Visão Geral da Autenticação de Usuário. . . . .	18
Autenticação de Usuário Nativa. . . . .	19
Autenticação de Usuário LDAP. . . . .	19
Autenticação Kerberos. . . . .	20
Autenticação SAML. . . . .	20
Autenticação SAML para aplicativos da Web da Informatica. . . . .	21
Autenticação SAML para o Informatica Developer. . . . .	21
 <b>Capítulo 3: Autenticação LDAP.....</b>	 <b>23</b>
Visão geral. . . . .	23
Domínios de Segurança LDAP. . . . .	23
Sincronização de conta de usuário. . . . .	24
Serviços de diretório LDAP. . . . .	24
Azure Active Directory para autenticação LDAP segura. . . . .	25
Preparar para Importar Contas de Usuário do Active Directory. . . . .	26
Criando uma configuração do LDAP. . . . .	26
Criar a configuração do LDAP e configurar a conexão do servidor LDAP. . . . .	27
Configurar um domínio de segurança. . . . .	28
Configurar o agendamento de sincronização. . . . .	30

Usando grupos aninhados no diretório de serviço LDAP. . . . .	31
Usando um certificado SSL autoassinado. . . . .	31
Excluindo uma configuração do LDAP. . . . .	31

## **Capítulo 4: Autenticação Kerberos. . . . . 33**

Visão geral do Kerberos. . . . .	33
Como o Kerberos opera em um domínio Informatica. . . . .	34
Autenticação de realm cruzado Kerberos. . . . .	36
Convertendo um domínio da autenticação de realm único Kerberos para a autenticação de realm cruzado Kerberos. . . . .	36
Preparando-se para ativar a autenticação Kerberos. . . . .	37
Determinar o nível da entidade de segurança de serviço Kerberos. . . . .	37
Definir o arquivo de configuração Kerberos. . . . .	38
Criar contas de entidade de segurança Kerberos no Active Directory. . . . .	41
Gerar os formatos do nome da entidade de segurança de serviço e do nome do arquivo keytab. . . . .	42
Gerar os arquivos keytab. . . . .	48
Ativando a autenticação Kerberos. . . . .	52
Ativar a autenticação Kerberos no domínio. . . . .	52
Atualizar os Nós no Domínio. . . . .	54
Ativando o Kerberos em nós Informatica. . . . .	56
Copiar os arquivos keytab para os nós Informatica. . . . .	57
Ativar a autenticação Kerberos para clientes Informatica. . . . .	58
Habilitando o Kerberos para Integração com o Hadoop. . . . .	58
Ativando contas de usuário para usar a autenticação Kerberos. . . . .	59
Importar contas de usuário do Active Directory para domínios de segurança LDAP. . . . .	59
Migrar permissões e privilégios de usuários nativos para um domínio de segurança Kerberos. . . . .	62
Delegação Kerberos. . . . .	64
Tipos de delegação Kerberos. . . . .	64
Extensão de serviço para usuário (S4U). . . . .	64
Ativar a delegação restrita baseada em recursos com S4U2Self. . . . .	64
Ativar a delegação completa para as contas de usuário de entidade principal Kerberos no Active Directory. . . . .	65
Mudar de Delegação Completa para Delegação Restrita. . . . .	66

## **Capítulo 5: Autenticação SAML para aplicativos da Web da Informatica. . . . . 67**

Visão geral da autenticação SAML. . . . .	67
Default Keystore and Truststore Directory. . . . .	68
Provedores de Identidade Compatíveis. . . . .	68
Processo de autenticação SAML. . . . .	69
Ativar a autenticação SAML em um domínio. . . . .	70
Crie uma configuração LDAP para o provedor de identidade ou o armazenamento LDAP. . . . .	70
Exportar o certificado de assinatura de declaração. . . . .	70

Importar o certificado para o truststore usado na autenticação SAML. . . . .	71
Configurar o provedor de identidade. . . . .	71
Adicionar URLs do aplicativo da Web da Informatica ao provedor de identidade. . . . .	71
Configurar a Autenticação SAML no Domínio. . . . .	71
Ativar a autenticação SAML nos nós de . . . . .	72
Segurança de Autenticação Aprimorada. . . . .	72
Assinatura de Solicitação. . . . .	73
Resposta Assinada. . . . .	74
Asserção Criptografada. . . . .	75
Configurando aplicativos da Web para usar diferentes provedores de identidade. . . . .	75
Preparar-se para usar um provedor de identidade. . . . .	76
Configurar o Informatica Administrator para usar um provedor de identidade. . . . .	76
Configurar um aplicativo da Web da Informatica. . . . .	78

## **Capítulo 6: Segurança de domínio..... 80**

Visão Geral da Segurança do Domínio. . . . .	80
Secure Communication Within the Domain. . . . .	81
Comunicação Segura para Serviços e o Gerenciador de Serviços. . . . .	82
Banco de Dados do Repositório de Configuração de Domínio Seguro. . . . .	88
Banco de Dados do Repositório do PowerCenter Seguro. . . . .	91
Banco de Dados do Repositório do Modelo Seguro. . . . .	91
Comunicação Segura para Fluxos de Trabalho e Sessões. . . . .	92
Conexões Seguras com um Serviço de Aplicativo da Web. . . . .	93
Requisitos para Conexões Seguras para Serviços de Aplicativo da Web. . . . .	93
Ativando Conexões Seguras para a Ferramenta Administrator. . . . .	94
Serviços de Aplicativo da Web Informatica. . . . .	94
Pacotes de criptografia para o domínio Informatica. . . . .	97
Criar as listas de pacote de criptografia. . . . .	98
Ativar o TLS 1.3 . . . . .	100
Configure o domínio Informatica com uma nova lista efetiva de pacotes de criptografia. . . . .	100
Origens e Destinos Seguros. . . . .	101
Origens e Destinos do Serviço de Integração de Dados. . . . .	101
Origens e Destinos do PowerCenter. . . . .	102
Secure Data Storage. . . . .	103
Diretório Seguro no UNIX. . . . .	103
Alterando a Chave de Criptografia da Linha de Comando. . . . .	104
Serviços de Aplicativo e Portas. . . . .	106

## **Capítulo 7: Gerenciamento de Segurança no Informatica Administrator..... 109**

Usando a visão geral do Informatica Administrator. . . . .	109
Segurança do Usuário. . . . .	110
Encryption. . . . .	110
Autenticação. . . . .	110

Autorização. . . . .	111
Guia Segurança. . . . .	112
Usando a seção Pesquisa. . . . .	112
Usando o Navegador de Segurança. . . . .	113
Grupos. . . . .	113
Usuários. . . . .	114
Funções. . . . .	114
Perfis do sistema operacional. . . . .	115
Configuração do LDAP. . . . .	115
Gerenciamento de conta. . . . .	115
Relatórios de Auditoria. . . . .	116
Gerenciamento de Senha. . . . .	116
Alterando a senha. . . . .	117
Gerenciamento de segurança do domínio. . . . .	117
Gerenciamento de segurança do usuário. . . . .	117
<b>Capítulo 8: Usuários e grupos. . . . .</b>	<b>119</b>
Visão geral de usuários e grupos. . . . .	119
Grupos Padrão. . . . .	120
Grupo Administrador. . . . .	120
Grupo Todos. . . . .	120
Grupo Operador. . . . .	121
Entendendo as contas de usuário. . . . .	121
Administrador Padrão. . . . .	121
Administrador de domínio. . . . .	121
Administrador de Cliente de Aplicativo. . . . .	122
Usuário. . . . .	123
Gerenciando usuários. . . . .	123
Criando usuários nativos. . . . .	123
Editando Propriedades Gerais de Usuários Nativos. . . . .	124
Atribuindo Usuários Nativos a Grupos Nativos. . . . .	124
Atribuindo Usuários LDAP a Grupos Nativos. . . . .	125
Ativando e desativando contas de usuário. . . . .	125
Excluindo usuários nativos. . . . .	125
Usuários LDAP. . . . .	126
Desbloqueando uma conta de usuário. . . . .	126
Aumentando a Memória do Sistema para Muitos Usuários. . . . .	127
Exibindo a Atividade do Usuário. . . . .	127
Gerenciando grupos. . . . .	131
Adicionando um Grupo Nativo. . . . .	131
Editando Propriedades de um Grupo Nativo. . . . .	132
Movendo um grupo nativo para outro grupo nativo. . . . .	132
Excluindo um grupo nativo. . . . .	133

Grupos LDAP. . . . .	133
Managing operating system profiles. . . . .	133
Propriedades do perfil do sistema operacional para o Serviço de Integração do PowerCenter	133
Propriedades do Perfil do Sistema Operacional para o Serviço de Integração de Dados. . . . .	135
Propriedades do perfil do sistema operacional para o Serviço de Acesso a Metadados. . . . .	137
Criando um perfil do sistema operacional. . . . .	137
Editando um perfil do sistema operacional. . . . .	139
Atribuindo um perfil do sistema operacional padrão a um usuário ou grupo. . . . .	139
Excluindo um perfil do sistema operacional . . . . .	140
Working with Operating System Profiles in a Secure Domain. . . . .	140
Trabalhando com Perfis do Sistema Operacional em um Domínio com Autenticação Kerberos	141
Bloqueio de conta. . . . .	142
Configurando o bloqueio de conta. . . . .	142
Regras e diretrizes para o bloqueio de conta. . . . .	143
<b>Capítulo 9: Privilégios e funções.....</b>	<b>144</b>
Privilégios. . . . .	144
Grupos de Privilégio. . . . .	145
Funções. . . . .	145
Privilégios do domínio. . . . .	146
Grupo de privilégio Administração de segurança. . . . .	146
Grupo de Privilégios Administração de Domínio. . . . .	147
Grupo de privilégio Monitoramento. . . . .	151
Grupo de privilégio Ferramentas. . . . .	153
Grupo de Privilégio da Administração de Nuvem. . . . .	153
Privilégios do Serviço Analyst. . . . .	153
Privilégios do Serviço do Gerenciamento de Conteúdo. . . . .	155
Privilégios do Data Integration Service. . . . .	155
Privilégio do Serviço de Ingestão em Massa. . . . .	156
Privilégios do Serviço do Metadata Manager. . . . .	156
Grupo de Privilégio Catálogo. . . . .	157
Carregar grupo de privilégio. . . . .	158
Grupo de privilégio Modelo. . . . .	159
Grupo de privilégio Segurança. . . . .	159
Privilégios do Serviço de Repositório do Modelo. . . . .	159
Privilégios do Serviço de Repositório do PowerCenter. . . . .	160
Grupo de privilégio Ferramentas. . . . .	161
Grupo de Privilégio Pastas. . . . .	162
Grupo de privilégio Objetos de design. . . . .	163
Grupo de privilégio Origens e destinos. . . . .	166
Grupo de privilégio de Objetos em Tempo de Execução. . . . .	168
Grupo de privilégio de objetos globais. . . . .	172
Privilégios do Serviço do Ouvinte do PowerExchange. . . . .	175

Privilégios do Serviço do Agente de Log do PowerExchange. . . . .	175
Privilégios do Serviço de Agendador. . . . .	176
Privilégios do Serviço do Test Data Manager. . . . .	177
Grupo de Privilégios Administração. . . . .	177
Grupo de Privilégio Conexões. . . . .	177
Grupo de Privilégio Domínios de Dados. . . . .	178
Grupo de Privilégio Mascaramento de Dados. . . . .	178
Grupo de Privilégios Subconjunto de Dados. . . . .	178
Grupo de Privilégio Diretivas. . . . .	179
Grupo de Privilégios Projetos. . . . .	179
Grupo de Privilégios Regras. . . . .	179
Grupo de Privilégio Geração de Dados. . . . .	180
Gerenciando Funções. . . . .	180
Funções definidas pelo sistema. . . . .	180
Funções personalizadas. . . . .	182
Atribuindo privilégios e funções aos usuários e grupos. . . . .	183
Privilégios herdados. . . . .	184
Atribuindo Privilégios e Funções a um Usuário ou Grupo por Navegação. . . . .	184
Exibindo usuários com privilégios para um serviço. . . . .	185
Solucionando problemas de privilégios e funções. . . . .	185
<b>Capítulo 10: Permissões. . . . .</b>	<b>188</b>
Visão geral de permissões. . . . .	188
Tipos de Permissões. . . . .	189
Filtros de pesquisa de permissão. . . . .	190
Permissões do Objeto de Domínio. . . . .	190
Permissões do objeto de domínio. . . . .	191
Permissões por usuário ou grupo. . . . .	192
Permissões do perfil do sistema operacional. . . . .	193
Permissões de Conexão. . . . .	194
Tipos de permissões de conexão. . . . .	195
Permissões de Conexão Padrão. . . . .	195
Atribuindo Permissões sobre uma Conexão. . . . .	195
Exibindo detalhes de permissão em uma conexão. . . . .	196
Editando permissões em uma conexão. . . . .	196
Permissões de configuração de cluster. . . . .	197
Permissões de aplicativos e objetos de aplicativo. . . . .	197
Tipos de permissões de aplicativos e objetos de aplicativo. . . . .	197
Atribuindo permissões em um aplicativo ou objeto de aplicativo. . . . .	197
Exibindo detalhes de permissões em um aplicativo ou objeto de aplicativo. . . . .	198
Editando permissões em um aplicativo ou objeto de aplicativo. . . . .	198
Negando permissões em um aplicativo ou objeto de aplicativo. . . . .	199
Permissões de Serviço de Dados SQL. . . . .	199



Tipos de Permissões de Serviço de Dados SQL. . . . .	199
Atribuindo Permissões em um serviço de dados SQL. . . . .	200
Exibindo Detalhes de Permissão em um Serviço de Dados SQL. . . . .	200
Editando permissões em um Serviço de Dados SQL. . . . .	201
Negando Permissões em um Serviço de Dados SQL. . . . .	201
Segurança em Nível de Coluna. . . . .	202
Permissões do serviço da Web. . . . .	203
Tipos de Permissões de Serviços da Web. . . . .	203
Atribuindo permissões em um serviço da Web. . . . .	204
Exibindo Detalhes de Permissão em um Serviço da Web. . . . .	205
Editando permissões em um serviço Web. . . . .	205
<b>Capítulo 11: Relatórios de Auditoria. . . . .</b>	<b>207</b>
Visão Geral dos Relatórios de Auditoria. . . . .	207
Informações Pessoais do Usuário. . . . .	208
Associação de Grupo de Usuários. . . . .	208
Privilégios. . . . .	209
Associação de Funções. . . . .	210
Permissões em Objetos de Domínio. . . . .	210
Selecionando Usuários para um Relatório de Auditoria. . . . .	211
Selecionando Grupos para um Relatório de Auditoria . . . . .	212
Selecionando Funções para um Relatório de Auditoria. . . . .	212
<b>Apêndice A: Permissões e Privilégios da Linha de Comando. . . . .</b>	<b>214</b>
Comandos infacmd as. . . . .	214
Comandos infacmd cluster. . . . .	215
Comandos infacmd dis. . . . .	216
Comandos infacmd dp. . . . .	218
Comandos infacmd es. . . . .	218
Comandos infacmd ipc. . . . .	218
Comandos infacmd isp. . . . .	218
Comandos infacmd mas. . . . .	228
Comandos infacmd mi. . . . .	229
Comandos infacmd mrs. . . . .	229
Comandos infacmd ms. . . . .	232
Comandos infacmd tools. . . . .	232
Comandos infacmd ps. . . . .	232
Comandos infacmd pwx. . . . .	233
Comandos infacmd rms. . . . .	234
Comandos infacmd rtm. . . . .	235
Comandos infacmd sch. . . . .	235
Comandos infacmd sql. . . . .	236
Comandos infacmd wfs. . . . .	237

Comandos pmcmd. . . . .	237
Comandos pmrep. . . . .	240
<b>Apêndice B: Funções personalizadas. . . . .</b>	<b>245</b>
Função Personalizada do Serviço Analyst. . . . .	245
Funções Personalizadas do Serviço do Metadata Manager. . . . .	246
Função Personalizada do Operador. . . . .	248
Funções Personalizadas do Serviço do Repositório do PowerCenter. . . . .	249
Regras personalizadas do Test Data Manager. . . . .	250
<b>Índice. . . . .</b>	<b>254</b>

# Prefácio

Use o *Guia de Segurança da Informatica* para aprender como habilitar a segurança em um domínio Informatica. Entenda como configurar e gerenciar vários protocolos de autenticação, incluindo o Lightweight Directory Access Protocol, o Kerberos e a Security Assertion Markup Language. Aprenda como gerenciar usuários e grupos e como usar permissões, privilégios e funções para gerenciar a segurança do usuário.

## 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](mailto: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](mailto: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](mailto: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 Informatica Network.

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 Suporte.

# CAPÍTULO 1

## Introdução à Segurança do Informatica

Este capítulo inclui os seguintes tópicos:

- [Visão Geral da Segurança da Informatica, 13](#)
- [Segurança de Infraestrutura, 14](#)
- [Segurança Operacional, 16](#)
- [Repositório de Configuração de Domínio, 16](#)
- [Domínio de segurança, 17](#)

## Visão Geral da Segurança da Informatica

Você pode proteger o domínio Informatica contra ameaças de dentro e de fora da rede em que o domínio é executado.

Veja a seguir os tipos de segurança para o domínio Informatica:

### **Segurança de Infraestrutura**

A segurança de infraestrutura protege o domínio Informatica contra acesso não autorizado ou modificação de recursos e serviços no domínio Informatica. A segurança de infraestrutura inclui os seguintes aspectos:

- Proteção de dados transmitidos e armazenados no domínio Informatica
- Autenticação de usuários e serviços que se conectam ao domínio Informatica
- Segurança de conexões para componentes externos, incluindo aplicativos cliente e bancos de dados relacionais para repositórios, origens e destinos.

### **Segurança Operacional**

A segurança operacional controla o acesso a dados e serviços no domínio Informatica. A segurança operacional inclui os seguintes aspectos:

- Definição de restrições para o acesso do usuário a dados e metadados com base na função do usuário na organização
- Definição de restrições para a capacidade do usuário em realizar operações no domínio Informatica com base na função do usuário na organização

O Informatica armazena as informações de configuração de domínio e a lista de usuários autorizados a acessar o domínio no repositório de configuração de domínio. O repositório de configuração de domínio

também contém os grupos, as funções, os privilégios e as permissões atribuídos a cada usuário no domínio Informatica.

O Informatica organiza a lista de usuários por domínios de segurança. Um domínio de segurança contém um conjunto de contas de usuário. Um domínio pode ter vários domínios de segurança.

## Segurança de Infraestrutura

A segurança de infraestrutura inclui a autenticação de serviço e de usuário, a comunicação segura no domínio e o armazenamento seguro de dados.

### Autenticação

O Gerenciador de Serviços autentica os serviços executados no domínio e os usuários que fazem login nas ferramentas do cliente Informatica.

Você pode configurar o domínio Informatica para usar os seguintes tipos de autenticação:

#### **Autenticação Nativa**

A autenticação nativa é um modo de autenticação disponível somente para contas de usuário no domínio Informatica. Quando o domínio Informatica usa a autenticação nativa, o Gerenciador de Serviços armazena as credenciais e os privilégios do usuário no repositório de configuração de domínio e executa a autenticação de usuário completa no domínio Informatica.

Se o domínio Informatica usar a autenticação nativa, por padrão, o domínio terá um domínio de segurança Nativo e todas as contas de usuário pertencerão ao domínio de segurança Nativo.

A Informatica usa o nome de usuário e as senhas para autenticar usuários e serviços no domínio Informatica.

#### **Autenticação de Protocolo LDAP (Lightweight Directory Access Protocol)**

LDAP é um protocolo de software para acessar usuários e recursos em uma rede. Se o domínio Informatica usar a autenticação LDAP, as contas e as credenciais de usuário são armazenadas no serviço de diretório LDAP. Os privilégios e as permissões do usuário são armazenados no repositório de configuração de domínio. É necessário sincronizar periodicamente as contas de usuário no repositório de configuração de domínio com as contas de usuário no serviço de diretório LDAP.

A Informatica usa o nome de usuário e as senhas para autenticar os usuários e os serviços da Informatica no domínio Informatica.

#### **Autenticação Kerberos**

Kerberos é um protocolo de autenticação de rede que usa tíquetes para autenticar usuários e serviços em uma rede. Quando o domínio Informatica usa a autenticação Kerberos, as contas de usuário e as credenciais são armazenadas no banco de dados de entidades de segurança do Kerberos, que pode ser um serviço de diretório LDAP. Os privilégios e as permissões do usuário são armazenados no repositório de configuração de domínio. É necessário sincronizar periodicamente as contas de usuário no repositório de configuração de domínio com as contas de usuário no banco de dados de entidades de segurança do Kerberos.

A Informatica usa os tíquetes Kerberos para autenticar os usuários e os serviços da Informatica no domínio Informatica.

### Single Sign-on com base em SAML

A SAML (Security Assertion Markup Language) é um formato de dados com base em XML para a troca de informações de autenticação e autorização entre um provedor de serviços e um provedor de identidade. É possível configurar o logon único com base em SAML para aplicativos da Web da ferramenta Administrator, da ferramenta Analyst e da ferramenta Monitoring.

Em um domínio Informatica, o aplicativo da Web Informatica é o provedor de serviços, e o Microsoft Active Directory Federation Services (AD FS) é o provedor de identidade. As contas e credenciais para usuários de aplicativos da Web Informatica são armazenadas no Microsoft Active Directory. Você pode importar contas do Active Directory em um domínio de segurança no domínio Informatica.

Periodicamente, você deve sincronizar as contas de usuários no domínio de segurança com as contas de usuários no serviço de diretório do Active Directory.

Observe que você não pode ativar o logon único com base em SAML em um domínio Informatica configurado para usar a autenticação Kerberos.

## Comunicação Segura no Domínio

O domínio Informatica tem várias opções para proteger dados e metadados que são transmitidos entre o Gerenciador de Serviços e os serviços no domínio e nos aplicativos cliente. O Informatica usa os protocolos TCP/IP e HTTP para se comunicar entre os componentes no domínio e usa certificados SSL para proteger a comunicação entre os serviços e o Gerenciador de Serviços no domínio.

O protocolo SSL/TLS usa a criptografia de chaves pública para criptografar e descriptografar o tráfego da rede. A chave pública usada para criptografar e descriptografar o tráfego é armazenada em um certificado SSL que pode ser autoassinado ou assinado. Um certificado autoassinado é assinado pelo criador do certificado. Como a identidade de signatário não é verificada, um certificado autoassinado é menos seguro do que um certificado assinado. Um certificado assinado é um certificado SSL que tem a identidade da pessoa que solicitou o certificado verificada por uma autoridade de certificação (CA). A Informatica recomenda os certificados assinados por CA para obter um nível de segurança mais alto.

Um armazenamento de chaves contém chaves privadas e certificados. Ele é usado para fornecer uma credencial. Um truststore contém o certificado de servidores SSL e TLS confiáveis. Ele é usado para verificar uma credencial.

Para proteger conexões no domínio, a Informatica exige armazenamentos de chaves e truststores nos formatos PEM e JKS. Você pode usar os seguintes programas para criar os arquivos obrigatórios:

#### keytool

Você pode usar a chave keytool Java e o utilitário de gerenciamento de certificados para criar um certificado SSL ou uma solicitação de assinatura de certificado (CSR), assim como armazenamentos de chaves e truststores no formato JKS.

O utilitário keytool está disponível no seguinte diretório nos nós de domínio:

```
<Informatica installation directory>\java\bin
```

Se os nós de domínio forem executados no AIX, você poderá usar o keytool fornecido com o IBM JDK para criar um certificado SSL ou uma Solicitação de Assinatura de Certificado (CSR), assim como armazenamentos de chaves e truststores.

#### OpenSSL

Você pode usar o OpenSSL para criar um certificado SSL ou CSR, bem como converter um armazenamento de chaves no formato JKS em formato PEM.

Para obter mais informações sobre o OpenSSL, consulte a documentação no seguinte site:

<https://www.openssl.org/docs/>

O tipo de conexão que você protege determina os arquivos exigidos.

## Armazenamento de Dados Seguro

O Informatica criptografa dados confidenciais, como senhas e parâmetros de conexão segura, antes de armazená-los no repositório de configuração de domínio. O Informatica também salva arquivos confidenciais, como arquivos de configuração, em um diretório seguro.

## Segurança Operacional

Você pode atribuir privilégios, funções e permissões para usuários ou grupos de usuários para gerenciar o nível de acesso que usuários e grupos podem ter e o escopo das ações que usuários e grupos podem realizar no domínio.

Você pode usar os seguintes métodos para gerenciar o acesso de usuários e grupos no domínio:

### Privilégios

Os privilégios determinam as ações que os usuários podem executar nas ferramentas do cliente Informatica. Você pode atribuir um conjunto de privilégios a um usuário para restringir o acesso aos serviços disponíveis no domínio. Você também pode atribuir privilégios a um grupo para permitir que todos os usuários do grupo tenham o mesmo acesso aos serviços.

### Funções

Uma função é um conjunto de privilégios que você pode atribuir a usuários e grupos. Você pode usar as funções para facilitar o gerenciamento de atribuições de privilégios aos usuários. Você pode criar uma função com privilégios limitados e atribuí-la a usuários e grupos que têm acesso restrito a serviços do domínio. Se preferir, você poderá criar funções com privilégios relacionados para atribuir aos usuários e grupos que precisam do mesmo nível de acesso.

### Permissões

As permissões definem o nível de acesso que os usuários têm em um objeto. Um usuário que tem o privilégio para executar determinada ação pode precisar de permissão para executar a ação em um objeto específico. Por exemplo, para gerenciar um serviço de aplicativo, um usuário deve ter o privilégio para gerenciar serviços e a permissão para o serviço de aplicativo específico.

### Grupo Administrador Padrão

O domínio Informatica tem um grupo Administrador definido pelo sistema que inclui todos os privilégios e as permissões de um serviço. Todas as contas de usuário que você adiciona ao grupo Administrador têm os privilégios e as permissões em todos os serviços e objetos no domínio. Quando você instala os serviços Informatica, o instalador cria uma conta de usuário que pertence ao grupo Administrador. Você pode usar a conta de Administrador padrão para fazer login inicialmente na ferramenta Administrator.

## Repositório de Configuração de Domínio

O repositório de configuração de domínio contém informações sobre a configuração de domínio e privilégios e permissões de usuário.

Se o domínio Informatica usa a autenticação de usuário nativa, o repositório de configuração de domínio também inclui as credenciais do usuário. Se o domínio usa a autenticação LDAP ou Kerberos, o repositório de configuração de domínio não inclui as credenciais do usuário. Todas as credenciais do usuário do LDAP e



Kerberos são armazenadas fora do domínio Informatica, no serviço de diretório LDAP ou no banco de dados de entidades de segurança do Kerberos.

Quando você cria o domínio Informatica durante a instalação, o instalador cria um repositório de configuração de domínio em um banco de dados relacional. Você deve especificar o banco de dados no qual criar o repositório de configuração de domínio. Você pode criar o repositório em um banco de dados protegido com o protocolo SSL.

## Domínio de segurança

Um domínio de segurança é um conjunto de contas de usuário e grupos no domínio Informatica.

O domínio Informatica pode ter os seguintes tipos de domínios de segurança:

### **Domínio de Segurança Nativo**

O domínio de segurança Nativo contém os usuários e grupos criados e gerenciados na ferramenta Administrator. A Informatica armazena todas as credenciais de contas de usuário no domínio de segurança Nativo no repositório de configuração de domínio. Por padrão, o domínio de segurança Nativo é criado durante a instalação. Após a instalação, você não poderá criar domínios de segurança Nativos adicionais ou excluir o domínio de segurança Nativo.

Se o domínio Informatica usar a autenticação Kerberos, não poderá usar o domínio de segurança Nativo.

### **Domínio de Segurança LDAP**

Um domínio de segurança LDAP contém os usuários e grupos importados de um serviço de diretório LDAP. Se o domínio Informatica usa a autenticação LDAP ou Kerberos, você pode criar um domínio de segurança LDAP e adicionar usuários e grupos que você importar do serviço de diretório LDAP.

Quando você instala serviços Informatica e cria um domínio que usa a autenticação nativa ou LDAP, o instalador cria o domínio de segurança Nativo, mas não cria um domínio de segurança LDAP. Você poderá criar domínios de segurança LDAP após a instalação.

Quando você instala serviços Informatica e cria um domínio que usa a autenticação Kerberos, o instalador cria os seguintes domínios de segurança LDAP:

- Domínio de segurança interno. O instalador cria um domínio de segurança LDAP com o nome `_infalInternalNamespace`. O domínio de segurança `_infalInternalNamespace` inclui a conta de usuário do administrador padrão que você cria durante a instalação. Após a instalação, você não poderá adicionar usuários ao domínio de segurança `_infalInternalNamespace`, nem excluir o domínio de segurança.
- Domínio de segurança do realm do usuário. O instalador cria um domínio de segurança LDAP vazio e dá a ele o mesmo nome do realm do usuário Kerberos especificado durante a instalação. Após a instalação, você poderá importar usuários do banco de dados de entidades de segurança do Kerberos para o domínio de segurança do realm do usuário. Você não pode excluir o domínio de segurança do realm do usuário.  
Quando você executa programas de linha de comando em um domínio que usa a autenticação Kerberos, o padrão da opção do domínio de segurança é o domínio de segurança do realm do usuário criado durante a instalação.

Crie e gerencie domínios de segurança LDAP da mesma maneira, seja qual for a autenticação usada pelo domínio Informatica (LDAP ou Kerberos).

## CAPÍTULO 2

# Autenticação de Usuário

Este capítulo inclui os seguintes tópicos:

- [Visão Geral da Autenticação de Usuário, 18](#)
- [Autenticação de Usuário Nativa, 19](#)
- [Autenticação de Usuário LDAP, 19](#)
- [Autenticação Kerberos, 20](#)
- [Autenticação SAML, 20](#)

## Visão Geral da Autenticação de Usuário

A autenticação de usuário no domínio Informatica depende do tipo de autenticação que você configura ao instalar os serviços Informatica.

O domínio Informatica pode usar os seguintes tipos de autenticação para autenticar os usuários no domínio Informatica:

- Autenticação de usuário nativa
- Autenticação de usuário LDAP
- Autenticação de rede Kerberos
- Logon único com base em SAML (Security Assertion Markup Language)

As contas de usuário nativas são armazenadas no domínio Informatica e podem ser usadas somente nele.

As contas de usuário, LDAP e Kerberos são armazenadas em um serviço de diretório LDAP e compartilhadas por aplicativos dentro da empresa.

O logon único com base em SAML autentica os usuários usando as credenciais de contas armazenadas no Microsoft Active Directory. As contas são importadas do Active Directory para um domínio de segurança no domínio Informatica.

Você pode selecionar o tipo de autenticação para usar no domínio Informatica durante a instalação. Se você ativar a autenticação Kerberos durante a instalação, deverá configurar o domínio Informatica para trabalhar com o KDC (Centro de Distribuição de Chaves). Você deve criar os nomes principais de serviço (SPN) exigidos pelo domínio Informatica no banco de dados de entidades de segurança do Kerberos. O banco de dados de entidades de segurança Kerberos pode ser um serviço de diretório LDAP. Você também deve criar os arquivos keytab para os SPNs e armazená-los no diretório da Informatica, conforme exigido pelo domínio Informatica.

Se você não ativar a autenticação Kerberos durante a instalação, o instalador vai configurar o domínio Informatica para usar a autenticação nativa. Após a instalação, você poderá estabelecer uma conexão com

um servidor LDAP e configurar o domínio Informatica para usar a autenticação LDAP juntamente com a autenticação nativa.

Você pode usar a autenticação nativa e a autenticação LDAP juntas no domínio Informatica. O Gerenciador de Serviços autentica os usuários com base no domínio de segurança. Se o usuário pertencer ao domínio de segurança nativo, o Gerenciador de Serviços o autenticará no repositório de configuração de domínio. Se o usuário pertencer a um domínio de segurança LDAP, o Gerenciador de Serviços enviará o nome de usuário e a senha ao servidor LDAP para autenticação.

Você não pode usar a autenticação nativa com a autenticação Kerberos. Se o domínio Informatica usar a autenticação Kerberos, todas as contas de usuário deverão estar nos domínios de segurança LDAP. O servidor Kerberos autentica a conta de usuário quando o usuário faz logon na rede. Os aplicativos cliente Informatica usam as credenciais do logon de rede para autenticar os usuários no domínio Informatica. Os grupos e funções nativos ainda são compatíveis.

Durante ou após a instalação, você pode ativar o logon único com base em SAML para aplicativos da Web Informatica. No entanto, você deve concluir todas as tarefas de configuração necessárias antes de habilitar o logon único com base em SAML. Você não pode ativar o logon único com base em SAML em um domínio Informatica configurado para usar a autenticação Kerberos.

Quando o domínio Informatica reside no local e não em uma instância AWS EC2, você não pode usar o protocolo de autenticação EMRFS na integração com o Amazon EMR.

Você pode criptografar o token de credencial do usuário com a chave exclusiva do site. Para criptografar o token de credencial do usuário, defina a variável de ambiente `infaEnableAdvancedEncryptionSchemeForCredential` como `true`. No caso de autenticação de usuário nativo e LDAP, após a autenticação de usuário bem-sucedida, o token de credencial criptografado será usado em vez da senha do usuário.

## Autenticação de Usuário Nativa

Se o domínio Informatica usa a autenticação nativa, o Gerenciador de Serviços armazena todas as informações da conta de usuário e executa a autenticação de usuário completa no domínio Informatica. Quando um usuário faz logon, o Gerenciador de Serviços usa o domínio de segurança nativo para autenticar o nome de usuário e a senha.

Se você não configurar o domínio Informatica para usar a autenticação de rede Kerberos, ele incluirá um domínio de segurança nativo por padrão. Ele é criado na instalação e não pode ser excluído. Um domínio Informatica pode ter somente um domínio de segurança nativa. Crie e mantenha contas de usuário no domínio de segurança nativo na ferramenta Administrator. O Gerenciador de Serviços armazena detalhes sobre as contas de usuário, incluindo as credenciais e os privilégios do usuário, no repositório de configuração de domínio.

## Autenticação de Usuário LDAP

Você pode configurar um domínio Informatica para permitir que os usuários em um serviço de diretório LDAP façam logon nos aplicativos cliente da Informatica. Você pode criar várias configurações do LDAP

para um domínio, cada uma conectando-se a um servidor LDAP diferente. Um domínio pode usar a autenticação de usuário LDAP juntamente com a autenticação de usuário nativa.

Para permitir que o domínio Informatica utilize a autenticação de usuário LDAP, você deve configurar uma conexão com um servidor LDAP e especificar os usuários e os grupos do serviço de diretório LDAP que podem ter acesso ao domínio Informatica. Você pode usar a ferramenta Administrator para configurar a conexão com o servidor LDAP.

Quando você sincroniza os domínios de segurança LDAP com o serviço de diretório LDAP, o Gerenciador de Serviços importa a lista de contas de usuário LDAP com acesso ao domínio Informatica para os domínios de segurança LDAP. Quando você atribui privilégios e permissões aos usuários em domínios de segurança LDAP, o Gerenciador de Serviços armazena as informações no repositório de configuração de domínio. O Gerenciador de Serviços não armazena as credenciais do usuário no repositório de configuração de domínio.

Quando um usuário faz logon, o Gerenciador de Serviços envia o nome de usuário e a senha ao servidor LDAP para autenticação.

**Nota:** O Gerenciador de Serviços requer que os usuários LDAP façam logon em um aplicativo cliente usando uma senha, mesmo que um serviço de diretório LDAP permita uma senha em branco para o modo de logon anônimo.

## Autenticação Kerberos

Você pode configurar o domínio Informatica para usar a autenticação de rede Kerberos para autenticar os usuários e os serviços em uma rede.

Kerberos é um protocolo de autenticação de rede que usa tíquetes para autenticar o acesso a serviços e nós em uma rede. O Kerberos usa um KDC (Centro de Distribuição de Chaves) para validar as identidades de usuários e serviços e para conceder tickets a contas de usuário e serviço autenticadas. No protocolo Kerberos, os usuários e serviços são conhecidos como entidades. O KDC tem um banco de dados de entidades e suas chaves secretas associadas que são usadas como comprovação de identidade. O Kerberos pode usar um serviço de diretório LDAP como um banco de dados de entidade.

Para usar a autenticação Kerberos, você deve instalar e executar o domínio Informatica em uma rede que usa a autenticação de rede Kerberos. O Informatica pode ser executado em uma rede na qual a autenticação Kerberos é usada com o serviço do Microsoft Active Directory como o banco de dados de entidade.

Você pode configurar um domínio Informatica para usar autenticação de realm cruzado Kerberos. A autenticação de realm cruzado Kerberos permite que os clientes da Informatica que pertencem a um realm Kerberos se autenticuem com nós e serviços de aplicativos que pertencem a outro realm Kerberos.

O domínio Informatica requer arquivos keytab para autenticar nós e serviços no domínio sem transmitir senhas pela rede. Os arquivos keytab contêm os nomes de entidades de serviço (SPN) e as chaves criptografadas associadas. Crie os arquivos keytab antes de criar nós e serviços no domínio Informatica.

## Autenticação SAML

É possível configurar um domínio Informatica para permitir que os usuários usem a autenticação SAML (Security Assertion Markup Language) para fazer logon nos aplicativos Web da ferramenta Administrator, da ferramenta Analyst, da ferramenta Ingestão em Massa, do Metadata Manager e da ferramenta Monitoring.

Você também pode configurar um domínio Informatica para usar a autenticação SAML no Informatica Developer (a Developer tool).

A SAML é um formato de dados com base em XML para a troca de informações de autenticação e autorização entre um provedor de serviços e um provedor de identidade.

## Autenticação SAML para aplicativos da Web da Informatica

Em um domínio Informatica, o aplicativo da Web Informatica é o provedor de serviços. O Microsoft Active Directory Federation Services (ADFS) é o provedor de identidade que autentica os usuários de aplicativos da Web com o repositório de identidade do Active Directory da sua organização.

Para permitir que o domínio Informatica use o logon único com base em SAML, você deve criar um domínio de segurança LDAP para contas de usuário de aplicativos da Web Informatica e, em seguida, importar os usuários para o domínio do Active Directory. Você pode usar a ferramenta Administrator para configurar a conexão para o servidor Active Directory e em seguida, importar os usuários para o domínio de segurança.

Quando um usuário faz login em um aplicativo da Web Informatica, o aplicativo envia uma solicitação de autenticação SAML ao ADFS. O ADFS autentica as credenciais do usuário com base nas informações de contas de usuários no Active Directory e, em seguida, retorna um token de assertiva SAML contendo informações relacionadas à segurança sobre o usuário ao aplicativo da Web.

Configure o ADFS para emitir tokens SAML para autenticar os usuários do aplicativo da Web Informatica. Você também deve exportar o Certificado de Assinatura de Declaração do Provedor de Identidade do ADFS e depois importar esse certificado para o arquivo de truststore padrão do Informatica em cada nó de gateway do domínio.

## Autenticação SAML para o Informatica Developer

Você pode habilitar a autenticação SAML no Informatica Developer (a Developer tool).

Para habilitar a autenticação SAML, ative o seguinte sinalizador no arquivo developerCore.ini:

```
-DsamlAuthenticationEnabled=true
```

Você pode encontrar o arquivo developerCore.ini no seguinte diretório: <diretório de instalação do Informatica>\clients\DeveloperClient

Você também deve exportar o Certificado de Assinatura de Declaração do provedor SAML e depois importar esse certificado para o arquivo de truststore padrão do Informatica na Developer tool.

### Modos de autenticação SAML

Você pode autenticar um usuário em um domínio habilitado para SAML dos seguintes modos:

#### Nome de usuário e senha

Usa as credenciais de login do usuário.

Adicione a seguinte propriedade ao arquivo developerCore.ini:

```
-DkerberosLoginType=TYPE_USER_PWD
```

#### Keytab

Usa o keytab gerado para o usuário no provedor SAML. Selecione o espaço de nome configurado por SAML ao conectar a Developer tool ao repositório do modelo.

Adicione as seguintes propriedades ao arquivo developerCore.ini:

```
-DkerberosLoginType=TYPE_KEYTAB
```

```
-DkerberosAuthSPN=<SPN value generated from the SAML provider for the user>
```

```
-DkerberosAuthKeytab=<Location of the keytab file generated from the SAML provider  
for the user>
```

**Usuário conectado**

Usa as credenciais de login do usuário para fazer login no computador em que a Developer tool está instalada. Selecione o espaço de nome configurado por SAML ao conectar a Developer tool ao repositório do modelo.

Adicione a seguinte propriedade ao arquivo developerCore.ini:

```
-DkerberosLoginType=TYPE_LOGGED_IN_USER
```

## CAPÍTULO 3

# Autenticação LDAP

Este capítulo inclui os seguintes tópicos:

- [Visão geral, 23](#)
- [Domínios de Segurança LDAP, 23](#)
- [Sincronização de conta de usuário, 24](#)
- [Serviços de diretório LDAP, 24](#)
- [Azure Active Directory para autenticação LDAP segura, 25](#)
- [Criando uma configuração do LDAP, 26](#)
- [Excluindo uma configuração do LDAP, 31](#)

## Visão geral

Você pode configurar um domínio Informatica para permitir que usuários importados de um ou mais serviços de diretório LDAP façam login nos nós, serviços e clientes de aplicativos da Informatica, como Informatica Developer e Informatica Analyst.

Um serviço de diretório LDAP armazena nomes de usuário e senhas da conta. O uso da autenticação LDAP permite consolidar as credenciais de todos os usuários do Informatica em um único repositório de identidades, simplificando a tarefa de criar e atualizar as credenciais da conta.

Você pode usar a autenticação nativa e a autenticação LDAP juntas em um domínio Informatica. O Gerenciador de Serviços em execução no nó de gateway mestre no domínio autentica os usuários com base no domínio de segurança ao qual os usuários pertencem. Se o usuário pertencer ao domínio de segurança nativo padrão, o Gerenciador de Serviços o autenticará em relação às informações da conta no repositório de configuração de domínio. Se o usuário pertencer a um domínio de segurança LDAP, o Gerenciador de Serviços enviará as credenciais ao servidor LDAP para autenticação.

## Domínios de Segurança LDAP

Um domínio de segurança LDAP contém os usuários e grupos importados de um serviço de diretório LDAP. Você pode definir vários domínios de segurança LDAP em um domínio Informatica. Você pode importar contas dos serviços de diretório LDAP para os domínios de segurança.

Você deverá criar um domínio de segurança LDAP se configurar um domínio Informatica para usar a autenticação Kerberos. Quando você instala serviços Informatica ativando a autenticação Kerberos, o

instalador do Informatica cria um domínio de segurança LDAP com o nome do realm Kerberos especificado durante a instalação.

Ao criar um domínio de segurança LDAP, você configura bases e filtros de pesquisa que definem o conjunto de contas e grupos de usuários LDAP a serem incluídos no domínio de segurança. O Gerenciador de Serviços usa a configuração do domínio de segurança para importar ou sincronizar usuários e grupos no domínio de segurança com usuários e grupos no serviço de diretório LDAP.

O Gerenciador de Serviços usa os seguintes critérios quando importa ou sincroniza usuários e grupos em um domínio de segurança LDAP:

- O Gerenciador de Serviços usa as bases e filtros de pesquisa de usuário para importar contas de usuários.
- O Gerenciador de Serviços usa as bases e filtros de pesquisa de grupo para importar grupos.
- O Gerenciador de Serviços importa os grupos incluídos no filtro de grupos e as contas de usuário incluídas no filtro de usuários.

## Sincronização de conta de usuário

O Gerenciador de Serviços atualiza o domínio de segurança com os usuários e grupos em um serviço de diretório LDAP com base em agendamento. Você pode configurar o agendamento de sincronização ao configurar a autenticação LDAP.

O Gerenciador de Serviços executa as seguintes etapas durante a sincronização:

- Recupera uma lista atualizada de usuários e grupos do serviço de diretório LDAP, de acordo com a base de pesquisa e nos filtros configurados para o domínio de segurança.
- Atualiza a lista de usuários e grupos LDAP no domínio de segurança. Se um usuário LDAP no domínio de segurança tiver sido excluído do serviço de diretório LDAP, o Gerenciador de Serviços transferirá a propriedade dos objetos do usuário para a conta de administrador do domínio.

## Serviços de diretório LDAP

Você pode importar contas de usuário para domínios de segurança da Informatica a partir de serviços de diretório LDAP.

Você pode importar usuários dos seguintes serviços de diretório LDAP:

- IBM Tivoli Directory Server
- Microsoft Active Directory
- Microsoft Azure Active Directory
- Novell eDirectory
- OpenLDAP
- Oracle Directory Server (ODSEE)
- Oracle Unified Directory (OUD)
- Servidor de Diretório Sun Java System



**Nota:** Se você usar a autenticação Kerberos, poderá importar somente os usuários do Microsoft Active Directory.

O Gerenciador de Serviços exige um ID exclusivo (UID) particular para identificar usuários em cada serviço de diretório LDAP. A tabela a seguir mostra o UID padrão para cada serviço de diretório LDAP:

Serviço de Diretório LDAP	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Microsoft Azure Active Directory	UserPrincipalName
Novell eDirectory	uid
OpenLDAP	uid
Oracle Directory Server (ODSEE)	uid
Oracle Unified Directory (OUD)	uid
Servidor de Diretório Sun Java System	uid

## Azure Active Directory para autenticação LDAP segura

Você pode importar usuários do Azure Active Directory (Azure AD) para um domínio de segurança LDAP.

O Azure Active Directory Domain Services fornece um endereço IP público LDAP seguro que você usa para importar contas de usuários do Azure Active Directory para um domínio de segurança LDAP. Os usuários importados podem usar suas credenciais LDAP para efetuar login nos nós, serviços e aplicativos do Informatica que são executados em máquinas virtuais de um domínio gerenciado do Azure Active Directory.

Para ver as versões com suporte do Active Directory, consulte a Matriz de Disponibilidade do Produto na Informatica Network:

<https://network.informatica.com/community/informatica-network/product-availability-matrices>.

Você deve habilitar a autenticação do protocolo LDAP (Secure Lightweight Access Protocol) no Azure Active Directory Domain Services para autenticar os usuários da Informatica.

Você pode ler os seguintes artigos na Biblioteca de Instruções da Informatica para ver uma exibição completa do processo de uso da autenticação LDAP com o Active Directory:

- [Enabling SAML Authentication with Active Directory Federation Services in Informatica 10.4.0](#)
- [Enabling SAML Authentication with Azure Active Directory for Web Applications](#)

## Preparar para Importar Contas de Usuário do Active Directory

Conclua as seguintes etapas para preparar a importação de contas de usuário do Azure Active Directory para um domínio Informatica:

1. Verifique se a porta 636, que é a porta LDAP segura do Azure Active Directory, pode ser acessada por meio do firewall.
2. Ative a autenticação LDAP segura no Azure Active Directory Domain Services.  
Use o portal do Azure para habilitar o LDAP seguro no Azure Active Directory Domain Services. Para obter informações sobre como configurar o LDAP seguro no Azure Active Directory Domain Services, consulte o seguinte link:  
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap>
3. Ao configurar o certificado LDAP seguro nos Azure Active Directory Domain Services, verifique se o nome da entidade no certificado é FQDN (Nome de Domínio Totalmente Qualificado) do Azure Active Directory.
4. Converta o certificado LDAP seguro do formato PFX no formato PEM. O Java requer que o certificado esteja no formato PEM.
5. Importe os certificados usados por todos os nós de domínio para o arquivo `truststore cacerts` do Java no seguinte diretório em um único nó de gateway no domínio:  
`<diretório de instalação da Informatica>/java/jre/lib/security/`
6. Copie o arquivo `cacerts` que contém os certificados importados para o mesmo diretório em todos os outros nós de gateway no domínio.
7. Adicione o endereço IP público do Azure Active Directory e o FQDN (Nome de Domínio Totalmente Qualificado) do Azure Active Directory ao arquivo `/etc/hosts` em cada nó de gateway no domínio. Use o seguinte formato:  
`<endereço IP do host do Azure Active Directory> ldaps.<FQDN do Azure Active Directory>`

## Criando uma configuração do LDAP

Você pode criar uma ou mais configurações do LDAP para permitir que contas e grupos de usuários importados dos serviços de diretório LDAP se autenticem com um domínio Informatica.

Crie e gerencie usuários e grupos LDAP no serviço de diretório LDAP. Configure uma conexão com o servidor de diretório LDAP e use filtros de pesquisa para especificar os usuários e os grupos que podem ter acesso ao domínio Informatica. Em seguida, importe as contas de usuário para um domínio de segurança LDAP. Se o servidor LDAP usa o protocolo SSL, também é necessário especificar a localização do certificado SSL.

Após importar usuários para um domínio de segurança LDAP, você poderá atribuir funções, privilégios e permissões a eles. É possível atribuir contas de usuário LDAP a grupos nativos para organizá-las com base em suas funções no domínio Informatica.

Não é possível usar a ferramenta Administrator para criar, editar ou excluir usuários e grupos em um domínio de segurança LDAP. Você deve fazer alterações em usuários e grupos LDAP no serviço de diretório LDAP e sincronizar o domínio de segurança LDAP com o serviço de diretório LDAP.

Use a caixa de diálogo Configuração do LDAP para configurar a conexão com o serviço de diretório LDAP e criar o domínio de segurança LDAP para o qual as contas de usuário serão importadas. Você também pode usar a caixa de diálogo Configuração LDAP para configurar um agendamento de sincronização.

Para criar uma configuração do LDAP, realize as seguintes etapas:

1. Configure a conexão com o servidor LDAP que contenha o serviço de diretório do qual você deseja importar as contas e os grupos de usuários.
2. Crie um domínio de segurança LDAP para cada conjunto de contas de usuário e grupos que você deseja importar do serviço de diretório LDAP.
3. Configure um agendamento diário para o Gerenciador de Serviços atualizar os domínios de segurança LDAP com usuários e grupos novos ou alterados no serviço de diretório LDAP.

## Criar a configuração do LDAP e configurar a conexão do servidor LDAP

Crie a configuração do LDAP e configure a conexão com o servidor LDAP que contém o serviço de diretório do qual você deseja importar as contas de usuário.

Ao configurar a conexão com o servidor LDAP, indique se o Gerenciador de Serviços deve ignorar a distinção entre maiúsculas e minúsculas dos atributos de nome diferenciado das contas de usuário LDAP ao atribuir usuários a grupos no domínio Informatica. Se o Gerenciador de Serviços não ignorar a distinção entre maiúsculas e minúsculas, talvez ele não atribua todos os usuários pertencentes a um grupo.

Se o servidor LDAP usar SSL, você deverá importar o certificado usado por cada nó de domínio para o arquivo truststore `cacerts` em um domínio de nó de gateway. Em seguida, copie o arquivo `cacerts` que contém os certificados importados para o mesmo diretório em todos os nós no domínio. Para obter mais informações, consulte ["Usando um certificado SSL autoassinado" na página 31](#).

Para configurar uma conexão com o serviço de diretório LDAP, execute as seguintes tarefas:

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Clique na guia **Configuração do LDAP**.
3. Clique no menu **Ações** e selecione **Criar Configuração do LDAP**.
4. Na caixa de diálogo **Criar Configuração do LDAP**, clique na guia **Conectividade do LDAP**.
5. Configure as propriedades de conexão do servidor LDAP.

Talvez seja necessário consultar o administrador do LDAP para obter as informações necessárias para a conexão com o servidor LDAP.

A tabela a seguir descreve as propriedades de configuração do servidor LDAP:

Propriedade	Descrição
Nome da Configuração do LDAP	Nome da configuração do LDAP.
Nome do servidor	Nome do host ou endereço IP da máquina que hospeda o serviço de diretório LDAP.
Porta	Porta de escuta do servidor LDAP. Esse é o número da porta para comunicação com o serviço de diretório LDAP. Normalmente, o número da porta do servidor LDAP é 389. Se o servidor LDAP usar SSL, o número da porta do servidor LDAP será 636. O número máximo da porta é 65535.
Serviço de Diretório LDAP	Tipo do serviço de diretório LDAP. <b>Nota:</b> Se você usa a autenticação Kerberos, selecione o Serviço do Microsoft Active Directory.

Propriedade	Descrição
Nome	Nome Diferenciado (DN) do usuário principal. O nome de usuário geralmente consiste em um nome comum (CN), uma organização (O) e um país (C). O nome do usuário principal é um usuário administrativo com acesso ao diretório. Especifique um usuário que tenha permissão para ler outras entradas do usuário no serviço de diretório LDAP. Para se conectar ao Azure Active Directory, especifique o Nome Principal do Usuário (UPN) para o usuário principal.
Senha	Senha do usuário principal. Deixe em branco para login anônimo.
Usar Certificado SSL	Indica que o servidor LDAP usa o protocolo SSL (Secure Socket Layer).
Confiar no Certificado LDAP	Determina se o Gerenciador de Serviços pode confiar no certificado SSL do servidor LDAP. Se for selecionado, o Gerenciador de Serviços se conectará ao servidor LDAP sem verificar o certificado SSL. Se não for selecionado, o Gerenciador de Serviços verificará se o certificado SSL está assinado por uma autoridade de certificado antes de se conectar ao servidor LDAP.
Não Diferencia Maiúsculas de Minúsculas	Indica que o Service Manager deve ignorar maiúsculas e minúsculas para atributos de nome distinto ao atribuir usuários a grupos.
Atributo de Associação de Grupo	Nome do atributo que contém informações de associação do grupo para um usuário. Esse é o atributo no objeto do grupo LDAP que contém os DNs dos usuários ou grupos que são membros de um grupo. Por exemplo, <i>member</i> ou <i>memberof</i> .
Tamanho Máximo	Número máximo de contas de usuário a serem importadas para um domínio de segurança. Por exemplo, se o valor for definido como 100, você poderá importar no máximo 100 contas de usuário para o domínio de segurança.  Se o número dos usuários a serem importados exceder o valor para essa propriedade, o Gerenciador de Serviços gerará uma mensagem de erro e não importará nenhum usuário. Defina essa propriedade com um valor mais alto se você tiver muito usuários para importar.  O padrão é 1000.

6. Clique em **Testar Conexão** para verificar se a conexão com o servidor LDAP é válida.
7. Clique em **OK** para salvar a configuração do LDAP.

## Configurar um domínio de segurança

Crie um domínio de segurança LDAP para cada conjunto de contas de usuário e grupos que você deseja importar do serviço de diretório LDAP. Configure bases e filtros de pesquisa para definir o conjunto de contas de usuários e grupos a ser incluídos em um domínio de segurança.

Os nomes de usuários e grupos a ser importados do serviço de diretório LDAP devem atender às mesmas regras que os nomes de usuários e grupos nativos. O Gerenciador de Serviços não importa usuários ou grupos LDAP se os nomes não atenderem às regras de nomes de usuários e grupos nativos. Observe que, diferentemente dos nomes de usuários nativos, os nomes de usuários LDAP podem fazer distinção entre maiúsculas e minúsculas.

O Gerenciador de Serviços usa as bases e filtros de pesquisa de usuários para importar contas de usuários e as bases e filtros de pesquisa de grupos para importar grupos. O Gerenciador de Serviços usa os filtros para importar grupos e a lista de usuários que pertencem a cada grupo.

Se você modificar as propriedades de conexão do LDAP para fazer a conexão a um servidor LDAP diferente, o Gerenciador de Serviços não excluirá os domínios de segurança existentes. Você deve garantir que os domínios de segurança LDAP estejam corretos para o novo servidor LDAP. Modifique os filtros de usuários e grupos nos domínios de segurança ou crie domínios de segurança adicionais para que o Gerenciador de Serviços importe corretamente os usuários e grupos que você deseja usar no domínio Informatica.

Para configurar um domínio de segurança LDAP, execute as seguintes etapas:

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Clique no menu **Ações** e selecione **Configuração do LDAP**.
3. Na caixa de diálogo **Configuração LDAP**, clique na guia **Domínios de Segurança**.
4. Clique em **Adicionar**.

A tabela a seguir descreve as propriedades de filtro que você pode definir para um domínio de segurança:

Propriedade	Descrição
Domínio de Segurança	Nome do domínio de segurança LDAP. O nome não faz distinção entre maiúsculas e minúsculas, e deve ser exclusivo no domínio. A cadeia não pode ter mais de 128 caracteres, nem conter os seguintes caracteres especiais: , + / < > @ ; \ % ? O nome pode conter um caractere de espaço ASCII, exceto para o primeiro e o último caracteres. Nenhum outro caractere de espaço é permitido.
Base de pesquisa do usuário	Nome diferenciado (DN) da entrada que serve como ponto de partida para pesquisar nomes de usuário no serviço de diretório LDAP. A pesquisa localiza um objeto no diretório de acordo com o caminho no nome distinto do objeto. Por exemplo, no Microsoft Active Directory, o nome diferenciado de um objeto de usuário pode ser cn=UserName,ou=OrganizationalUnit,dc=DomainName, onde a série de nomes diferenciados relativos indicada por dc=DomainName identifica o domínio DNS do objeto.
Filtro de usuário	Uma sequência de consulta LDAP especifica os critérios de pesquisa para usuários no serviço de diretório. O filtro pode especificar os tipos de atributos, os valores de declaração e os critérios de correspondência. Por exemplo: (objectclass=*) pesquisa todos os objetos. (&(objectClass=user)(!(cn=susan))) pesquisa todos os objetos de usuário, exceto "susan". Para obter mais informações sobre filtros de pesquisa, consulte a documentação do serviço de diretório LDAP.
Base de pesquisa do grupo	Nome diferenciado (DN) da entrada que serve como ponto de partida para pesquisar nomes de grupos no serviço de diretório LDAP.
Filtro de grupo	Uma cadeia de consulta LDAP especifica os critérios para pesquisar grupos no serviço de diretório.

5. Clique em **Visualizar** para exibir um subconjunto da lista de usuários e grupos que se enquadram nos parâmetros do filtro.

Se a visualização não exibir o conjunto correto de usuários e grupos, modifique os filtros de usuários e grupos e as bases de pesquisa para obter os usuários e grupos corretos.

6. Para sincronizar imediatamente os usuários e os grupos nos domínios de segurança com os usuários e os grupos do serviço de diretório LDAP, clique em **Sincronizar Agora**.

O Gerenciador de Serviços sincroniza os usuários em todos os domínios de segurança LDAP com os usuários no serviço de diretório LDAP. O tempo que leva para concluir o processo de sincronização depende do número de usuários e grupos a serem importados.

7. Clique em **OK** para salvar o domínio de segurança.

## Configurar o agendamento de sincronização

Você pode configurar um agendamento diário para o Gerenciador de Serviços para atualizar os domínios de segurança LDAP com usuários e grupos novos ou alterados no serviço de diretório LDAP.

Quando o Gerenciador de Serviços sincroniza os domínios de segurança LDAP com o serviço de diretório LDAP, ele importa todos os usuários que correspondem às configurações do filtro de usuário do serviço de diretório LDAP para o domínio de segurança. Em seguida, o Gerenciador de Serviços importa todos os grupos que correspondem às configurações do filtro de grupo e associa os usuários aos grupos correspondentes. O Gerenciador de Serviços também exclui qualquer usuário ou grupo não encontrado no serviço de diretório LDAP do domínio de segurança.

Por padrão, o Gerenciador de Serviços não possui um horário agendado para sincronização com o serviço de diretório LDAP. Para garantir que a lista de usuários e grupos nos domínios de segurança LDAP seja precisa, agende quando o Gerenciador de Serviços deve sincronizar os domínios de segurança LDAP com o serviço de diretório LDAP. O Gerenciador de Serviços sincroniza os domínios de segurança LDAP com o serviço de diretório LDAP todos os dias nos horários definidos.

Para garantir que a sincronização seja bem-sucedida, considere as seguintes recomendações antes de configurar o agendamento de sincronização:

**Verifique se o arquivo `/etc/hosts` contém uma entrada para o servidor LDAP.**

Verifique se o arquivo `/etc/hosts` em cada gateway de nó no domínio contém uma entrada com o nome do host e o endereço IP do servidor LDAP. Se o Gerenciador de Serviços não puder resolver o nome do host do servidor LDAP, a sincronização poderá falhar.

**Habilite a paginação no LDAP se você estiver sincronizando mais de 100 usuários ou grupos.**

Habilite a paginação no serviço de diretório LDAP antes de sincronizar mais de 100 usuários ou grupos. Se você não habilitar a paginação no serviço de diretório LDAP, a sincronização poderá falhar.

**Sincronize os domínios de segurança durante os horários em que a maioria dos usuários não está conectada aos aplicativos Informatica.**

Durante a sincronização, o Gerenciador de Serviços bloqueia todas as contas de usuário que ele sincroniza. Os usuários podem não conseguir fazer login nos clientes do aplicativo Informatica durante a sincronização. Os usuários que fizeram login em um aplicativo cliente quando a sincronização é iniciada podem não conseguir executar determinadas tarefas.

Para configurar um agendamento que sincroniza os domínios de segurança LDAP com o serviço de diretório LDAP, execute as seguintes etapas:

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Clique no menu **Ações** e selecione **Configuração LDAP**.
3. Na caixa de diálogo **Configuração LDAP**, clique na guia **Agendamento**.
4. Clique no botão **Adicionar (+)** para adicionar um horário.  
O agendamento da sincronização usa um formato de 24 horas.
5. Para sincronizar imediatamente os usuários e os grupos nos domínios de segurança LDAP com os usuários e os grupos do serviço de diretório LDAP, clique em **Sincronizar Agora**.

6. Clique em **OK** para salvar o agendamento da sincronização.

**Nota:** Aguarde até que o Gerenciador de Serviços seja sincronizado com o serviço de diretório LDAP antes de reiniciar o domínio Informatica para evitar a perda dos tempos de sincronização definidos no planejamento.

## Usando grupos aninhados no diretório de serviço LDAP

Um domínio de segurança LDAP pode conter grupos LDAP aninhados. O Service Manager pode importar grupos aninhados que sejam criados da seguinte maneira:

- Crie os grupos nas mesmas unidades organizacionais (OU).
- Configure o relacionamento entre os grupos.

Por exemplo, é possível criar um agrupamento aninhado onde GrupoB é um membro de GrupoA, e GrupoD é um membro do GrupoC.

1. Crie o GrupoA, o GrupoB, o GrupoC e o GrupoD na mesma OU.
2. Edite o GrupoA e adicione o GrupoB como um membro.
3. Edite o GrupoC e adicione o GrupoD como um membro.

Não é possível importar grupos LDAP aninhados para um domínio de segurança LDAP que seja criado de maneira diferente.

## Usando um certificado SSL autoassinado

É possível conectar-se a um servidor LDAP que usa um certificado SSL assinado por uma autoridade de certificação (CA). Por padrão o Gerenciador de Serviços não conecta-se a um servidor LDAP que usa um certificado autoassinado.

Para se conectar a um servidor LDAP que usa um certificado SSL, use a chave keytool do Java e o utilitário de gerenciamento de chaves para importar os certificados usados por todos os nós de domínio no arquivo truststore `cacerts` do Java no único nó de gateway no domínio. Em seguida, copie o arquivo keystore `cacerts` que contém os certificados importados para outros nós de no domínio.

O arquivo de truststore `cacerts` está no seguinte diretório de cada nó:

```
<diretório de instalação do Informatica>\java\jre\lib\security
```

O utilitário keytool está disponível no seguinte diretório em cada nó:

```
<diretório de instalação Informatica>\java\bin
```

Reinicie o nó depois de importar o certificado.

## Excluindo uma configuração do LDAP

Você pode excluir uma configuração do LDAP e os domínios de segurança associados para proibir permanentemente os usuários de acessar o domínio.

Ao excluir uma configuração do LDAP, você deve primeiro excluir os domínios de segurança associados à configuração do LDAP. O Gerenciador de Serviços exclui todas as contas e grupos de usuários em cada domínio de segurança LDAP excluído do banco de dados de configuração do domínio.

1. Na ferramenta Administrator, clique na guia **Segurança**.

2. Clique na guia **Configuração do LDAP**.
3. Clique na guia **Domínios de Segurança** e clique no botão **Editar**.
4. Selecione o domínio de segurança na caixa de diálogo **Editar Configuração do LDAP** e clique em **Excluir**.
5. Selecione a configuração LDAP a ser excluída no navegador de Configuração LDAP.
6. Clique no menu **Ações** e selecione **Excluir Configuração do LDAP**.
7. Clique em **OK** para confirmar que você deseja excluir a configuração do LDAP.



## CAPÍTULO 4

# Autenticação Kerberos

Este capítulo inclui os seguintes tópicos:

- [Visão geral do Kerberos, 33](#)
- [Como o Kerberos opera em um domínio Informatica, 34](#)
- [Autenticação de realm cruzado Kerberos, 36](#)
- [Preparando-se para ativar a autenticação Kerberos, 37](#)
- [Ativando a autenticação Kerberos, 52](#)
- [Ativando o Kerberos em nós Informatica, 56](#)
- [Habilitando o Kerberos para Integração com o Hadoop, 58](#)
- [Ativando contas de usuário para usar a autenticação Kerberos, 59](#)
- [Delegação Kerberos, 64](#)

## Visão geral do Kerberos

O Kerberos é um protocolo de autenticação de rede de computador que permite a comunicação de clientes, nós e serviços Informatica em uma rede, para que eles se conectem uns aos outros de forma segura.

A autenticação Kerberos elimina contas nativas Informatica e dispensa a necessidade de o domínio transmitir credenciais de usuário para um servidor LDAP. Depois que você ativar a autenticação Kerberos em um domínio, os clientes Informatica usarão os tíquetes Kerberos criados durante o processo de autenticação do Windows para fazer logon nos serviços Informatica em execução nesse domínio.

Você pode ativar a autenticação Kerberos em um domínio executado em uma rede Windows. A rede deve usar o Microsoft Active Directory Domain Services (AD DS) como o banco de dados de entidades de segurança Kerberos.

Para ativar a autenticação Kerberos em um domínio Informatica, realize as seguintes etapas:

### **Prepare-se para ativar a autenticação Kerberos.**

Você deve concluir várias tarefas antes de ativar a autenticação Kerberos. As tarefas que você deve concluir incluem as seguintes:

- Crie o arquivo de configuração Kerberos.
- Crie contas para usuários de entidade de segurança Kerberos no Active Directory.
- Gere os formatos de nomes de entidade de segurança de serviço (SPN) e de keytabs.
- Crie os arquivos keytab usados para autenticar usuários e serviços na rede.

**Ative a autenticação Kerberos no domínio Informatica.**

Você pode ativar a autenticação Kerberos em um domínio Informatica ao instalar os serviços Informatica ou pode ativar a autenticação Kerberos depois de instalar os serviços. Se você não ativar a autenticação Kerberos durante a instalação, poderá usar os programas de linha de comando do Informatica para configurar o domínio para usar a autenticação Kerberos.

**Ative a autenticação Kerberos em nós e hosts de clientes Informatica.**

Depois de ativar o Kerberos no domínio, copie o arquivo de configuração Kerberos para cada nó do domínio e para cada host de cliente Informatica. Você também configura os navegadores da Web para acessar os aplicativos da Web Informatica.

**Permita que os usuários Informatica usem a autenticação Kerberos.**

Depois de ativar a autenticação Kerberos, importe usuários Informatica do Active Directory para um domínio de segurança LDAP que contenha as contas de usuário Kerberos. Você também deve migrar os grupos, as funções, os privilégios e as permissões das contas de usuários nativos para as contas de usuários no domínio de segurança LDAP.

## Como o Kerberos opera em um domínio Informatica

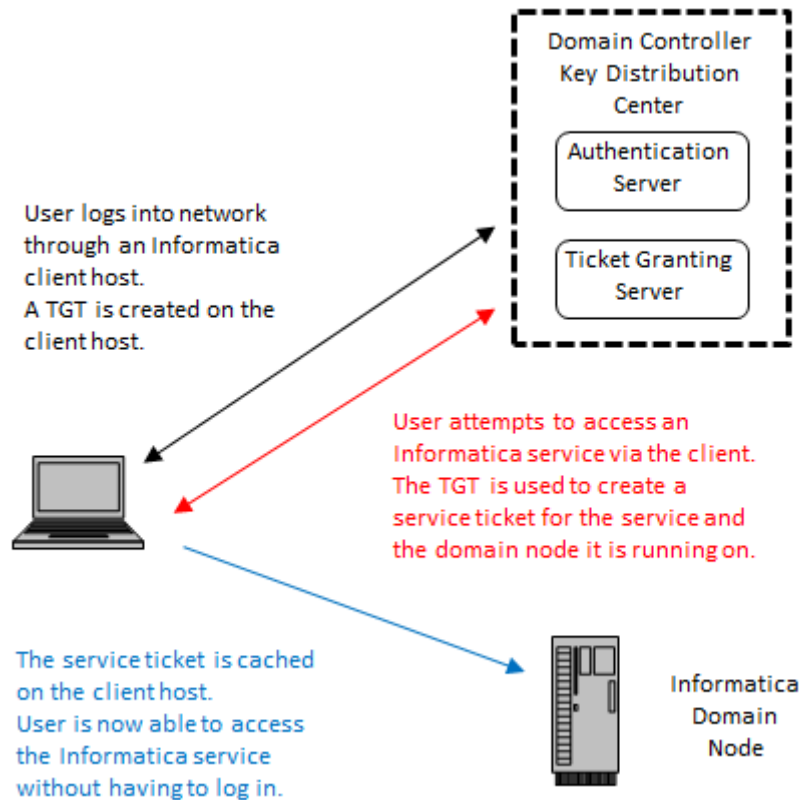
Em um domínio configurado para usar a autenticação Kerberos, os clientes Informatica se autenticam em nós e serviços de aplicativo dentro do domínio, sem a exigência de senhas.

Em um domínio que usa autenticação Kerberos, os serviços executados no domínio, incluindo processos de nós, processos de aplicativos Web e serviços de aplicativos da Informatica, são as *entidades de segurança* do Kerberos. O banco de dados da entidade de segurança do Active Directory que a região do Kerberos usa contém uma conta de usuário para cada entidade de segurança.

O protocolo de autenticação Kerberos usa *keytabs* para autenticar clientes da Informatica com serviços executados no domínio. O keytab de uma entidade de segurança é armazenado no nó em que o serviço é executado. O keytab contém o *nome da entidade de segurança do serviço (SPN)* que identifica o serviço dentro do realm Kerberos e a chave atribuída ao SPN no Active Directory.

Quando o KDC fornece um tíquete de serviço a um cliente, ele criptografa esse tíquete com a chave atribuída ao SPN. O serviço solicitado usa a chave para descriptografar o tíquete de serviço.

A seguinte imagem ilustra o fluxo básico de autenticação Kerberos:



O seguinte esquema descreve o fluxo básico de autenticação Kerberos:

1. Um usuário do cliente Informatica faz logon em um computador de rede que hospeda um cliente Informatica.
2. A solicitação de logon é direcionada ao *Servidor de Autenticação*, um componente do *Kerberos Key Distribution Center (KDC)*. O KDC é um serviço de rede com acesso a informações de contas de usuário que são executadas em cada controlador de domínio dentro do domínio Active Directory.
3. O Servidor de Autenticação verifica se o usuário existe no banco de dados de entidades de segurança e, em seguida, cria um token Kerberos chamado de *tíquete de concessão de tíquete (TGT)* no computador do usuário.
4. O usuário tenta acessar um processo ou serviço dentro do domínio Informatica por meio de um cliente Informatica.
5. O Informatica e as bibliotecas Kerberos usam o TGT para solicitar um *tíquete de serviço* e uma *chave de sessão* para o serviço solicitado do *Servidor de Concessão de Tíquete*, que também é executado no KDC.  
 Por exemplo, se o usuário acessar um Serviço de Repositório do Modelo a partir do cliente Informatica Developer, o TGT solicitará um tíquete de serviço para o nó no qual o serviço solicitado é executado. O TGT também solicita um tíquete de serviço ao Serviço de Repositório do Modelo.
6. O Kerberos usa esse tíquete de serviço para autenticar o cliente no serviço solicitado.  
 O tíquete de serviço é armazenado em cache no computador que hospeda o cliente Informatica, permitindo que o cliente use esse tíquete enquanto ele permanecer válido. Se o usuário encerrar e depois reiniciar o cliente Informatica, este reutilizará o mesmo tíquete para acessar processos e serviços no domínio Informatica.

# Autenticação de realm cruzado Kerberos

Você pode configurar um domínio Informatica para usar autenticação de realm cruzado Kerberos. A autenticação de realm cruzado Kerberos permite que os clientes da Informatica que pertencem a um realm Kerberos se autenticuem com nós e serviços de aplicativos que pertencem a outro realm Kerberos.

Ao configurar um domínio para usar a autenticação de realm cruzado Kerberos, você adiciona propriedades de cada realm Kerberos ao arquivo de configuração do Kerberos. Você também inclui o nome de cada realm ao executar comandos `infasetup` para ativar a autenticação Kerberos no domínio e nos nós de domínio.

Os servidores do Active Directory que o domínio usa para a autenticação de realm cruzado Kerberos devem pertencer à mesma floresta do Active Directory. Uma floresta do Active Directory é um grupo de domínios do Active Directory que compartilha um catálogo global, um esquema de diretório, uma estrutura lógica e uma configuração de diretório comuns. Você se conecta ao catálogo global para importar usuários dos servidores do Active Directory para domínios de segurança LDAP.

Para usar a autenticação de domínio cruzado Kerberos, a confiança bidirecional deve ser habilitada entre os servidores do Active Directory na floresta.

## Convertendo um domínio da autenticação de realm único Kerberos para a autenticação de realm cruzado Kerberos

Você pode converter um domínio Informatica que usa um único realm Kerberos para autenticar usuários para usar a autenticação de realm cruzado Kerberos.

Você deve atualizar o domínio para a versão 10.2 HotFix 2 antes de converter o domínio para usar a autenticação de realm cruzado Kerberos.

Você também deve importar contas de usuários e grupos do catálogo global do Active Directory para um domínio de segurança LDAP. Quando você importa contas, as contas existentes no domínio de segurança LDAP, que usam o atributo `samAccountName`, são excluídas e substituídas por novas contas que usam o atributo de nome da entidade de segurança do usuário.

Os usuários efetuam login nos clientes Informatica com o nome da entidade de segurança do usuário totalmente qualificado, que está no seguinte formato:

```
<nome de usuário>@<KERBEROS REALM NAME>
```

Depois de importar as contas de usuários e grupos, atribua privilégios, funções e permissões às contas.

1. Atualize o domínio para a versão 10.2 HotFix 2.
2. Adicione as propriedades necessárias para cada realm Kerberos ao arquivo de configuração do Kerberos.

Defina as propriedades para cada realm no arquivo de configuração `krb5.conf` em cada nó no domínio. Reinicie o domínio depois de atualizar o arquivo em todos os nós no domínio.

Para obter mais informações sobre como configurar o arquivo de configuração `krb5.conf` para a autenticação de realm cruzado Kerberos, consulte ["Definir o arquivo de configuração Kerberos" na página 38](#).

3. Copie o arquivo `krb5.conf` atualizado para o seguinte diretório em cada computador que hospeda um cliente Informatica:

```
<diretório de instalação Informatica>\clients\shared\security
```

4. Execute os comandos `infasetup UpdateGatewayNode` e `infasetup UpdateWorkerNode` nos nós do domínio.

Especifique o nome de cada realm Kerberos que o domínio usa para autenticar usuários como os valores das opções -srn e -urn, separados por uma vírgula.

Para obter mais informações sobre como executar os comandos infasetup, consulte o capítulo "Referência do Comando infasetup" na *Referência de Comandos do Informatica 10.2 HotFix 2*.

5. Execute o comando UpdateKerberosConfig em um nó de gateway no domínio.

Especifique o nome de cada realm Kerberos que o domínio usa para autenticar usuários como os valores das opções -srn e -urn, separados por uma vírgula.

6. Execute o comando UpdateKerberosAdminUser em um nó de gateway no domínio.

Especifique o nome da entidade de segurança do usuário totalmente qualificado para a conta do usuário administrador do domínio.

7. Importe contas de usuários e grupos para domínios de segurança LDAP.

Conecte-se ao catálogo global do Active Directory. Ao se conectar ao catálogo global, você importa usuários do servidor do Active Directory usado por cada realm Kerberos.

Para obter mais informações sobre como conectar-se ao catálogo global e importar contas, consulte ["Importar contas de usuário do Active Directory para domínios de segurança LDAP" na página 59](#).

8. Atribua privilégios, funções e permissões às contas de usuários e grupos que você importou para um domínio de segurança LDAP.

Para mais informações sobre como atribuir privilégios e funções, consulte [Capítulo 9, "Privilégios e funções" na página 144](#).

Para obter mais informações sobre como atribuir permissões, consulte [Capítulo 10, "Permissões" na página 188](#).

## Preparando-se para ativar a autenticação Kerberos

Você deve concluir várias tarefas para se preparar para ativar a autenticação Kerberos em um domínio Informatica. Os procedimentos seguidos para cada tarefa dependem do nível da entidade de segurança de serviço em que você ativa o Kerberos.

**Nota:** Não é possível desativar a autenticação Kerberos em um domínio depois de ativá-la. Você também não pode alternar o nível da entidade de segurança de serviço entre o nível de nó e o nível de processo.

## Determinar o nível da entidade de segurança de serviço Kerberos

Ao preparar-se para ativar a autenticação Kerberos, você deve determinar o nível necessário da entidade de segurança de serviço. O nível necessário da entidade de segurança de serviço determina os procedimentos que você deve seguir para preparar-se para ativar a autenticação Kerberos no domínio.

É possível ativar a autenticação Kerberos em um dos seguintes níveis:

### Nível de Nó

Se você usar o domínio para testes ou desenvolvimento, e o domínio não exigir um alto nível de segurança, será possível ativar o Kerberos em nível de nó. Você pode usar um único nome da entidade de segurança de serviço e um único arquivo keytab para o nó e para todos os processos e serviços que são executados nesse nó. Você também deve criar um SPN e um arquivo keytab para os processos HTTP que são executados no nó.

## Nível de Processo

Se você usar o domínio para produção, e ele exigir alto nível de segurança, será possível definir a entidade de segurança de serviço em nível de processo. Você cria um SPN e um arquivo keytab exclusivos para cada nó e cada processo no nó. Você também deve criar um SPN e um arquivo keytab para os processos HTTP que são executados no nó.

O Kerberos ativado em nível de processo fornece o mais alto nível de segurança, mas pode ser difícil de gerenciar em um domínio Informatica que contenha muitos nós ou serviços. Nesse cenário, talvez você queira ativar o Kerberos em nível de nó.

## Definir o arquivo de configuração Kerberos

Defina as propriedades exigidas pelo Informatica no arquivo de configuração Kerberos e, em seguida, copie esse arquivo para cada nó do domínio Informatica.

O Kerberos armazena informações de configuração em um arquivo denominado *krb5.conf*. Você deve definir as propriedades no arquivo de configuração *krb5.conf* e, em seguida, copiar esse arquivo para cada nó do domínio Informatica.

Se o domínio usar a autenticação de realm cruzado Kerberos, insira as propriedades necessárias para cada realm Kerberos.

1. Configure as seguintes propriedades da biblioteca Kerberos na seção *libdefaults* do arquivo.

A seguinte tabela descreve as propriedades a serem inseridas:

Propriedade	Descrição
default_realm	Nome do realm Kerberos ao qual os serviços do domínio Informatica pertencem. O nome do realm deve estar em maiúsculas.  Se o domínio usar um único realm Kerberos para autenticação, o nome do realm do serviço e o nome do realm do usuário deverão ser iguais.
encaminável	Permite que um serviço delegue credenciais de usuário do cliente para outro serviço. O domínio Informatica exige que os serviços de aplicativo autenticuem as credenciais de usuário do cliente com outros serviços.  Defina como true.
default_tkt_enctypes	Tipos de criptografia para a chave da sessão incluída em TGTs (tíquetes de concessão de tíquete). Defina essa propriedade somente se as chaves de sessão tiverem que usar tipos de criptografia específicos. Certifique-se de que o KDC (Centro de Distribuição de Chaves) Kerberos ofereça suporte ao tipo de criptografia que você especificar.  Não defina essa propriedade para permitir que o protocolo Kerberos selecione o tipo de criptografia a ser usado.  Se os hosts de nó ou os hosts de clientes Informatica usarem a criptografia de 256 bits, instale os arquivos de diretiva de força ilimitada JCE (Java Cryptography Extension) em todos os hosts de nós e hosts de clientes Informatica, para evitar problemas de autenticação.
rdns	Determina se a pesquisa de nomes inversa é usada além da pesquisa de nomes direta para canonizar nomes de host para uso em nomes de entidades de segurança de serviço.  Defina como false.
renew_lifetime	A vida útil renovável padrão para solicitações de tíquetes iniciais.

Propriedade	Descrição
ticket_lifetime	A vida útil padrão para solicitações de tíquetes iniciais.
udp_preference_limit	Determina o protocolo usado pelo Kerberos ao enviar uma mensagem ao KDC. Defina como 1 para usar o protocolo TCP se o domínio apresentar falhas de autenticação Kerberos intermitentes.
dns_lookup_kdc	Indica se o cliente Kerberos usa registros SRV do DNS para localizar os KDCs e outros servidores de um realm, caso eles não estejam listados nas informações do realm. O DNS usa registros SRV para identificar computadores que hospedam serviços específicos. Necessário quando o domínio está ativado para Kerberos. Requer que você defina a propriedade de realm admin_server. Defina como true.
dns_lookup_realm	Indica se o cliente Kerberos usa registros TXT do DNS para determinar o realm Kerberos de um host. O DNS usa texto ou registros TXT para associar texto arbitrário a um host ou outro nome, como informações legíveis por humanos sobre um servidor, uma rede, um datacenter ou outras informações contábeis. Necessário quando o domínio está ativado para Kerberos. Defina como true.

- Defina cada realm Kerberos na seção *realms* do arquivo.

O exemplo a seguir mostra a entrada para um realm Kerberos chamado COMPANY.COM:

```
[realms]
COMPANY.COM = {...}
```

- Insira as propriedades de realm a seguir dentro dos colchetes para cada realm Kerberos na seção *realms* do arquivo.

A seguinte tabela descreve as propriedades a serem inseridas:

Propriedade	Descrição
admin_server	O nome ou o endereço IP do host do servidor de administração Kerberos. Você pode incluir um número de porta opcional, separado do nome do host por dois um caractere de dois pontos. O padrão é 749. Necessário se você configurar dns_lookup_kdc na seção <i>libdefaults</i> .
kdc	O nome ou endereço IP de um host que executa o KDC (Centro de Distribuição de Chaves) para o realm. Você pode incluir um número de porta opcional, separado do nome do host por dois um caractere de dois pontos. O padrão é 88.

O exemplo a seguir mostra as entradas para cada realm Kerberos em uma configuração de realm cruzado Kerberos:

```
[realms]
COMPANY.COM = {
  admin_server = KDC01.COMPANY.COM:749
  kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
  kdc = 10.75.141.193
  admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
```

```
kdc = 10.78.140.111
admin_server = 10.78.140.111
}
```

4. Na seção *domain\_realms*, mapeie o nome do domínio ou nome do host para um nome de realm Kerberos. O nome do domínio é precedido por um ponto (.).

O exemplo a seguir mostra os parâmetros para o domain\_realm Hadoop se o domínio Informatica não usar a autenticação Kerberos:

```
[domain_realm]
.hadoop_realms.com = HADOOP-REALM
hadoop_realms.com = HADOOP-REALM
```

O exemplo a seguir mostra os parâmetros para o domain\_realm Hadoop se o domínio Informatica não usar a autenticação Kerberos:

```
[domain_realms]
.infa_ad_realms.com = INFA-AD-REALM
infa_ad_realms.com = INFA-AD-REALM
.hadoop_realms.com = HADOOP-REALM
hadoop_realms.com = HADOOP-REALM
```

5. Copie o arquivo *krb5.conf* para as seguintes localizações na máquina que hospeda o Serviço de Integração de Dados:

- <diretório de instalação Informatica>/services/shared/security
- <diretório de instalação Informatica>/java/jre/lib/security/

O exemplo a seguir mostra o conteúdo de um arquivo de configuração do Kerberos com as propriedades necessárias para uma configuração de realm único Kerberos:

```
[libdefaults]
default_realms = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realms = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}

[domain_realms]
.company.com = COMPANY.COM
company.com = COMPANY.COM
```

O exemplo a seguir mostra o conteúdo de um arquivo de configuração do Kerberos com as propriedades necessárias para uma configuração de realm cruzado Kerberos:

```
[libdefaults]
default_realms = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realms = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}
```



```

EAST.COMPANY.COM = {
kdc = 10.75.141.193
admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
kdc = 10.78.140.111
admin_server = 10.78.140.111

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
.east.company.com = EAST.COMPANY.COM
east.company.com = EAST.COMPANY.COM
.west.company.com = WEST.COMPANY.COM
west.company.com = WEST.COMPANY.COM

```

Para obter mais informações sobre o arquivo de configuração Kerberos, consulte a documentação da autenticação de rede Kerberos.

## Criar contas de entidade de segurança Kerberos no Active Directory

Crie contas de usuário LDAP para as entidades de segurança Kerberos no Active Directory. Uma entidade de segurança Kerberos é um processo, serviço ou usuário dentro do realm Kerberos.

Se você definir a propriedade `default_tkt_enctypes` no arquivo de configuração `krb5.conf` como os tipos de criptografia AES de 128 bits ou 256 bits, configure cada conta para usar o tipo de criptografia correspondente no Active Directory.

As contas criadas dependem da sua opção por ativar o Kerberos em nível de nó ou em nível de processo.

**Nota:** Nomes de contas podem ter no máximo 20 caracteres.

### Contas Necessárias no Nível do Nó

Crie as contas de usuário LDAP necessárias para ativar a autenticação Kerberos em nível de nó no Active Directory.

Crie as seguintes contas de entidades de segurança do Kerberos no Active Directory se você ativar o Kerberos em nível de nó:

#### Processos de nó

Crie uma conta para cada nó que é executado no domínio.

#### Processo HTTP

Crie uma conta para os aplicativos da Web Informatica que são executados em um nó do domínio. Os aplicativos da Web executados em um nó podem incluir a ferramenta Administrator, o Informatica Analyst e o Catalog Administrator. Crie uma única conta compartilhada por todos os aplicativos da Web em execução no nó.

#### Nome Diferenciado (DN) do Usuário de Associação

Crie uma conta de usuário de associação LDAP que você utilizará para sincronizar o domínio de segurança LDAP que contém contas de usuário Kerberos com o Active Directory.

## Contas Necessárias em Nível de Processo

Crie as contas de usuário LDAP necessárias para ativar a autenticação Kerberos em nível de processo no Active Directory.

Crie as seguintes contas de entidades de segurança do Kerberos no Active Directory se você ativar o Kerberos em nível de processo:

### Processos de nó

Crie uma conta para cada nó que é executado no domínio.

### Processos HTTP

Crie uma conta para os aplicativos da Web Informatica que são executados em um nó do domínio. Os aplicativos da Web executados em um nó podem incluir o Informatica Analyst e o Catalog Administrator. Crie uma única conta compartilhada por todos os aplicativos da Web em execução no nó.

### Serviço Informatica Administrator

Crie uma conta para a ferramenta Administrator em cada nó de gateway no domínio.

### Serviços de aplicativo Informatica

Crie uma conta para cada serviço de aplicativo Informatica executado em cada nó do domínio.

### Nome Diferenciado (DN) do Usuário de Associação

Crie uma conta de usuário LDAP que você utilizará para sincronizar o domínio de segurança LDAP que contém contas de usuário Kerberos com o Active Directory.

## Gerar os formatos do nome da entidade de segurança de serviço e do nome do arquivo keytab

Use o utilitário Gerador de Formatos de SPN Kerberos da Informatica para gerar os formatos de SPNs (nomes de entidades de segurança de serviço) e de nomes de arquivos keytab necessários para usar a autenticação Kerberos. O utilitário Gerador de Formatos de SPN Kerberos da Informatica gera um arquivo de texto chamado SPNKeytabFormat.txt, que contém o formato correto para os SPNs e os nomes de arquivos keytab.

Os formatos de SPNs e nomes de arquivos keytab gerados dependem da sua opção por ativar o Kerberos em nível de nó ou em nível de processo.

## Gerar os formatos do nome da entidade de segurança de serviço e do nome do arquivo keytab em nível de nó

Gere os formatos para os SPNs e os nomes de arquivos keytab necessários para ativar a autenticação Kerberos em nível de nó.

O domínio Informatica requer SPNs e arquivos keytab para os seguintes processos quando você ativa a autenticação Kerberos em nível de nó:

### Processos de nó

A Informatica requer um SPN e um arquivo keytab para cada nó do domínio. O Kerberos usa o mesmo nome de entidade de segurança de serviço e keytab para autenticar os serviços de aplicativo Informatica que são executados no nó.

## Processos HTTP

A Informatica requer um SPN e um arquivo keytab para os aplicativos Web que são executados em cada nó do domínio. Os aplicativos da Web executados em um nó podem incluir a ferramenta Administrator, o Informatica Analyst e o Catalog Administrator. O Kerberos usa o mesmo nome de entidade de segurança de serviço para autenticar todos os aplicativos da Web que são executados no nó.

1. Em um host de nó Informatica do Windows, acesse o diretório que contém o arquivo de lote SPNFormatGenerator.bat:

```
<diretório de instalação Informatica>\tools\Kerberos
```

Em um host de nó Informatica do UNIX, acesse o diretório que contém o arquivo de shell SPNFormatGenerator.sh:

```
<diretório de instalação Informatica>/tools/Kerberos
```

2. Execute SPNFormatGenerator.bat ou SPNFormatGenerator.sh.
3. Clique em **Avançar**.
4. Selecione **Nível de Nó**.
5. Clique em **Avançar**.
6. Insira as propriedades necessárias para gerar os formatos de SPN e arquivo keytab.

A seguinte tabela descreve as propriedades:

Aviso	Descrição
Nome do Domínio	Nome do domínio Informatica. O nome não deve exceder 128 caracteres e deve ser ASCII de 7 bits. Ele não pode conter espaço nem qualquer um dos seguintes caracteres: ` % * + ; " ? , < > \ /
Nome do Realm de Serviço	Nome do realm Kerberos. O nome do realm deve estar em maiúsculas.
Nome do nó	Nome do nó da Informatica.
Nome de Host do Nó	Nome totalmente qualificado do host do nó. O nome de host do nó não pode conter o caractere sublinhado (_). <b>Nota:</b> Não use <i>localhost</i> . O nome do host deve identificar explicitamente o host.

7. Para gerar o formato de SPN adicional de um nó, clique em **+Nó** e especificar o nome do nó e o nome do host.

A seguinte imagem mostra as entradas para vários nós do domínio InfaDomain no utilitário Gerador de Formatos de SPN:

Informatica Kerberos SPN Format Generator

Authentication Parameters - Kerberos Authentication - Step 3 of 4

Specify the domain and Kerberos authentication parameters.

Domain name: InfaDomain

Service realm name: COMPANY.COM

Node name: node01

Node host name: JS001DEV

+Node -Node

Node name: node02

Node host name: JS005DEV

< Previous Next > Cancel

8. Clique em **Avançar**.  
O utilitário Gerador de Formatos de SPN exibe o caminho e o nome do arquivo que contém a lista de nomes de entidades de segurança de serviço e nomes de arquivos keytab.
9. Clique em **Concluir** para sair do utilitário SPN Format Generator.

## Gerar os formatos de nomes de entidades de segurança de serviço e de nomes de arquivos keytab em nível de processo

Gere os formatos para os SPNs e os nomes de arquivos keytab necessários para ativar a autenticação Kerberos em nível de processo.

O domínio Informatica requer SPNs e arquivos keytab para os seguintes processos e serviços quando você ativa a autenticação Kerberos em nível de processo:

### Processos de nó

A Informatica requer um SPN e um arquivo keytab para cada nó do domínio.

### Informatica Administrator

A Informatica requer um SPN e um arquivo keytab na ferramenta Administrator para cada nó de gateway do domínio.

## Processos HTTP

A Informatica requer um SPN e um arquivo keytab para os aplicativos Web que são executados em um nó do domínio. Os aplicativos da Web executados em um nó podem incluir o Informatica Analyst e o Catalog Administrator.

## Processos de serviços de aplicativo Informatica

A Informatica requer um SPN e um arquivo keytab para cada serviço de aplicativo Informatica que é executado em cada nó do domínio.

1. Em um host de nó Informatica do Windows, acesse o diretório que contém o arquivo de lote SPNFormatGenerator.bat:

```
<diretório de instalação Informatica>\tools\Kerberos
```

Em um host de nó Informatica do UNIX, acesse o diretório que contém o arquivo de shell SPNFormatGenerator.sh:

```
<diretório de instalação Informatica>/tools/Kerberos
```

2. Execute SPNFormatGenerator.bat ou SPNFormatGenerator.sh.
3. Clique em **Avançar**.
4. Selecione **Nível de Processo**.
5. Clique em **Avançar**.
6. Insira as propriedades necessárias para gerar os formatos de SPN e arquivo keytab.

A seguinte tabela descreve as propriedades:

Aviso	Descrição
Nome do Domínio	Nome do domínio Informatica. O nome não deve exceder 128 caracteres e deve ser ASCII de 7 bits. Ele não pode conter espaço nem qualquer um dos seguintes caracteres: ` % * + ; " ? , < > \ /
Nome do Realm de Serviço	Nome do realm Kerberos. O nome do realm deve estar em maiúsculas.
Nome do nó	Nome do nó da Informatica.
Nome de Host do Nó	Nome totalmente qualificado ou endereço IP do host do nó. O nome do host do nó não pode conter o caractere de sublinhado (_). <b>Nota:</b> Não use <i>localhost</i> . O nome do host deve identificar explicitamente o host.

7. Para gerar o formato do SPN para um serviço de aplicativo Informatica que é executado em um nó, clique em **Serviço** depois de inserir os detalhes do nó.

Insira o nome do serviço de aplicativo Informatica, conforme mostrado na ferramenta Administrator. Conclua essa etapa para cada serviço de aplicativo Informatica executado em cada nó do domínio.

8. Para gerar o formato de SPN adicional de um nó, clique em **+Nó** e especificar o nome do nó e o nome do host.

A seguinte imagem mostra as entradas para vários nós e serviços de aplicativo que são executados no domínio InfaDomain no utilitário Gerador de Formatos de SPN:

Informatica Kerberos SPN Format Generator

Authentication Parameters - Kerberos Authentication - Step 3 of 4

Specify the domain and Kerberos authentication parameters.

Domain name: InfaDomain

Service realm name: COMPANY.COM

Node name: node01

Node host name: JS001DEV

Service on node: MRS\_dev

Service on node: DIS\_dev

Node name: node02

Node host name: JS005DEV

Service on node: CMS\_dev

+Node +Service -Node

< Previous Next > Cancel

9. Clique em **Avançar**.

O utilitário Gerador de Formatos de SPN exibe o caminho e o nome do arquivo que contém a lista de nomes de entidades de segurança de serviço e nomes de arquivos keytab.

10. Clique em **Concluir** para sair do utilitário SPN Format Generator.

## Examinar o arquivo de texto de formatos de nomes de entidades de segurança de serviço e nomes de arquivos keytab

Depois de gerar o arquivo SPNKeytabFormat.txt, você pode examinar esse arquivo.

Use as informações nesse arquivo para gerar os arquivos keytab e para associar cada SPN à conta de usuário de entidade de segurança correspondente no Active Directory.

O arquivo SPNKeytabFormat.txt contém as seguintes informações:

### Nome da Entidade

Identifica o nó ou o serviço associado ao processo.

### Nome da entidade de segurança de serviço

Formato do SPN. O SPN faz distinção entre maiúsculas e minúsculas.

**Nota:** Se você inserir uma cadeia contendo vários nomes de domínio Kerberos ou incluir um asterisco antes de um sufixo do realm para incluir todos os realms que incluam o sufixo, o formato SPN não incluirá o nome do realm.

A seguinte tabela descreve os formatos de SPN:

Tipo de keytab	Formato do SPN
NODE_SPN	isp/<nome do nó>/<nome do domínio>@<REALM NAME>
NODE_AC_SPN	_AdminConsole/<nome do nó>/<nome do domínio>@<REALM NAME>
NODE_HTTP_SPN	HTTP/<nome do host do nó>@<REALM NAME> <b>Nota:</b> O Kerberos SPN Format Generator valida o nome do host do nó. Se o nome do host do nó não for válido, o utilitário não gerará um SPN. Em vez disso, ele exibirá a seguinte mensagem: Não é possível resolver o nome do host.
SERVICE_PROCESS_SPN	<nome do serviço de aplicativo>/<nome do nó>/<nome do domínio>@<REALM NAME>

### Nome do Arquivo Keytab

Formato do nome do arquivo keytab a ser criado para o SPN associado. O nome de arquivo keytab faz distinção entre maiúsculas e minúsculas.

A seguinte tabela descreve os formatos de nomes de arquivo keytab:

Tipo de keytab	Nome de Arquivo Keytab
NODE_SPN	<nome do nó>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<nome do serviço de aplicativo>.keytab

### Entidades de Serviço em Nível de Nó

A seguinte imagem mostra o conteúdo do arquivo SPNKeytabFormat.txt gerado para as entidades de segurança de serviço em nível de nó:

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN

### Principal de Serviço em Nível de Processo

A seguinte imagem mostra o conteúdo do arquivo SPNKeytabFormat.txt gerado para as entidades de segurança de serviço em nível de processo:

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	_AdminConsole/node01/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	_AdminConsole/node02/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
MRS_dev:node01	MRS_dev/node01/Infadomain@COMPANY.COM	MRS_dev.keytab	SERVICE_PROCESS_SPN
DIS_dev:node01	DIS_dev/node01/Infadomain@COMPANY.COM	DIS_dev.keytab	SERVICE_PROCESS_SPN
CAT_dev:node02	CAT_dev/node02/Infadomain@COMPANY.COM	CAT_dev.keytab	SERVICE_PROCESS_SPN

## Gerar os arquivos keytab

Gere os arquivos keytab usados para autenticar usuários e serviços Informatica.

Você pode usar o utilitário ktpass do Microsoft Windows Server para gerar um arquivo keytab para cada conta de usuário criada no Active Directory. Você deve gerar os arquivos keytab em um servidor membro ou em um controlador de domínio dentro do domínio Active Directory. Não é possível gerar arquivos keytab em um sistema operacional de estação de trabalho, como o Microsoft Windows 7.

Para usar ktpass de forma a gerar um arquivo keytab, execute o seguinte comando:

```
ktpass.exe -out <keytab filename> -princ <service principal name> -mapuser <user account> [-pass <user account password>] -crypto <key types> -ptype <principal type> [-target <realm name>]
```

A tabela a seguir descreve as opções de comando:

Opção	Descrição
-out	O nome do arquivo keytab Kerberos a ser gerado, conforme mostrado na coluna KEY_TAB_NAME no arquivo SPNKeytabFormat.txt.
-princ	O nome da entidade de segurança de serviço que consta na coluna SPN no arquivo SPNKeytabFormat.txt. Se o domínio usar a autenticação de realm cruzado Kerberos, o nome da entidade de segurança do serviço deverá ser exclusivo em todos os realms Kerberos.
-mapuser	A conta de usuário Active Directory a ser associada ao SPN. O nome da conta pode ter no máximo 20 caracteres.
-pass	A senha definida no Active Directory para a conta de usuário Active Directory, se aplicável.
-crypto	Especifica os tipos de chaves gerados no arquivo keytab. Defina como all para usar todos os tipos de criptografia com suporte.
-ptype	O tipo da entidade de segurança. Defina como KRB5_NT_PRINCIPAL.
-target	O nome do realm ao qual o servidor do Active Directory pertence. Inclua essa opção se o seguinte erro ocorrer quando você executar o utilitário: DsCrackNames retornou 0x2 no nome

Os arquivos keytab gerados dependem da sua opção por ativar o Kerberos em nível de nó ou em nível de processo.

## Gerar arquivos keytab em nível de nó

Quando executa ktpass para gerar os arquivos keytab em nível de nó, você associa cada conta de usuário de entidade de segurança Kerberos ao SPN correspondente no Active Directory.

A seguinte tabela mostra a associação entre as contas de usuário de entidades de segurança Kerberos e os SPNs mostrados no arquivo de exemplo SPNKeytabFormat.txt:

Conta de usuário	Tipo de keytab	Nome da entidade de segurança de serviço
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM



Conta de usuário	Tipo de keytab	Nome da entidade de segurança de serviço
nodeuser02	NODE_SPN	isp/node02/InfraDomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

Você também cria um keytab para a conta de usuário de associação LDAP que é usada para acessar e pesquisar o Active Directory durante a sincronização LDAP.

1. Crie um arquivo keytab para a conta de usuário de entidade de segurança Kerberos que você criou para cada nó do Active Directory.

Copie o nome do arquivo keytab da coluna `KEY_TAB_NAME` no arquivo `SPNKeytabFormat.txt`. Copie o nome da entidade de segurança do serviço da coluna `SPN` no arquivo `SPNKeytabFormat.txt`.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança Kerberos chamada `nodeuser01`:

```
ktpass.exe -out node01.keytab -princ isp/node01/InfraDomain/COMPANY.COM -mapuser
nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. Crie um arquivo keytab para cada conta de usuário de entidade de segurança Kerberos de processo HTTP que você criou no Active Directory.

Se o domínio usar a autenticação de realm cruzado Kerberos, a conta do usuário da entidade de segurança poderá existir em qualquer realm Kerberos que o domínio usar.

Copie o nome do arquivo keytab da coluna `KEY_TAB_NAME` no arquivo `SPNKeytabFormat.txt`. Copie o nome da entidade de segurança do serviço da coluna `SPN` no arquivo `SPNKeytabFormat.txt`.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança Kerberos chamada `httpuser01`:

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser
httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. Crie um keytab para a conta de usuário de associação LDAP que é usada para acessar e pesquisar o Active Directory durante a sincronização LDAP.

Estruture o valor da opção `-princ` como `<nome da entidade de segurança>@<KERBEROS REALM>`. Inclua o nome da configuração do LDAP do servidor Active Directory no nome do arquivo keytab. Estruture o nome do arquivo keytab da seguinte maneira: `<configuration_name do LDAP do Active Directory>.keytab`.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança de serviço chamada `ldapuser`:

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser
ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

## Gerar os arquivos keytab em nível de processo

Quando executa ktpass para gerar os arquivos keytab em nível de processo, você associa cada conta de usuário de entidade de segurança Kerberos ao SPN correspondente no Active Directory.

A seguinte tabela mostra a associação entre as contas de usuário de entidades de segurança Kerberos e os SPNs mostrados no arquivo de exemplo SPNKeytabFormat.txt:

Conta de usuário	Tipo de keytab	Nome da entidade de segurança de serviço
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/InfaDomain@COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/InfaDomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/InfaDomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/InfaDomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/InfaDomain@COMPANY.COM

Você também cria um keytab para a conta de usuário de associação LDAP que é usada para acessar e pesquisar o Active Directory durante a sincronização LDAP.

1. Crie um arquivo keytab para a conta de usuário de entidade de segurança Kerberos que você criou para cada nó do Active Directory.

Copie o nome do arquivo da coluna **KEY\_TAB\_NAME** no arquivo SPNKeytabFormat.txt. Copie o nome da entidade de segurança do serviço da coluna **SPN** no arquivo SPNKeytabFormat.txt.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança Kerberos chamada nodeuser01:

```
ktpass.exe -out node01.keytab -princ isp/node01/InfaDomain/COMPANY.COM -mapuser  
nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. Crie um arquivo keytab para cada conta de usuário de entidade de segurança Kerberos de processo HTTP que você criou.

Se o domínio usar a autenticação de realm cruzado Kerberos, a conta do usuário da entidade de segurança poderá existir em qualquer realm Kerberos que o domínio usar.

Copie o nome do arquivo da coluna **KEY\_TAB\_NAME** no arquivo SPNKeytabFormat.txt. Copie o nome da entidade de segurança do serviço da coluna **SPN** no arquivo SPNKeytabFormat.txt.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança Kerberos chamada httpuser01:

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser  
httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. Crie um arquivo keytab para cada conta de usuário de entidade de segurança Kerberos da ferramenta Administrator que você criou.

Copie o nome do arquivo da coluna `KEY_TAB_NAME` no arquivo `SPNKeytabFormat.txt`. Copie o nome da entidade de segurança do serviço da coluna `SPN` no arquivo `SPNKeytabFormat.txt`.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança Kerberos chamada `admintooluser01`:

```
ktpass.exe -out _AdminConsole.keytab -princ _AdminConsole/node01/InfraDomain@COMPANY.COM -mapuser admintooluser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

4. Crie um arquivo keytab para cada conta de usuário de entidade de segurança Kerberos de serviço de aplicativo Informatica que você criou.

Copie o nome do arquivo da coluna `KEY_TAB_NAME` no arquivo `SPNKeytabFormat.txt`. Copie o nome da entidade de segurança do serviço da coluna `SPN` no arquivo `SPNKeytabFormat.txt`.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança Kerberos de serviço chamada `MRSdevuser01`:

```
ktpass.exe -out MRS_dev.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser MRSdevuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

5. Crie um keytab para a conta de usuário de associação LDAP que é usada para acessar e pesquisar o Active Directory durante a sincronização LDAP.

Estruture o valor da opção `-princ` como `<nome da entidade de segurança>@<KERBEROS REALM>`. Inclua o nome da configuração do LDAP do servidor Active Directory no nome do arquivo keytab. Estruture o nome do arquivo keytab da seguinte maneira: `<configuration_name do LDAP do Active Directory>.keytab`.

O seguinte exemplo cria um arquivo keytab para uma conta de usuário de entidade de segurança de serviço chamada `ldapuser`:

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

## Verificar os nomes de entidades de segurança de serviço e arquivos keytab

Você pode usar os utilitários Kerberos para verificar se os SPNs e os arquivos keytab são válidos. Você também pode usar os utilitários para determinar o status do KDC (Centro de Distribuição de Chaves).

É possível usar os utilitários Kerberos *kinit* e *klist* para exibir e verificar os arquivos SPN e keytab. Para usar os utilitários, certifique-se de que a variável de ambiente `KRB5_CONFIG` contenha o caminho e o nome do arquivo de configuração Kerberos. Para obter mais informações sobre como executar os utilitários Kerberos, consulte a documentação Kerberos.

Use os seguintes utilitários para verificar os SPNs e os arquivos keytab:

### **kinit**

Você pode usar o utilitário *kinit* para solicitar um tíquete de concessão de tíquete (TGT) do KDC e verificar se um arquivo keytab pode ser usado para estabelecer uma conexão Kerberos. Se o keytab e SPN especificado forem válidos, o comando obterá um tíquete e, em seguida, o armazenará no cache especificado.

O utilitário *kinit* está disponível no seguinte diretório em um nó Informatica:

```
<diretório de instalação Informatica>\java\jre\bin
```

Para solicitar uma concessão de tíquete para um SPN, execute o seguinte comando:

```
kinit -c <nome do cache> -k -t <nome do arquivo keytab> <nome da entidade de segurança de serviço>
```

O seguinte exemplo de saída mostra a concessão de tíquete criada no cache padrão para um arquivo keytab especificado e um SPN:

```
Cache: \temp\krb Usando a entidade de segurança: isp/node01/Infadomain/COMPANY.COM
Usando o keytab: node01.keytab Autenticado no Kerberos v5
```

#### klist

Você pode usar o utilitário *klist* para listar as entidades de segurança Kerberos e as chaves em um arquivo keytab. Para listar as chaves no arquivo keytab e o registro de data/hora da entrada keytab, execute o seguinte comando:

```
klist -k -t <nome do arquivo keytab>
```

O seguinte exemplo de saída mostra as entidades de segurança em um arquivo keytab:

```
Nome do Keytab: FILE:node01.keytab KVNO Registro de data/hora Entidade de segurança
----- 3
12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/
node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/
Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM
```

## Ativando a autenticação Kerberos

Você pode ativar a autenticação Kerberos em um domínio Informatica ao instalar os serviços Informatica ou pode ativar a autenticação Kerberos depois de instalar os serviços.

Se você não ativar a autenticação Kerberos durante a instalação, siga as etapas desta seção para usar os programas de linha de comando Informatica de forma a ativar a autenticação Kerberos depois de instalar os serviços.

### Ativar a autenticação Kerberos no domínio

Ative o Kerberos em um nó de gateway dentro do domínio.

Execute o comando `infasetup switchToKerberosMode` em um nó de gateway dentro do domínio para alterar a autenticação para a autenticação de rede Kerberos.

1. Encerre o domínio e todos os serviços Informatica. Encerre os serviços na seguinte ordem:

- Serviço do Metadata Manager
- Serviço de Integração do PowerCenter®
- Serviço do Repositório do PowerCenter®
- Serviço do Gerenciamento de Conteúdo
- Serviço Analyst
- Serviço de Integração de Dados
- Serviço de Repositório do Modelo

2. No prompt de comando de um nó de gateway, alterne para o diretório em que o executável `infasetup` está localizado:

```
<diretório de instalação Informatica>\isp\bin
```

3. Execute o seguinte comando:

```
infasetup switchToKerberosMode -ad <administrador name> -srn <Kerberos realm names> -
urn <Kerberos realm names> -spnSL <service principal level>
```

A seguinte tabela descreve as opções e os argumentos para o comando `infasetup switchToKerberosMode`:

Opção	Argumento	Descrição
-administratorName -ad	user_name	<p>Nome de usuário da conta de administrador de domínio criada quando você configura a autenticação Kerberos. Especifique o nome de uma conta que existe no Active Directory.</p> <p>Após a configuração da autenticação Kerberos, esse usuário é incluído no domínio de segurança <code>_infalInternalNamespace</code> que é criado por esse comando.</p> <p>Se o domínio usar um único realm Kerberos para autenticar usuários, especifique o nome <code>samAccount</code> da conta que você deseja usar como conta de administrador.</p> <p>Se o domínio usar a autenticação de realm cruzado Kerberos, especifique o nome da entidade de segurança do usuário totalmente qualificado da conta que você deseja usar como a conta do administrador, incluindo o nome do realm. Por exemplo: <code>sysadmin@COMPANY.COM</code></p>
-ServiceRealmName -srn	Kerberos_realm_name	<p>Nome do realm Kerberos que o domínio usa para autenticar usuários. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas.</p> <p>Para configurar a autenticação de realm cruzado Kerberos, especifique o nome de cada realm Kerberos que o domínio usa para autenticar usuários, separados por uma vírgula. Por exemplo: <code>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</code></p> <p>Use um asterisco como um caractere curinga antes de um nome de realm para incluir todos os realms que incluem o nome. Por exemplo: <code>*EAST.COMPANY.COM</code></p>

Opção	Argumento	Descrição
-UserRealmName -urn	Kerberos_realm_name	<p>Nome do realm Kerberos que o domínio usa para autenticar usuários. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas.</p> <p>Para configurar a autenticação de realm cruzado Kerberos, especifique o nome de cada realm Kerberos que o domínio usa para autenticar usuários, separados por uma vírgula. Por exemplo:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Use um asterisco como um caractere curinga antes de um nome de realm para incluir todos os realms que incluem o nome. Por exemplo:</p> <p>*EAST.COMPANY.COM</p>
-SPNShareLevel -spnSL	NODE PROCESS	<p>Nível da entidade de segurança de serviço do domínio.</p> <p>Defina como NODE para ativar o Kerberos em nível de nó.</p> <p>Defina como PROCESS para ativar o Kerberos em nível de processo.</p>

O exemplo a seguir altera a autenticação de domínio para o Kerberos e define a conta de usuário sysadmin como a conta de administrador em um domínio que usa um único realm Kerberos para autenticar usuários:

```
infasetup switchToKerberosMode -ad sysadmin -srn COMPANY.COM -urn COMPANY.COM -spnSL
NODE
```

O exemplo a seguir altera a autenticação de domínio para o Kerberos e define a conta de usuário sysadmin como a conta de administrador em um domínio que usa a autenticação de realm cruzado Kerberos:

```
infasetup switchToKerberosMode -ad sysadmin@COMPANY.COM -srn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -spnSL NODE
```

## Atualizar os Nós no Domínio

Atualize todos os nós de gateway e do funcionário com as informações do servidor de autenticação Kerberos, exceto os nós de gateway nos quais você executou o comando `infasetup switchToKerberosMode`.

Use os seguintes comandos para atualizar o gateway e os nós do funcionário:

### **infasetup UpdateGatewayNode**

Use o comando `UpdateGatewayNode` para definir os parâmetros de autenticação Kerberos em um nó de gateway no domínio. Se o domínio tiver vários nós de gateway, execute o comando `UpdateGatewayNode` em cada nó de gateway.

## infasetup UpdateWorkerNode

Use o comando UpdateWorkerNode para definir os parâmetros de autenticação Kerberos em um nó de trabalho no domínio. Se o domínio tiver vários nós de trabalho, execute o comando UpdateWorkerNode em cada nó de trabalho.

1. No prompt de comando de um nó, alterne para o diretório em que o executável infasetup está localizado:

```
<diretório de instalação Informatica>\isp\bin
```

2. Para definir os parâmetros de autenticação Kerberos em um nó de gateway, execute o seguinte comando:

```
infasetup UpdateGatewayNode -krb <true|false> -srn <Kerberos realm names> -urn  
<Kerberos realm names>
```

Para definir os parâmetros de autenticação Kerberos em um nó do funcionário, execute o seguinte comando:

```
infasetup UpdateWorkerNode -krb <true|false> -srn <Kerberos realm names> -urn  
<Kerberos realm names>
```

A seguinte tabela descreve as opções e os argumentos necessários para ativar a autenticação Kerberos em um nó:

Opção	Argumento	Descrição
-EnableKerberos -krb	verdadeiro falso	Configura o domínio Informatica para usar a autenticação Kerberos.  Defina como true para ativar a autenticação Kerberos. O padrão é Falso.
-ServiceRealmName -srn	Kerberos_realm_name	Nome do realm Kerberos que o domínio usa para autenticar usuários. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas.  Para configurar a autenticação de realm cruzado Kerberos, especifique o nome de cada realm Kerberos que o domínio usa para autenticar usuários, separados por uma vírgula. Por exemplo:  COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM  Use um asterisco como um caractere curinga antes de um nome de realm para incluir todos os realms que incluem o nome. Por exemplo:  *EAST.COMPANY.COM
-UserRealmName -urn	Kerberos_realm_name	Nome do realm Kerberos que o domínio usa para autenticar usuários. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas.  Para configurar a autenticação de realm cruzado Kerberos, especifique o nome de cada realm Kerberos que o domínio usa para autenticar usuários, separados por uma vírgula. Por exemplo:  COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM  Use um asterisco como um caractere curinga antes de um nome de realm para incluir todos os realms que incluem o nome. Por exemplo:  *EAST.COMPANY.COM

O exemplo a seguir atualiza um nó do funcionário para usar a autenticação Kerberos:

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM -urn COMPANY.COM
```

O exemplo a seguir atualiza um nó do funcionário para usar a autenticação de realm cruzado Kerberos:

```
infasetup updateWorkerNode -krb true -srn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM
```

## Ativando o Kerberos em nós Informatica

Depois de ativar o Kerberos no domínio, você deve copiar o arquivo de configuração Kerberos para cada nó do domínio. Você também deve configurar os navegadores da Web para acessar os aplicativos da Web Informatica.

Copie os arquivos keytab para o seguinte diretório em cada nó:

```
<diretório de instalação Informatica>\isp\config\keys
```

Os arquivos keytab copiados dependem da sua opção por ativar a autenticação Kerberos em nível de nó ou em nível de processo.

### Arquivos keytab em nível de nó

Copie cada arquivo keytab gerado em nível de nó para o nó correspondente.

A seguinte tabela mostra o nó para o qual copiar cada arquivo keytab:

Arquivo keytab	Localização no nó
<nome do nó>.keytab	Copie cada arquivo para o nó correspondente.
webapp_http.keytab	Copie cada arquivo para o nó de gateway correspondente.
ldapuser.keytab	Copie o arquivo para cada nó de gateway.

### Arquivos keytab em nível de processo

Copie cada arquivo keytab gerado em nível de processo para o nó correspondente.

A seguinte tabela mostra o nó para o qual copiar cada arquivo keytab:

Arquivo keytab	Localização no nó
<nome do nó>.keytab	Copie cada arquivo para o nó correspondente.
webapp_http.keytab	Copie cada arquivo para o nó de gateway correspondente.
_AdminConsole.keytab	Copie cada arquivo para o nó de gateway correspondente.
<nome do serviço de aplicativo>.keytab	Copie cada arquivo para o nó correspondente no qual o serviço de aplicativo Informatica é executado.
ldapuser.keytab	Copie o arquivo para cada nó de gateway.



## Configure navegadores da Web para acessar aplicativos da Web Informatica.

No Microsoft Internet Explorer e no Google Chrome, adicione a URL do aplicativo da Web Informatica, como a ferramenta Analyst, à lista de sites confiáveis.

Se você estiver usando o Chrome versão 41 ou posterior, deverá definir também as diretivas Políticas AuthServerWhitelist e AuthNegotiateDelegateWhitelist.

## Copiar os arquivos keytab para os nós Informatica

Depois de criar os arquivos keytab, copie cada um deles para o nó correspondente.

Copie os arquivos keytab para o seguinte diretório em cada nó:

```
<diretório de instalação Informatica>\isp\config\keys
```

Os arquivos keytab copiados dependem da sua opção por ativar a autenticação Kerberos em nível de nó ou em nível de processo.

### Arquivos keytab em nível de nó

Copie cada arquivo keytab gerado em nível de nó para o nó correspondente.

A seguinte tabela mostra o nó para o qual copiar cada arquivo keytab:

Arquivo keytab	Localização no nó
<nome do nó>.keytab	Copie cada arquivo para o nó correspondente.
webapp_http.keytab	Copie cada arquivo para o nó correspondente.
Idapuser.keytab	Copie o arquivo para cada nó de gateway.

### Arquivos keytab em nível de processo

Copie cada arquivo keytab gerado em nível de processo para o nó correspondente.

A seguinte tabela mostra o nó para o qual copiar cada arquivo keytab:

Arquivo keytab	Localização no nó
<nome do nó>.keytab	Copie cada arquivo para o nó correspondente.
webapp_http.keytab	Copie cada arquivo para o nó correspondente.
_AdminConsole.keytab	Copie cada arquivo para o nó correspondente.
<nome do serviço de aplicativo>.keytab	Copie cada arquivo para o nó correspondente no qual o serviço de aplicativo Informatica é executado.
Idapuser.keytab	Copie o arquivo para cada nó de

## Ativar a autenticação Kerberos para clientes Informatica

Copie o arquivo de configuração Kerberos para cada computador que hospeda um cliente Informatica e, em seguida, defina uma variável de ambiente de forma a apontar para esse arquivo de configuração. Você também deve permitir que os navegadores dos clientes acessem os aplicativos da Web Informatica.

Depois de configurar o domínio Informatica a ser executado com a autenticação Kerberos, execute as seguintes tarefas nas ferramentas do cliente Informatica:

### **Copie o arquivo de configuração Kerberos para cada host de cliente Informatica.**

Copie o arquivo `krb5.conf` para cada computador que hospeda um cliente Informatica, como o Cliente do PowerCenter ou o Informatica Developer (a Developer tool). Copie o arquivo para o seguinte diretório em cada host:

```
<diretório de instalação Informatica>\clients\shared\security
```

### **Defina a variável de ambiente KRB5\_CONFIG em cada host de cliente Informatica.**

Defina a variável de ambiente `KRB5_CONFIG` como o caminho e o nome do arquivo de configuração Kerberos em cada computador que hospeda clientes Informatica, como o Cliente do PowerCenter e a Developer tool.

### **Configure navegadores da Web para acessar aplicativos da Web Informatica.**

No Microsoft Internet Explorer e no Google Chrome, adicione a URL do aplicativo da Web Informatica, como a ferramenta Analyst, à lista de sites confiáveis.

Se você estiver usando o Chrome versão 41 ou posterior, deverá definir também as diretivas Políticas `AuthServerWhitelist` e `AuthNegotiateDelegateWhitelist`.

## Habilitando o Kerberos para Integração com o Hadoop

Para executar mapeamentos em um cluster habilitado para Kerberos e exibir metadados da Developer tool, realize tarefas de configuração na ferramenta Administrator e em cada máquina da Developer tool.

Realize as seguintes tarefas:

- Definir o arquivo de configuração Kerberos
- Criar artefatos de autenticação do usuário
- Configurar propriedades de autenticação Kerberos para o domínio Informatica
- Importar arquivos de configuração para cada máquina da Developer tool
- Gerar um arquivo de credenciais Kerberos para a máquina da Developer tool

Para ver como realizar essas tarefas, leia o capítulo sobre como executar mapeamentos com autenticação Kerberos no *Guia do Administrador do Data Engineering*.

# Ativando contas de usuário para usar a autenticação Kerberos

Depois de ativar a autenticação Kerberos no domínio, importe contas de usuário Informatica do Active Directory para o domínio de segurança LDAP que contém as contas de usuário Kerberos. Você também deve migrar os grupos, as funções, os privilégios e as permissões do domínio de segurança nativo para as contas de usuário Active Directory correspondentes no domínio de segurança LDAP que contém as contas de usuário do Kerberos.

## Importar contas de usuário do Active Directory para domínios de segurança LDAP

Importar contas de usuário do Active Directory para domínios de segurança LDAP.

Quando você ativa a autenticação Kerberos no domínio, o Informatica cria um domínio de segurança LDAP vazio com o mesmo nome que o realm Kerberos. Você pode importar contas de usuários do Active Directory para esse domínio de segurança LDAP ou pode importar as contas de usuário para um domínio de segurança LDAP diferente.

Use a ferramenta Administrator para importar as contas de usuários que usam a autenticação Kerberos do Active Directory para um domínio de segurança LDAP.

Para configurar a autenticação de realm cruzado Kerberos, conecte-se ao catálogo global do Active Directory. Ao se conectar ao catálogo global, você importa usuários do servidor do Active Directory usado por cada realm Kerberos.

1. Inicie o domínio e todos os serviços Informatica.
2. Faça logon no Windows com a conta de administrador que você especificou quando ativou a autenticação Kerberos no domínio.
3. Faça logon na ferramenta Administrator. Selecione \_infalInternalNamespace como domínio de segurança.
4. Na ferramenta Administrator, clique na guia **Segurança**.
5. Clique no menu **Ações** e selecione **Configuração LDAP**.
6. Na caixa de diálogo **Configuração LDAP**, clique na guia **Conectividade do LDAP**.
7. Configure as propriedades de conexão do Active Directory.

Talvez seja necessário consultar o administrador do LDAP para obter as informações necessárias para a conexão com o servidor LDAP.

A tabela a seguir descreve as propriedades de configuração do servidor LDAP:

Propriedade	Descrição
Nome do servidor	Nome do host ou endereço IP do servidor Active Directory. Para configurar a autenticação de realm cruzado Kerberos, conecte-se ao host do catálogo global do Active Directory. Especifique o nome totalmente qualificado do host. Por exemplo: host.empresa.local
Porta	Porta de escuta para o servidor Active Directory. O padrão é 389. A porta SSL padrão é 636. Para configurar a autenticação de realm cruzado Kerberos, conecte-se à porta do catálogo global do Active Directory. O padrão é 3268. A porta SSL padrão é 3269.
Serviço de Diretório LDAP	Selecione <b>Serviço Microsoft Active Directory</b> .
Nome	Especifique a conta de usuário vinculada que você criou no Active Directory para sincronizar contas no Active Directory com o domínio de segurança LDAP. Como o domínio está ativado para autenticação Kerberos, você não tem a opção de fornecer uma senha para a conta. Se o domínio usar a autenticação de realm cruzado Kerberos, inclua o nome do realm ao qual o banco de dados da entidade de segurança do Active Directory pertence.
Usar Certificado SSL	Indica que o servidor LDAP usa o protocolo SSL (Secure Socket Layer).
Confiar no Certificado LDAP	Determina se o Gerenciador de Serviços pode confiar no certificado SSL do servidor LDAP. Se for selecionado, o Gerenciador de Serviços se conectará ao servidor LDAP sem verificar o certificado SSL. Se não for selecionado, o Gerenciador de Serviços verificará se o certificado SSL está assinado por uma autoridade de certificado antes de se conectar ao servidor LDAP.
Não Diferencia Maiúsculas de Minúsculas	Indica que o Service Manager deve ignorar maiúsculas e minúsculas para atributos de nome distinto ao atribuir usuários a grupos.
Atributo de Associação de Grupo	Nome do atributo que contém informações de associação do grupo para um usuário. Esse é o atributo no objeto do grupo LDAP que contém os DN's dos usuários ou grupos que são membros de um grupo. Por exemplo, <i>member</i> ou <i>memberof</i> .
Tamanho Máximo	Número máximo de contas de usuário a serem importadas para um domínio de segurança. Por exemplo, se o valor for definido como 100, você poderá importar no máximo 100 contas de usuário para o domínio de segurança. Se o número dos usuários a serem importados exceder o valor para essa propriedade, o Gerenciador de Serviços gerará uma mensagem de erro e não importará nenhum usuário. Defina essa propriedade com um valor mais alto se você tiver muito usuários para importar. O padrão é 1000.

8. Na caixa de diálogo **Configuração LDAP**, clique na guia **Domínios de Segurança**.
9. Clique em **Adicionar**.

A tabela a seguir descreve as propriedades de filtro que você pode definir para um domínio de segurança:

Propriedade	Descrição
Domínio de Segurança	Nome do domínio de segurança LDAP para o qual você deseja importar contas de usuários do Active Directory.
Base de pesquisa do usuário	<p>Nome diferenciado (DN) da entrada que serve como ponto de partida para procurar nomes de usuários no Active Directory. A pesquisa localiza um objeto no diretório de acordo com o caminho no nome diferenciado do objeto.</p> <p>Por exemplo, para pesquisar o contêiner USER que contém contas de usuário Informática no domínio example.com do Windows, especifique CN=USERS,DC=EXAMPLE,DC=COM.</p>
Filtro de usuário	<p>Uma sequência de consulta LDAP especifica os critérios de pesquisa para usuários no serviço de diretório. O filtro pode especificar os tipos de atributos, os valores de declaração e os critérios de correspondência.</p> <p>Por exemplo: (objectclass=*) pesquisa todos os objetos.  (&amp;(objectClass=user)(!(cn=susan))) pesquisa todos os objetos de usuário, exceto "susan". Para obter mais informações sobre filtros de pesquisa, consulte a documentação do serviço de diretório LDAP.</p>
Base de pesquisa do grupo	Nome diferenciado (DN) da entrada que serve como ponto de partida para pesquisar nomes de grupos no serviço de diretório LDAP.
Filtro de grupo	Uma cadeia de consulta LDAP especifica os critérios para pesquisar grupos no serviço de diretório.

A seguinte imagem mostra as informações necessárias para importar usuários LDAP do Active Directory para o domínio de segurança LDAP criado quando você ativou o Kerberos no domínio:

The screenshot shows the 'LDAP Configuration' dialog box with the 'Security Domains' tab selected. The dialog has three tabs: 'LDAP Connectivity', 'Security Domains', and 'Schedule'. Below the tabs, there is a message: 'Fields marked with an asterisk (\*) are required.' and 'You can specify multiple security domains for LDAP users and groups. Click Add to add a new security domain.' There is a green plus icon and the word 'Add'. Below this is a section titled 'Add new Security Domain' with a dropdown arrow, a magnifying glass icon, and the words 'Preview' and 'Cancel'. The section contains five input fields: 'Security Domain \*' with the value 'COMPANY.COM', 'User search base' with the value 'CN=USERS,DC=COMPANY,DC=COM', 'User filter', 'Group search base', and 'Group filter'. At the bottom of the dialog are three buttons: 'Synchronize Now', 'OK', and 'Cancel'.

10. Clique em **Sincronizar Agora**.

O Gerenciador de Serviços sincroniza os usuários em todos os domínios de segurança LDAP com os usuários no serviço de diretório LDAP. O tempo que leva para concluir o processo de sincronização depende do número de usuários e grupos a serem importados.

11. Clique em **OK** para salvar o domínio de segurança LDAP.

## Migrar permissões e privilégios de usuários nativos para um domínio de segurança Kerberos

Se o domínio Informatica tiver contas de usuário no domínio de segurança nativo, as contas de usuário Active Directory correspondentes no domínio de segurança Kerberos deverão ter os mesmos grupos, funções, privilégios e permissões. Migre os grupos, as funções, os privilégios e as permissões dos usuários nativos para as contas de usuário correspondentes no domínio de segurança LDAP Kerberos.

1. Reveja a lista de contas de usuários nativos e determine as contas que você deseja migrar para o domínio de segurança LDAP para autenticação Kerberos.

Para listar as contas de usuário no domínio Informatica, execute o seguinte comando:

```
infacmd isp ListAllUsers
```

Cada conta de usuário nativo que você deseja migrar para o domínio de segurança Kerberos deve ter uma conta correspondente no serviço Active Directory que você utiliza para a autenticação Kerberos.

2. Crie o arquivo de migração de usuários.

O arquivo de migração de usuários é um arquivo de texto simples que contém a lista de usuários nativos e dos usuários Kerberos correspondentes que exigem os mesmos grupos, funções, privilégios e permissões.

Use o seguinte formato para listar as entradas no arquivo de migração de usuários:

```
Native/<source user name>,<LDAP security domain>/<target user name>
```

O seguinte exemplo mostra um arquivo de migração de usuários contendo a seguinte lista de usuários a serem migrados para o domínio de segurança COMPANY.COM:

```
Native/User1,COMPANY.COM/User1
Native/User2,COMPANY.COM/User2
Native/User3,COMPANY.COM/User3
```

3. Execute o comando `infacmd isp migrateUsers` para migrar permissões e privilégios de contas no domínio de segurança nativo para as contas no domínio de segurança Kerberos.

Para migrar os grupos, as funções, os privilégios e as permissões de usuários, execute o seguinte comando:

```
infacmd isp migrateUsers -dn <domain name> -un <administrator user name> -pd
<administrator password> -sdn <security domain> -umf <user migration file>
```

A seguinte tabela descreve as opções para o comando

Opção	Descrição
-DomainName -dn	Nome do domínio Informatica.
-UserName -un	Nome de usuário a ser conectado ao domínio. Especifique o nome de usuário da conta de administrador que você especificou no comando <code>infasetup switchToKerberosMode</code> .
-Password -pd	Senha para a conta do administrador.
-SecurityDomain -sdn	Domínio de segurança LDAP da conta de administrador usada para conexão com o domínio. Especifique <code>_infaInternalNamespace</code> .
-UserMigrationFile -umf	O caminho e o nome do arquivo de migração de usuários. O comando ignora as entradas com um nome de usuário de origem ou de destino duplicado.

O exemplo a seguir migra os grupos, as funções, os privilégios e as permissões para usuários com base no arquivo de migração de usuários `um_s.txt`:

```
infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn
_infaInternalNamespace -umf C:\Infa\um_s.txt
```

O comando substitui as permissões do objeto de conexão atribuídas ao usuário LDAP com as permissões do objeto de conexão com o usuário nativo. O comando mescla os grupos, as funções, os privilégios e as permissões em objeto de domínio para os usuários nativos e para os usuários LDAP correspondentes.

O comando `migrateUsers` cria um arquivo de log detalhado denominado

`infacmd_umt_<date>_<time>.txt` no diretório em que você executa o comando.

# Delegação Kerberos

A delegação Kerberos permite que um serviço Kerberos personifique um usuário cliente Kerberos e obtenha um tíquete de serviço para outro serviço em nome do usuário cliente.

Os serviços em um domínio Informatica precisam se conectar a outros serviços para concluir uma operação. Você pode se conectar a outros serviços por meio de autenticação delegada. Na autenticação delegada, quando um usuário é autenticado por um serviço, o serviço usa essas credenciais para se conectar a outro serviço. Por exemplo, quando um usuário pmcmd acessa o Serviço de Integração do Power Center, o serviço atua como o usuário pmcmd para autenticar com o Serviço de Repositório do PowerCenter .

## Tipos de delegação Kerberos

Ao usar a autenticação delegada, você pode escolher um dos seguintes tipos de delegação:

### Delegação completa

A delegação completa é a implementação inicial da delegação Kerberos. Nesse método de delegação, um cliente encaminha seu Ticket Granting Ticket (TGT) para um serviço após a autenticação Kerberos. O serviço usa o TGT para obter tíquetes de serviço para acessar qualquer outro serviço na rede. Esse tipo de delegação não é considerado seguro porque um administrador não pode controlar os serviços que o servidor pode acessar usando a identidade do cliente. A delegação completa também é conhecida como delegação irrestrita.

### Delegação restrita baseada em recursos

Com a delegação restrita baseada em recursos, os administradores podem restringir o uso da identidade do cliente pelos serviços. Nesse método de delegação, o cliente não encaminha o TGT ao servidor. Nesse método, os serviços especificam em quem eles confiam e quem pode delegar autenticação a eles.

A delegação restrita usa extensões de protocolo Kerberos chamadas Service for User (S4U), que permitem que um serviço obtenha um tíquete de serviço Kerberos em nome de um usuário.

**Nota:** Você não pode usar a delegação restrita e a delegação completa em um único domínio. Você pode configurar o domínio para usar a delegação completa ou a delegação restrita.

## Extensão de serviço para usuário (S4U)

As extensões Service for User (S4U) permitem que um serviço obtenha um tíquete de serviço Kerberos em nome de um usuário. A seguir estão os dois tipos de extensões S4U:

- Serviço para o próprio usuário (S4U2Self). Essa extensão permite que um serviço obtenha um tíquete de serviço para si mesmo em nome de um usuário cliente.
- Serviço de usuário para proxy (S4U2Proxy). Essa extensão permite que um serviço obtenha um tíquete de serviço para outro serviço em nome de um usuário cliente. Para executar S4U2proxy, um serviço precisa de um tíquete de serviço para si mesmo. O tíquete de serviço pode ser apresentado pelo usuário cliente ou obtido através da extensão S4U2Self.

Para obter mais informações sobre as extensões S4U, consulte a documentação da Microsoft.

## Ativar a delegação restrita baseada em recursos com S4U2Self

Certifique-se de que o sinalizador forwardable esteja definido como true na seção libdefaults do arquivo krb5.conf.



Você pode configurar a Delegação restrita baseada em recursos apenas por meio de comandos do PowerShell. Certifique-se de que o PowerShell seja iniciado por um usuário com os privilégios necessários para alterar as propriedades das contas de KDC, de preferência um administrador de KDC.

Para ativar a Delegação Restrita Baseada em Recursos com S4U2Self, realize as seguintes etapas para cada conta de keytab Informatica no servidor KDC:

1. Clique com o botão direito na conta do usuário e selecione **Propriedades**.  
A caixa de diálogo **Propriedades** é exibida.
2. Na guia **Delegação**, selecione **Não confie neste computador para delegação**.
3. Clique em **Aplicar**.
4. Execute o seguinte comando para definir o atributo `PrincipalsAllowedToDelegateToAccount`:  

```
$IntermediateService = Get-ADUser -Identity <samAccountName da conta do servidor intermediária> -Properties *  
  
Set-ADUser -Identity <samAccountName da conta do servidor de destino> -  
PrincipalsAllowedToDelegateToAccount $IntermediateService1, $IntermediateService2,  
$IntermediateService3
```

**Nota:** Você pode usar valores separados por vírgula para adicionar várias contas no atributo `PrincipalsAllowedToDelegateToAccount`.
5. Se quiser cancelar a definição do atributo `PrincipalsAllowedToDelegateToAccount`, execute o seguinte comando:  

```
Set-ADUser -Identity <samAccountName da conta do servidor de destino>  
PrincipalsAllowedToDelegateToAccount $null
```
6. Para ver as entidades principais existentes na lista `PrincipalsAllowedToDelegateToAccount`, execute os seguintes comandos:  

```
$FormatEnumerationLimit=-1  
Get-ADUser -Identity <nome da conta sam> -properties  
PrincipalsAllowedToDelegateToAccount
```

**Nota:** Por padrão, a saída do comando do PowerShell mostra quatro valores na lista de entidades principais de serviço na saída. Defina esse parâmetro como -1 para mostrar a lista completa de entidades principais.

## Ativar a delegação completa para as contas de usuário de entidade principal Kerberos no Active Directory

Crie os arquivos keytab usando o comando `ktpass`.

Para usar a delegação completa, você deve ativar a delegação para todas as contas criadas, exceto para a conta de usuário LDAP que você usa para acessar e pesquisar Active Directory durante a sincronização LDAP.

Para ativar a delegação completa, execute as seguintes etapas para cada conta de usuário:

1. Clique com o botão direito na conta do usuário e selecione **Propriedades**.  
A caixa de diálogo **Propriedades** é exibida.
2. Na guia **Delegação**, selecione **Confiar neste usuário para delegação a qualquer serviço (apenas Kerberos)**.
3. Clique em **Aplicar**.  
A delegação completa está ativada.

## Mudar de Delegação Completa para Delegação Restrita

Se você estiver usando a delegação completa e quiser usar a delegação restrita, execute as etapas a seguir.

1. Desligue o domínio.
2. [“Ativar a delegação restrita baseada em recursos com S4U2Self” na página 64](#) para usuários existentes do Active Directory associados à conta keytab no servidor KDC.
3. Inicie o domínio.

## CAPÍTULO 5

# Autenticação SAML para aplicativos da Web da Informatica

Este capítulo inclui os seguintes tópicos:

- [Visão geral da autenticação SAML, 67](#)
- [Processo de autenticação SAML, 69](#)
- [Ativar a autenticação SAML em um domínio, 70](#)
- [Segurança de Autenticação Aprimorada, 72](#)
- [Configurando aplicativos da Web para usar diferentes provedores de identidade, 75](#)

## Visão geral da autenticação SAML

Você pode configurar a autenticação SAML (Security Assertion Markup Language) para aplicativos da Web do Informatica.

Security Assertion Markup Language é um formato de dados baseado em XML para a troca de informações de autenticação entre um provedor de serviços e um provedor de identidade. Em um domínio Informatica, o aplicativo da Web Informatica é o provedor de serviços.

Você pode configurar os seguintes aplicativos da Web da Informatica para usar a autenticação SAML:

- Informatica Administrator
- Informatica Analyst
- Ferramenta Ingestão em Massa
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation
- Data Privacy Management

**Nota:** A autenticação SAML não pode ser usada em um domínio de Informatica configurado para usar a autenticação Kerberos.

Se você ativar um domínio para usar a autenticação SAML, todos os aplicativos da Web executados no domínio usarão o provedor de identidade configurado no domínio por padrão. No entanto, você pode configurar aplicativos da Web da Informatica executados em um domínio para usar diferentes provedores de identidade. Por exemplo, você pode configurar o Informatica Administrator para usar o AD FS como provedor de identidade e configurar o Informatica Analyst para usar PingFederate como provedor de identidade.

Para obter mais informações sobre como configurar aplicativos da Web para usar diferentes provedores de identidade, consulte ["Configurando aplicativos da Web para usar diferentes provedores de identidade" na página 75.](#)

## Default Keystore and Truststore Directory

The Informatica deployment includes default keystore and truststore files in the directory `<Informatica installation directory>\services\shared\security`.

Informatica recommends that you use the default keystore and truststore only for setup and proof-of-concept use cases. To secure a production environment, use the following guidelines:

- Configure a custom keystore and truststore for SAML authentication in a location other than the default directory:  
`<Informatica installation directory>\services\shared\security`
- You cannot use the default keystore and truststore to configure other services or clients.
- When you enable SAML authentication, you import keystore or truststore certificate files and private keys into the default directory:  
`<Informatica installation directory>\services\shared\security`
- When you assign an alias to the keystore or truststore, do not use "Informatica LLC," which Informatica uses for private key authentication and certificate signing.
- Modifying the default SAML keystore or truststore is allowed only when the default directory is configured as the SAML keystore and truststore directory and you want to import private key and certificate entries in the default keystore or truststore.

You cannot use "Informatica LLC" as the alias for new entries in default keystore and truststore. You can use "Informatica LLC" as the alias for custom keystore-truststore entries.

No other operation is allowed for the default keystore and truststore files, including deleting or replacing the files, changing the password of the keystore or truststore, or modifying, removing or replacing the Informatica-generated private key and signing certificate.

- If you replaced the default Informatica keystore and truststore files with custom keystore and truststore files in the previous Informatica installation directory structure, you must run the `infasetup UpdateGatewayNode` command to update the locations of the custom keystore and truststore for the domain.

## Provedores de Identidade Compatíveis

Use um provedor de identidade compatível para gerenciar a autenticação SAML no domínio para aplicativos da Web.

A Informatica oferece suporte aos seguintes provedores de identidade. Clique no link do artigo da Biblioteca de Instruções (H2L) para obter instruções de integração entre cada provedor de identidade e o domínio.

Provedor de Identidade	Artigo da Biblioteca de Instruções (H2L)
Microsoft Active Directory Federation Services (AD FS)	<a href="#">SAML Authentication with Active Directory Federation Services in Informatica 10.4.0</a>
PingFederate	<a href="#">SAML Authentication with PingFederate in Informatica 10.4.0</a>
F5 Big-IP	<a href="#">SAML Authentication with F5 Networks BIG-IP in Informatica 10.4.1</a>

Provedor de Identidade	Artigo da Biblioteca de Instruções (H2L)
NetScaler	<a href="#">SAML Authentication with NetScaler for Web Applications</a>
Oracle Access Manager (OAM)	<a href="#">SAML Authentication with Oracle Access Manager for Web Applications</a>
Okta SSO	<a href="#">SAML Authentication with Okta SSO for Web Applications</a>
Azure Active Directory	<a href="#">SAML Authentication with Azure Active Directory for Web Applications</a>

Para obter informações sobre versões com suporte desses provedores de identidade, consulte a Matriz de Disponibilidade de Produtos na Informatica Network:  
<https://network.informatica.com/community/informatica-network/product-availability-matrices>.

## Processo de autenticação SAML

Os aplicativos da Web da Informatica e o provedor de identidade trocam informações de autenticação para habilitar a autenticação SAML em um domínio Informatica.

As seguintes etapas descrevem o fluxo básico da autenticação SAML:

1. Um usuário acessa um aplicativo da Web da Informatica.
2. O usuário seleciona o domínio de segurança que contém as contas de usuário LDAP usadas para autenticação SAML na página de login do aplicativo e, em seguida, clica no botão logon.  
Se o usuário selecionar o domínio de segurança nativo, ele fornecerá um nome de usuário e uma senha e efetuará login no aplicativo.
3. Com base na configuração do provedor de identidade, o usuário é solicitado a fornecer as credenciais necessárias para a autenticação inicial.
4. O provedor de identidade valida as credenciais do usuário e cria uma sessão para o usuário.  
O provedor de identidade também valida o URL do aplicativo da Web de destino e, em seguida, redireciona o usuário para o aplicativo da Web com um token SAML contendo as informações de identidade do usuário.
5. O aplicativo valida o token SAML e as informações de identidade do usuário, cria uma sessão do usuário e conclui o processo de login do usuário.

A sessão do usuário existente no navegador é usada para autenticação subsequente. Para acessar outro aplicativo da Web da Informatica configurado para usar a autenticação SAML, o usuário seleciona o domínio de segurança LDAP na página de login do aplicativo. O usuário não precisa fornecer um nome de usuário ou senha.

O usuário permanecerá conectado a todos os aplicativos da Web da Informatica que estiverem em execução na mesma sessão do navegador. No entanto, se o usuário fizer logout de um aplicativo da Web Informatica, o usuário também será desconectado de outros aplicativos da Web Informatica executados na mesma sessão do navegador.

# Ativar a autenticação SAML em um domínio

Configure o provedor de identidade, o domínio Informatica e os nós de no domínio para usar a autenticação SAML.

Para configurar a autenticação SAML para aplicativos da Web da Informatica com suporte, executados em um domínio, execute as seguintes tarefas:

1. Crie uma configuração LDAP para conectar-se ao armazenamento de identidade LDAP que contém as contas de usuário do aplicativo da Web da Informatica. Crie também um domínio de segurança LDAP e importe as contas de usuário para o domínio de segurança.
2. Exporte o certificado de assinatura de declaração do provedor de identidade.
3. Importe o certificado de assinatura de declaração para um arquivo truststore em cada nó de gateway do domínio. É possível importar o certificado para o arquivo truststore padrão da Informatica ou para um arquivo truststore personalizado.
4. Adicione uma ou mais relações de confiança ou provedores de serviços de terceiros confiáveis ao provedor de identidade.
5. Adicione a URL para cada aplicativo da Web da Informatica ao provedor de identidade.
6. Ative a autenticação SAML no domínio.
7. Ative a autenticação SAML em cada nó de no domínio.

**Nota:** Para vários dos provedores de identidade SAML aos quais a Informatica oferece suporte, você pode seguir as etapas de integração detalhadas em um artigo da Biblioteca de Instruções (H2L). Consulte [“Provedores de Identidade Compatíveis” na página 68](#) para obter links para os artigos.

## Crie uma configuração LDAP para o provedor de identidade ou o armazenamento LDAP

Use a ferramenta Administrator para criar uma configuração LDAP para o provedor de identidade ou armazenamento LDAP que contenha as contas de usuário do aplicativo da Web que usam autenticação SAML.

Ao criar uma configuração LDAP, você cria um domínio de segurança para as contas de usuário e depois importa as contas para o domínio de segurança. Depois de importar as contas para o domínio de segurança, atribua as funções, os privilégios e as permissões de domínio Informatica apropriados para as contas dentro do domínio de segurança

Para obter mais informações sobre como criar uma configuração LDAP, consulte [“Criando uma configuração do LDAP” na página 26](#).

## Exportar o certificado de assinatura de declaração

O provedor de identidade envia asserções de autenticidade aos provedores de serviços na forma de um certificado de assinatura de asserção.

Uma asserção assinada contém uma assinatura que o provedor de identidade cria, usando um algoritmo escolhido pelo administrador do provedor de identidade. Em seguida, o Informatica verifica a assinatura usando o certificado público correspondente que o administrador de domínio importou para o truststore SAML.

A Informatica recomenda que você habilite a asserção assinada.

Exporte o certificado de assinatura de asserção do provedor de identidade para habilitar a asserção assinada.

## Importar o certificado para o truststore usado na autenticação SAML

Importe o certificado de assinatura de declaração usado pelo provedor de identidade no arquivo de armazenamento confiável usado para autenticação SAML em todos os nós de gateway no domínio Informatica.

É possível importar o certificado para o arquivo truststore da Informatica padrão ou para um arquivo truststore personalizado.

## Configurar o provedor de identidade

Configure o provedor de identidade para emitir tokens SAML para aplicativos da Web da Informatica.

Realize as seguintes tarefas para configurar o provedor de identidade:

- Adicione uma parte dependente confiável ao domínio no provedor de identidade. A definição de parte dependente confiável permite que o provedor de identidade aceite solicitações de autenticação de aplicativos da Web da Informatica que são executados no domínio.
- Edite a regra Enviar Atributos LDAP como Reivindicações para mapear atributos LDAP no seu repositório de identidade para os tipos correspondentes usados em tokens SAML emitidos pelo provedor de identidade.

Forneça o nome confiável da parte dependente quando habilitar a autenticação do SAML em um domínio. Dependendo dos requisitos de segurança, você pode criar várias partes dependentes confiáveis no provedor de identidade para permitir que domínios usados por diferentes organizações na empresa usem a autenticação SAML.

O Informatica reconhece "Informatica" como o nome confiável da parte dependente padrão. Se você criar uma única parte dependente confiável com "Informatica" como o nome confiável da parte dependente, não precisará fornecer o nome confiável da parte dependente ao habilitar a autenticação SAML em um domínio.

**Nota:** Todas as strings diferenciam maiúsculas de minúsculas no provedor de identidade, incluindo URLs.

## Adicionar URLs do aplicativo da Web da Informatica ao provedor de identidade

Adicione a URL para cada aplicativo da Web da Informatica que usa a autenticação SAML no provedor de identidade.

Você fornece a URL de um aplicativo da Web da Informatica para permitir que o provedor de identidade aceite solicitações de autenticação enviadas pelo aplicativo. Fornecer a URL também permite que o provedor de identidade envie o token SAML ao aplicativo depois de autenticar o usuário.

## Configurar a Autenticação SAML no Domínio

Você pode configurar a autenticação SAML em um domínio Informatica existente ou pode habilitá-la ao criar um domínio.

Quando você habilita um domínio para usar a autenticação SAML, todos os aplicativos da Web executados no domínio usam o provedor de identidade padrão especificado quando você habilita a autenticação SAML no domínio.

Selecione uma das seguintes opções:

**Ative a autenticação SAML quando executar o instalador da Informatica.**

Você pode ativar a autenticação SAML e especificar a URL do provedor de identidade ao configurar o domínio como parte do processo de instalação.

**Ative a autenticação SAML em um domínio existente.**

Use o comando `infasetup updateDomainSamlConfig` para ativar a autenticação SAML em um domínio Informatica existente. É possível executar o comando em qualquer nó de gateway no domínio.

**Ative a autenticação SAML ao criar um domínio.**

Use o comando `infasetup defineDomain` para ativar a autenticação SAML quando você criar um domínio.

Consulte a *IReferência de Comandos Informatica* para obter instruções sobre como usar os comandos.

## Ativar a autenticação SAML nos nós de

Você deve configurar a autenticação SAML em cada gateway e nó de trabalho no domínio Informatica.

Selecione uma das seguintes opções para configurar a autenticação SAML em um nó de gateway:

**Ative a autenticação SAML ao definir um nó de gateway em uma máquina.**

Use o comando `infasetup DefineGatewayNode` para ativar a autenticação SAML no nó de gateway.

**Ative a autenticação SAML ao configurar um nó de gateway para ingressar em um domínio que usa a autenticação SAML.**

Use o comando `infasetup UpdateGatewayNode` para ativar a autenticação SAML no nó de gateway.

**Ative a autenticação SAML ao converter um nó do funcionário em um nó de gateway.**

Use o comando `isp SwitchToGatewayNode` para ativar a autenticação SAML no nó.

Selecione uma das seguintes opções para configurar a autenticação SAML em um nó de trabalhador:

**Ative a autenticação SAML quando você definir um nó de trabalhador em uma máquina.**

Use o comando `infasetup DefineWorkerNode` para ativar a autenticação SAML no nó de trabalhador.

**Ative a autenticação SAML quando você configurar um nó de trabalhador para entrar em um domínio que usa autenticação SAML.**

Use o comando `infasetup UpdateWorkerNode` para ativar a autenticação SAML no nó de trabalhador.

Consulte a *IReferência de Comandos Informatica* para obter instruções sobre como usar os comandos.

## Segurança de Autenticação Aprimorada

Você pode habilitar a assinatura da solicitação, a resposta assinada ou a asserção criptografada para aprimorar a segurança da autenticação:

**Assinatura de solicitação**

Uma solicitação de autenticação assinada contém uma assinatura para verificar a autenticidade da própria solicitação. A Informatica, agindo como um provedor de serviços, envia uma solicitação de autenticação ao provedor de identidade. Para manter a integridade da solicitação, a solicitação de autenticação pode ser assinada.

O Informatica assina uma solicitação SAML usando uma chave privada, e o provedor de identidade verifica a assinatura usando o certificado público correspondente.



O Informatica envia solicitações de autenticação SAML via HTTP-Redirect. As solicitações usam codificação deflate, que coloca a assinatura em um parâmetro de URL.

#### Resposta assinada

O provedor de identidade responde às solicitações de autenticação de um provedor de serviços. Uma resposta assinada contém uma assinatura que o provedor de identidade cria, usando um algoritmo escolhido pelo administrador do provedor de identidade. Em seguida, o Informatica verifica a assinatura usando o certificado público correspondente que o administrador de domínio importou para o truststore SAML.

#### Asserção assinada e asserção criptografada

O provedor de identidade envia asserções de autenticidade aos provedores de serviço.

Uma asserção assinada contém uma assinatura que o provedor de identidade cria, usando um algoritmo escolhido pelo administrador do provedor de identidade. Em seguida, o Informatica verifica a assinatura usando o certificado público correspondente que o administrador de domínio importou para o truststore SAML. A Informatica recomenda que você habilite a asserção assinada.

O Informatica Administrator gera uma chave assimétrica (chave pública-privada).

A asserção pode ser criptografada pelo provedor de identidade usando uma chave de criptografia de asserção, que é uma chave simétrica gerada pelo provedor de identidade.

Quando você habilita a asserção criptografada, o provedor de identidade também criptografa a chave simétrica usando o certificado público que o administrador de segurança importou para o provedor de identidade. A resposta SAML conterá a asserção criptografada e uma chave simétrica criptografada. Atuando como um provedor de serviços, a Informatica descriptografa a chave simétrica criptografada usando a chave privada correspondente que o Informatica Administrator importa para o armazenamento de chaves SAML. Depois de obter a chave simétrica, a Informatica descriptografa a asserção criptografada.

Siga as etapas nesta seção para habilitar a assinatura da solicitação, a asserção criptografada ou a resposta assinada.

## Assinatura de Solicitação

Você pode ativar a assinatura de solicitação durante o processo de instalação/upgrade ou após a instalação/upgrade usando infasetup.

Durante o processo de instalação ou atualização, verifique a opção **Requisição assinada** no utilitário de instalação.

Após o processo de instalação ou upgrade, configure a assinatura de solicitação usando infasetup.

Você também pode configurar a assinatura de solicitação para os aplicativos Web usando a ferramenta Administrator ou a interface do usuário do aplicativo Web.

### infasetup

Para usar o infasetup, use as seguintes opções com o comando `infasetup updateDomainSamlConfig`:

```
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
```

Para obter detalhes sobre esses comandos, consulte a *Referência de Comandos da Informatica*.

## Ferramenta Administrador

Configure a assinatura de solicitação na ferramenta Administrator.

1. No Navegador do Domínio, selecione o nó do domínio.
2. Nas propriedades do nó, clique no ícone **Editar** na seção **Configuração SAML**.
3. Selecione **Habilitar Solicitação de Assinatura**.
4. Preencha as seguintes propriedades:
  - Alias da Chave Privada de Assinatura
  - Senha da Chave Privada de Assinatura
  - Algoritmo de Assinatura
5. Clique em **OK**.
6. Reinicie o domínio.

## Resposta Assinada

Habilite a resposta assinada para permitir que o provedor de identidade assine as respostas da solicitação de autenticação do provedor de serviços.

Você pode habilitar a resposta assinada durante o processo de instalação/upgrade ou após a instalação/upgrade usando infasetup.

Durante o processo de instalação ou atualização, marque a opção **Resposta assinada** no utilitário de instalação.

Após o processo de instalação ou upgrade, configure a assinatura de resposta usando infasetup.

Você também pode configurar a resposta assinada para os aplicativos Web usando a ferramenta Administrator ou a interface do usuário do aplicativo Web.

**Nota:** O provedor de identidade Okta SSO não oferece suporte à resposta assinada.

## infasetup

Para usar o infasetup, use as seguintes opções com o comando `infasetup updateDomainSamlConfig`:

```
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
```

Para obter detalhes sobre esses comandos, consulte a *Referência de Comandos da Informatica*.

## Ferramenta Administrador

Configure a assinatura de resposta na ferramenta Administrator.

1. No Navegador do Domínio, selecione o nó do domínio.
2. Nas propriedades do nó, clique no ícone **Editar** na seção **Configuração SAML**.
3. Selecione **Habilitar Assinatura de Resposta**.
4. Preencha a propriedade do Alias do Certificado de Assinatura de Resposta.
5. Clique em **OK**.
6. Reinicie o domínio.

## Asserção Criptografada

Habilite a asserção criptografada para permitir que o provedor de identidade criptografe as asserções de autenticidade usando uma chave simétrica.

Você pode ativar a assinatura de asserção ou a asserção criptografada durante o processo de instalação/upgrade ou após a instalação ou o upgrade usando infasetup.

Durante o processo de instalação ou atualização, marque a opção **Criptografar asserção** no utilitário de instalação.

Após o processo de instalação ou upgrade, configure a asserção criptografada usando infasetup.

Você também pode configurar a resposta assinada para os aplicativos Web usando a ferramenta Administrator ou a interface do usuário do aplicativo Web.

### infasetup

Para usar o infasetup, use as seguintes opções com o comando `infasetup updateDomainSamlConfig`:

```
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypted_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypted_assertion_private_key_password]
```

Para obter detalhes sobre esses comandos, consulte a *Referência de Comandos da Informatica*.

### Ferramenta Administrator

Configure a asserção criptografada na ferramenta Administrator.

1. No Navegador do Domínio, selecione o nó do domínio.
2. Nas propriedades do nó, clique no ícone **Editar** na seção **Configuração SAML**.
3. Selecione **Habilitar Criptografia de Asserção**.
4. Preencha as seguintes propriedades:
  - Alias da Chave Privada da Asserção de Criptografia
  - Senha da Chave Privada da Asserção de Criptografia
5. Clique em **OK**.
6. Reinicie o domínio.

## Configurando aplicativos da Web para usar diferentes provedores de identidade

Você pode configurar aplicativos da Web da Informatica executados em um domínio para usar diferentes provedores de identidade. Por exemplo, você pode configurar o Informatica Administrator para usar o AD FS como provedor de identidade e configurar o Informatica Analyst para usar PingFederate como provedor de identidade.

Quando você ativa um domínio para usar a autenticação SAML, todos os aplicativos da Web executados no domínio usam o provedor de identidade padrão especificado quando você ativa a autenticação SAML no

domínio. Por exemplo, se você configurar o AD FS como provedor de identidade, todos os aplicativos da Web usarão o AD FS como provedor de identidade, a menos que você configure um aplicativo da Web para usar um provedor de identidade diferente.

Especifique o provedor de identidade padrão ao usar uma das seguintes opções para ativar a autenticação SAML:

- Quando você cria o domínio e instala os serviços Informatica.
- Quando você executa o comando `infasetup defineDomain` para criar o domínio.
- Quando você usa o comando `infasetup updateDomainSamlConfig` para ativar a autenticação SAML em um domínio existente.

Use a ferramenta Administrator para configurar um aplicativo da Web para usar um provedor de identificação diferente. Para configurar a ferramenta Administrator ou o aplicativo de monitoramento para usar um provedor de identidade diferente, modifique a configuração SAML no nó em que o aplicativo é executado. Para configurar outros aplicativos da web para usar um provedor de identidade diferente, modifique a configuração SAML dentro do processo do aplicativo.

## Preparar-se para usar um provedor de identidade

Conclua as tarefas a seguir para preparar um aplicativo Web da Informatica para usar um provedor de identidade.

1. Crie uma configuração LDAP para o armazenamento do provedor de identidade que contém as contas de usuário do aplicativo Web da Informatica. Crie também um domínio de segurança LDAP e importe as contas de usuário para o domínio de segurança.
2. Exporte o certificado de assinatura de declaração do provedor de identidade.
3. Importe o certificado de assinatura de declaração do provedor de identidade para um arquivo truststore em cada nó de gateway do domínio. É possível importar o certificado para o arquivo truststore padrão da Informatica ou para um arquivo truststore personalizado.

Se você alterar o nome alternativo, importe o certificado correspondente para o arquivo truststore em cada nó do gateway e reinicie o nó.

4. Adicione uma ou mais partes dependentes confiáveis ao provedor de identidade e mapeie atributos LDAP para os tipos correspondentes usados em tokens de segurança emitidos pelo provedor de identidade.
5. Adicione a URL para o aplicativo da Web da Informatica ao provedor de identidade.

## Configurar o Informatica Administrator para usar um provedor de identidade

Use a ferramenta Administrator para configurar a ferramenta Administrator ou o aplicativo de monitoramento para usar um provedor de identidade SAML. Configure a ferramenta Administrator ou o aplicativo de monitoramento para usar um provedor de identidade no nó em que o aplicativo é executado.

1. Na ferramenta Administrator, clique na guia **Serviços e Nós**.
2. Selecione o nó do gateway em que a ferramenta Administrator e o aplicativo de monitoramento são executados no Navegador do Domínio.
3. Clique no ícone de edição ao lado de Configuração SAML.
4. Insira as propriedades necessárias para permitir que o aplicativo use um provedor de identidade.

A tabela a seguir descreve as propriedades que você insere:

Propriedade	Descrição
URL de Provedor de Identidade	Opcional. A URL para o servidor do provedor de identidade. Você deve especificar a cadeia de URL completa.
ID do Provedor de Serviços	Opcional. O nome confiável da parte dependente ou o identificador do provedor de serviços para o domínio, conforme definido no provedor de identidade.
Alias do Certificado de Assinatura de Declaração	Opcional. O nome do alias especificado ao importar o certificado de assinatura de declaração do provedor de identidade para o arquivo truststore usado para a autenticação SAML. Se você alterar o nome alternativo, importe o certificado correspondente para o arquivo truststore em cada nó do gateway e reinicie o nó.
Tolerância a Distorção do Relógio	Opcional. A diferença de tempo permitida entre o relógio do sistema host do provedor de identidade e o relógio do sistema no nó de gateway mestre. Opcional. O tempo de vida dos tokens SAML emitidos pelo provedor de identidade é definido de acordo com o relógio do sistema host do provedor de identidade. O tempo de vida de um token SAML emitido pelo provedor de identidade será válido se a hora de início ou a hora de término definida no token estiver dentro do número de segundos especificado no relógio do sistema do nó de gateway mestre. Os valores devem ser de 0 a 600 segundos. Defina como -1 para usar o valor configurado para o domínio. O padrão é 120 segundos.

A imagem a seguir mostra a configuração para permitir que a ferramenta Administrator use o AD FS como provedor de identidade. Se você não especificar um valor para uma propriedade, o domínio usará o valor definido na configuração SAML padrão.

**Edit SAML Configuration** [X]

Fields marked with an asterisk (\*) are required.

Web Application ID \* monitoring

Identity Provider URL

Service Provider ID

Assertion Signing Certificate Alias

Clock Skew Tolerance -1

Web Application ID \* AdministratorConsole

Identity Provider URL

Service Provider ID

Assertion Signing Certificate Alias

Clock Skew Tolerance

[?] [OK] [Cancel]

5. Clique em **OK**.
6. Reinicie o aplicativo.

## Configurar um aplicativo da Web da Informatica

Use a ferramenta Administrator para configurar um aplicativo da Web da Informatica para usar um provedor de identificação SAML.

1. Na ferramenta Administrator, clique na guia **Serviços e Nós**.
2. Selecione o aplicativo ou o serviço de aplicativo no Navegador do Domínio.
  - Para configurar o aplicativo da ferramenta Analyst para usar um provedor de identidade, selecione o Serviço Analyst e clique na guia **Processos**.
  - Para configurar o aplicativo da ferramenta Ingestão em Massa para usar um provedor de identidade, selecione o Serviço de Ingestão em Massa e clique na guia **Processos**.
  - Para configurar o aplicativo Metadata Manager para usar um provedor de identidade, selecione o Serviço do Metadata Manager e clique na guia **Propriedades**.
  - Para configurar o aplicativo Enterprise Data Catalog para usar um provedor de identidade, selecione o Serviço de Catálogo e clique na guia **Processos**.
  - Para configurar o aplicativo Enterprise Data Preparation para usar um provedor de identidade, selecione o Serviço Enterprise Data Preparation e clique na guia **Processos**.
  - Para configurar o aplicativo Data Privacy Management para usar um provedor de identidade, selecione o Serviço do Data Privacy Management e clique na guia **Processos**.
3. Clique no ícone de edição ao lado de **Configuração SAML**.
4. Insira as propriedades necessárias para permitir que o aplicativo da Web use um provedor de identidade.

A tabela a seguir descreve as propriedades que você insere:

Propriedade	Descrição
URL de Provedor de Identidade	Opcional. A URL para o servidor do provedor de identidade. Você deve especificar a cadeia de URL completa.
ID do Provedor de Serviços	Opcional. O nome confiável da parte dependente ou o identificador do provedor de serviços para o domínio, conforme definido no provedor de identidade.
Alias do Certificado de Assinatura de Declaração	Opcional. O nome do alias especificado ao importar o certificado de assinatura de declaração do provedor de identidade para o arquivo truststore usado para a autenticação SAML.  Se você alterar o nome alternativo, importe o certificado correspondente para o arquivo truststore em cada nó do gateway e reinicie o nó.
Tolerância a Distorção do Relógio	Opcional. A diferença de tempo permitida entre o relógio do sistema host do provedor de identidade e o relógio do sistema no nó de gateway mestre.  Opcional. O tempo de vida dos tokens SAML emitidos pelo provedor de identidade é definido de acordo com o relógio do sistema host do provedor de identidade. O tempo de vida de um token SAML emitido pelo provedor de identidade será válido se a hora de início ou a hora de término definida no token estiver dentro do número de segundos especificado no relógio do sistema do nó de gateway mestre.  Os valores devem ser de 0 a 600 segundos. O padrão é 120 segundos.

A imagem a seguir mostra a configuração para permitir que o Enterprise Data Catalog use o PingFederate como provedor de identidade:

**Edit Ldadmin SAML Configuration** X

Fields marked with an asterisk (\*) are required.

Web Application ID	catalog_service_ldadmin
IDP URL	https://10.70.140.70:9031/idp/startSSO.saml2
Service Provider ID	PingFed_Dev
Assertion Signing Certificate Alias	pingfed_cert
Clock Skew Tolerance	240

? OK Cancel

5. Clique em **OK**.
6. Reinicie o aplicativo ou serviço de aplicativo depois de configurar um aplicativo para usar um provedor de identidade SAML.

## CAPÍTULO 6

# Segurança de domínio

Este capítulo inclui os seguintes tópicos:

- [Visão Geral da Segurança do Domínio, 80](#)
- [Secure Communication Within the Domain, 81](#)
- [Conexões Seguras com um Serviço de Aplicativo da Web, 93](#)
- [Pacotes de criptografia para o domínio Informatica, 97](#)
- [Origens e Destinos Seguros, 101](#)
- [Secure Data Storage, 103](#)
- [Serviços de Aplicativo e Portas, 106](#)

## Visão Geral da Segurança do Domínio

Você pode ativar opções no domínio Informatica para configurar a comunicação segura entre os componentes no domínio e entre o domínio e os componentes do cliente.

Você pode ativar opções diferentes para proteger componentes específicos no domínio. Não é necessário proteger todos os componentes no domínio. Por exemplo, você pode proteger a comunicação entre os serviços no domínio, mas não proteger a conexão entre o Serviço de Repositório do Modelo e o banco de dados do repositório.

O Informatica usa os protocolos TCP/IP e HTTP para comunicação entre componentes no domínio. O domínio usa certificados SSL para a comunicação segura entre componentes.

Ao instalar os serviços Informatica, você pode ativar a comunicação segura para eles no domínio e para a ferramenta Administrator. Após a instalação, você pode configurar a comunicação segura no domínio usando a ferramenta Administrator ou a linha de comando.

Durante a instalação, o instalador gera uma chave de criptografia para criptografar dados confidenciais, como senhas, que são armazenados no domínio. Após a instalação, você poderá alterar a chave de criptografia para dados confidenciais. Você deve atualizar o conteúdo dos repositórios para atualizar os dados criptografados.

Você pode ativar a comunicação segura nas seguintes áreas:

### **Domínio**

No domínio, você pode selecionar opções para ativar a comunicação segura para os seguintes componentes:

- Entre o Gerenciador de Serviços, os serviços no domínio e as ferramentas do cliente Informatica



- Entre o domínio e o repositório de configuração de domínio
- Entre os serviços de repositório e os bancos de dados do repositório
- Entre o Serviço de Integração do PowerCenter e os processos do DTM

#### Serviços de aplicativo da Web

Você pode proteger a conexão entre um serviço de aplicativo da Web, como o Serviço Analyst ou o Serviço do Hub de Operações REST, e o navegador.

#### Origens e destinos

Você pode ativar a comunicação segura entre o Serviço de Integração de Dados e o Serviço de Integração de Dados e os bancos de dados de origem e destino.

#### Armazenamento de dados

O Informatica criptografa dados confidenciais, como senhas, ao armazenar dados no domínio. O Informatica gera uma chave de criptografia durante a instalação. O Informatica usa a chave de criptografia para criptografar e descriptografar dados confidenciais que são armazenados no domínio.

## Secure Communication Within the Domain

You can use the Secure Communication option to secure the connection between services and between services and the service managers in the domain. Additionally, you can enable security for workflows and use secure databases for the repositories that you create in the domain.

After you secure the domain, configure the Informatica client applications to work with a secure domain.

#### Default Directory for Keystore and Truststore

The Informatica deployment includes default keystore and truststore files in the following default directory:

```
<Informatica installation directory>\services\shared\security
```

Informatica recommends that you use the default keystore and truststore only for setup and proof-of-concept use cases.

To secure a production environment, use the following guidelines:

- When you configure secure communication, do not modify, replace, or delete files in the default directory:  
`<Informatica installation directory>\services\shared\security`
- You cannot use the default keystore and truststore to configure other services or clients.
- Configure a custom keystore and truststore for secure communication in a location other than the default directory.
- If you replaced the default Informatica keystore and truststore files with custom keystore and truststore files in the previous Informatica installation directory structure, you must run the `infasetup UpdateGatewayNode` command to update the locations of the custom keystore and truststore for the domain.

## Comunicação Segura para Serviços e o Gerenciador de Serviços

Você pode configurar a comunicação segura dentro do domínio durante a instalação. Após a instalação, você poderá configurar a comunicação segura para o domínio na ferramenta Administrator ou pela linha de comando.

O Informatica oferece um certificado SSL que você pode usar para proteger o domínio. No entanto, você deve fornecer um certificado SSL para os domínios que exigem um nível mais alto de segurança, como um domínio em um ambiente de produção. Especifique os arquivos de armazenamento de chaves e truststore que contêm os certificados SSL que você deseja usar.

**Nota:** A Informatica oferece certificados SSL para fins de avaliação. Se você não fornecer um certificado SSL, a Informatica usará a mesma chave privada padrão para todas as instalações da Informatica. A segurança de seu domínio pode estar comprometida. Forneça um certificado SSL para garantir um alto nível de segurança para o domínio. O certificado fornecido pode ser autoassinado ou de uma autoridade de certificação (CA).

Ao configurar a comunicação segura para o domínio, você protege as conexões entre os seguintes componentes:

- O Gerenciador de Serviços e todos os serviços em execução no domínio
- O Serviço de Integração de Dados e o Serviço de Repositório do Modelo
- O Serviço de Integração de Dados e os processos de fluxo de trabalho
- O Serviço de Integração do PowerCenter e o Serviço do Repositório do PowerCenter
- Os serviços do domínio, as ferramentas do cliente Informatica e os programas de linha de comando

### Requirements for Secure Communication within the Domain

Before you enable secure communication within the domain, ensure that the following requirements are met:

#### **Você criou um CSR (Certificate Signing Request) e uma chave privada.**

Você pode usar o keytool ou o OpenSSL para criar o CSR e a chave privada.

Observe que a criptografia RSA requer mais de 512 bits.

#### **Você tem um certificado SSL assinado.**

O certificado pode ser autoassinado ou assinado pela CA. A Informatica recomenda um certificado assinado pela CA.

#### **Você importou o certificado para armazenamentos de chaves.**

Você deve ter um armazenamento de chaves no formato PEM denominado `infa_keystore.pem` e um armazenamento de chaves no formato JKS denominado `infa_keystore.jks`.

Os arquivos de armazenamento de chaves devem conter os certificados SSL raiz e intermediário.

**Nota:** A senha para o armazenamento de chaves no formato JKS deve ser igual à frase secreta da chave privada usada para gerar o certificado SSL.

#### **Você importou o certificado para truststores.**

Você deve ter um truststore no formato PEM denominado `infa_truststore.pem` e um truststore no formato JKS denominado `infa_truststore.jks`.

Os arquivos de truststore devem conter os certificados SSL raiz, intermediário e de usuário final.

#### **Os armazenamentos de chaves e os truststores estão no diretório correto.**

Se você habilitar a comunicação segura durante a instalação, o armazenamento de chaves e o truststore deverão estar em um diretório acessível ao instalador.

Se você habilitar a comunicação segura após a instalação, o armazenamento de chaves e truststore deverão estar em um diretório acessível para os programas de linha de comando.

#### **You enforced the HTTP Strict Transport Security (HSTS) response header.**

You can choose to enable HSTS response header in your domain to prevent man-in-the-middle (MITM) security threats. If you enable HSTS response header, you can stop HTTP redirects to HTTPS and ensure that only secured URLs (HTTPS) are accessed.

**Importante:** Informatica supports multiple applications and services running on both HTTP and HTTPS. If you enable this option, you cannot access the applications or services with HTTP URL.

To enable this option, set the `INFA_HSTS_HEADER_ENABLED` environment variable to `true` and import the certificates from `infa_truststore` and Informatica Administrator keystore to your browser.

### **Diretrizes para usar arquivos de truststore padrão e personalizados**

O instalador coloca os arquivos `infa_truststore.jks` e de armazenamento de chaves padrão no diretório `<diretório de instalação da Informatica>/services/shared/security` em cada nó. Você pode usar o truststore padrão para configuração e prova de conceito, mas os arquivos de truststore e armazenamento de chaves padrão fornecem segurança limitada. Para produção, a Informatica recomenda o uso de arquivos de truststore e armazenamento de chaves personalizados para comunicação mais segura e autenticação SAML.

Coloque os arquivos de truststore e armazenamento de chaves personalizados em um diretório personalizado. O nome do arquivo truststore deve ser `infa_truststore.jks`.

Não sobrescreva, exclua nem mova os arquivos de armazenamento confiável e de armazenamento de chaves padrão. Não coloque os arquivos de truststore e armazenamento de chaves personalizados no diretório `<diretório de instalação da Informatica>/services/shared/security`

Ao criar um alias para novos certificados e chaves privadas, não use o nome padrão "Informatica LLC", que é usado pelos arquivos de truststore e armazenamento de chaves padrão.

### **Diretrizes para a criação de certificados e arquivos de truststore e armazenamento de chaves personalizados**

Você pode usar a chave `keytool` Java e o utilitário de gerenciamento de certificados para criar um certificado SSL ou uma solicitação de assinatura de certificado (CSR), assim como armazenamentos de chaves e truststores no formato JKS.

O `keytool` está disponível no seguinte diretório nos nós de domínio:

```
<Informatica installation directory>\java\bin
```

Se os nós de domínio forem executados no AIX, você poderá usar o `keytool` fornecido com o IBM JDK para criar um certificado SSL ou uma Solicitação de Assinatura de Certificado (CSR), assim como armazenamentos de chaves e truststores:

1. Copie os arquivos de certificado para uma pasta local em um nó de gateway dentro do domínio Informatica.
2. Na linha de comando, acesse o local do utilitário `keytool` no nó.
3. Execute o utilitário `keytool` para importar o certificado.
4. Reinicie o nó.

### **Next Steps**

For more information about how to create a custom keystore and truststore and import certificates in your browser, see the Informatica How-To Library article [How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain](#):

<https://docs.informatica.com/data-quality-and-governance/data-quality/h2l/0700-how-to-create-keystore-and-truststore-files-for-secure-comm/abstract.html>

After you secure the domain, configure the Informatica client applications to work with a secure domain.

## Ativando a Comunicação Segura para o Domínio na Linha de Comando

Use os comandos `infacmd` e `infasetup` para ativar a comunicação segura no domínio. Após ativar a comunicação segura, você deverá reiniciar o domínio para a alteração entrar em vigor.

Para usar os arquivos de certificado SSL, especifique os arquivos de armazenamento de chaves ao executar o comando `infasetup`.

Para configurar a comunicação segura no domínio usando a linha de comando, execute os seguintes comandos:

### **infacmd isp UpdateDomainOptions**

Use o comando `UpdateDomainOptions` para definir o modo de comunicação segura do domínio.

### **infasetup UpdateGatewayNode**

Use o comando `UpdateGatewayNode` para habilitar a comunicação segura para o Gerenciador de Serviços em um nó de gateway de um domínio. Se o domínio tiver vários nós de gateway, execute o comando `UpdateGatewayNode` em cada nó de gateway.

### **infasetup UpdateWorkerNode**

Use o comando `UpdateWorkerNode` para habilitar a comunicação segura para o Gerenciador de Serviços em um nó de trabalho de um domínio. Se o domínio tiver vários nós de trabalho, execute o comando `UpdateWorkerNode` em cada nó de trabalho.

1. Verifique se o domínio que você deseja proteger está em execução.
2. Atualize o domínio.

Execute o seguinte comando com as opções e os argumentos necessários:

- Windows: `infacmd isp UpdateDomainOptions`
- UNIX: `infacmd.sh isp UpdateDomainOptions`

Para configurar a comunicação segura para o domínio, inclua a seguinte opção quando você executar o comando `infacmd`:

Opção	Argumento	Descrição
-DomainOptions -do	option_name=value	Defina a seguinte opção para configurar a comunicação segura no domínio: TLSMode=True

3. Desligue o domínio.  
O domínio deve ser desligado antes de você executar os comandos `infasetup`.
4. Execute o `infasetup` com as opções e os argumentos necessários.

Insira o seguinte comando:

- Windows: `infasetup UpdateGatewayNode` ou `infasetup UpdateWorkerNode`
- UNIX: `infasetup.sh UpdateGatewayNode` ou `infasetup.sh UpdateWorkerNode`

Para configurar a comunicação segura nos nós, execute os comandos com as seguintes opções:

Opção	Argumento	Descrição
-EnableTLS -tls	enable_tls	Configura a comunicação segura para os serviços no domínio Informatica.
-NodeKeystore -nk	node_keystore_directory	Opcional se você usar o certificado SSL padrão da Informatica. Obrigatório se você usar seu certificado SSL. Diretório que contém os arquivos de armazenamento de chaves. O domínio Informatica exige que o certificado SSL esteja no formato PEM e em arquivos Java Keystore (JKS). O diretório deve conter arquivos de armazenamento de chaves nos formatos PEM e JKS. Os arquivos de armazenamento de chaves devem ser denominados infa_keystore.jks e infa_keystore.pem  Você pode usar o mesmo arquivo de armazenamento de chaves para vários nós.
-NodeKeystorePass -nkp	node_keystore_password	Opcional se você usar o certificado SSL padrão da Informatica. Obrigatório se você usar seu certificado SSL. Senha do arquivo infa_keystore.jks.
-NodeTruststore -nt	node_truststore_directory	Opcional se você usar o certificado SSL padrão da Informatica. Diretório que contém os arquivos de truststore.  Você pode usar o mesmo arquivo de truststore para vários nós.
-NodeTruststorePass -ntp	node_truststore_password	Opcional se você usar o certificado SSL padrão da Informatica. Senha do arquivo infa_truststore.jks.

5. Execute o comando `infasetup` em cada nó no domínio.

Se você tiver vários nós de gateway no domínio, execute o comando `infasetup UpdateGatewayNode` em cada nó de gateway. Se você tiver vários nós de trabalho, execute o comando `infasetup UpdateWorkerNode` em cada nó de trabalho. Você deve usar os mesmos arquivos de armazenamento de chaves para todos os nós no domínio.

6. Reinicie o domínio.

## Ativando a Comunicação Segura para o Domínio na Ferramenta Administrator

Você pode usar a ferramenta Administrator para ativar a comunicação segura no domínio. Ao ativar a comunicação segura na ferramenta Administrator, você também deve executar os comandos `infasetup` para atualizar os nós.

Ao ativar a opção de Comunicação Segura na ferramenta Administrator, você também precisa executar o comando `infasetup` para atualizar os arquivos de configuração do Informatica em cada nó. Para especificar os arquivos de certificado SSL que serão usados, especifique os arquivos de armazenamento de chaves ao executar o comando `infasetup`.

Para atualizar os arquivos de configuração da Informatica em cada nó, use os seguintes comandos:

### infasetup UpdateGatewayNode

Use o comando UpdateGatewayNode para habilitar a comunicação segura para o Gerenciador de Serviços em um nó de gateway de um domínio. Se o domínio tiver vários nós de gateway, execute o comando UpdateGatewayNode em cada nó de gateway.

### infasetup UpdateWorkerNode

Use o comando UpdateWorkerNode para habilitar a comunicação segura para o Gerenciador de Serviços em um nó de trabalho de um domínio. Se o domínio tiver vários nós de trabalho, execute o comando UpdateWorkerNode em cada nó de trabalho.

Para ativar a comunicação segura no domínio da ferramenta Administrator, execute as seguintes etapas:

1. Na ferramenta Administrator, selecione o domínio.
2. No painel de conteúdo, clique na exibição **Propriedades**.
3. Vá para a seção **Propriedades Gerais** e clique em **Editar**.
4. Na janela **Editar Propriedades Gerais**, selecione **Ativar Comunicação Segura**.
5. Clique em **OK**.
6. Desligue o domínio.

O domínio deve ser desligado antes de você executar os comandos infasetup.

7. Execute o infasetup com as opções e os argumentos necessários.

Insira o seguinte comando:

- Windows: `infasetup UpdateGatewayNode` ou `infasetup UpdateWorkerNode`
- UNIX: `infasetup.sh UpdateGatewayNode` ou `infasetup.sh UpdateWorkerNode`

Para configurar a comunicação segura nos nós, execute os comandos com as seguintes opções:

Opção	Argumento	Descrição
-EnableTLS -tls	enable_tls	Configura a comunicação segura para os serviços no domínio Informatica.
-NodeKeystore -nk	node_keystore_directory	Opcional se você usar o certificado SSL padrão da Informatica. Obrigatório se você usar seu certificado SSL. Diretório que contém os arquivos de armazenamento de chaves. O domínio Informatica exige que o certificado SSL esteja no formato PEM e em arquivos Java Keystore (JKS). O diretório deve conter arquivos de armazenamento de chaves nos formatos PEM e JKS. Os arquivos de armazenamento de chaves devem ser denominados infa_keystore.jks e infa_keystore.pem Você pode usar o mesmo arquivo de armazenamento de chaves para vários nós.
-NodeKeystorePass -nkp	node_keystore_password	Opcional se você usar o certificado SSL padrão da Informatica. Obrigatório se você usar seu certificado SSL. Senha do arquivo infa_keystore.jks.

Opção	Argumento	Descrição
-NodeTruststore -nt	node_truststore_directory	Opcional se você usar o certificado SSL padrão da Informatica. Diretório que contém os arquivos de truststore.  Você pode usar o mesmo arquivo de truststore para vários nós.
-NodeTruststorePass -ntp	node_truststore_password	Opcional se você usar o certificado SSL padrão da Informatica. Senha do arquivo infa_truststore.jks.

8. Execute o comando infasetup em cada nó no domínio.

Se você tiver vários nós de gateway no domínio, execute o comando infasetup UpdateGatewayNode em cada nó de gateway. Se você tiver vários nós de trabalho, execute o comando infasetup UpdateWorkerNode em cada nó de trabalho. Você deve usar os mesmos arquivos de armazenamento de chaves para todos os nós no domínio.

9. Reinicie o domínio.

## Configurando os Aplicativos Cliente Informatica para Trabalhar com um Domínio de Segurança

Ao ativar a comunicação segura dentro do domínio, você também protege as conexões entre o domínio e os aplicativos cliente Informatica, como Developer tool. Talvez seja necessário especificar o local e a senha dos arquivos de truststore que você usar para proteger o domínio em variáveis de ambiente. Você pode definir as variáveis de ambiente em máquinas que hospedam aplicativos cliente que acessam serviços no domínio.

Certificados SSL que são usados para proteger um domínio Informatica estão contidos em arquivos de truststore `infa_truststore.jks` e `infa_truststore.pem`. Os arquivos de truststore devem estar disponíveis em cada host cliente.

Talvez seja necessário definir as seguintes variáveis de ambiente em cada host cliente:

### INFA\_TRUSTSTORE

Defina essa variável como o diretório que contém os arquivos de truststore `infa_truststore.jks` e `infa_truststore.pem`.

### INFA\_TRUSTSTORE\_PASSWORD

Defina essa variável como a senha do truststore. A senha deve ser criptografada. Use o programa de linha de comando `pmpasswd` para criptografar a senha.

A Informatica fornece um certificado SSL nos arquivos de truststore padrão que você pode usar para proteger o domínio. Quando você instala os clientes Informatica, o instalador define as variáveis de ambiente e instala os arquivos de truststore no seguinte diretório por padrão: <Diretório de instalação Informatica>\clients\shared\security

Se você usar o certificado SSL padrão da Informatica, e os arquivos `infa_truststore.jks` e `infa_truststore.pem` estiverem no diretório padrão, não será necessário definir as variáveis de ambiente `INFA_TRUSTSTORE` ou `INFA_TRUSTSTORE_PASSWORD`.

Você deve definir as variáveis de ambiente `INFA_TRUSTSTORE` e `INFA_TRUSTSTORE_PASSWORD` em cada host cliente nos seguintes cenários:

**É possível usar um certificado SSL personalizado para proteger o domínio.**

Se você fornecer um certificado SSL a ser usado para proteger o domínio, importe-o para os arquivos de truststore `infa_truststore.jks` e `infa_truststore.pem` e depois copie os arquivos de truststore para cada host cliente. Você deve especificar a localização dos arquivos e a senha do truststore.

**Importante:** se você enviar o processamento para um cluster de computação e o Serviço de Integração de Dados for executado em uma grade, importe os certificados uma vez e copie-os para cada Serviço de Integração de Dados na grade. Cada vez que você importa um certificado, o conteúdo do certificado é idêntico, mas os valores hexadecimais são diferentes. Como resultado, os mapeamentos simultâneos que são executados na grade falham com erros de inicialização.

**Você substitui os arquivos de truststore Informatica padrão pelos seus próprios arquivos de truststore no diretório padrão.**

Se você substituir os arquivos de truststore `infa_truststore.jks` e `infa_truststore.pem` padrão pelos seus próprios arquivos de truststore no diretório padrão Informatica, deverá especificar a senha do truststore. Os arquivos de truststore devem ter os mesmos nomes de arquivos que os arquivos de truststore padrão.

**Você usa o certificado SSL Informatica padrão, mas os arquivos de truststore não estão no diretório Informatica padrão.**

Se você usar o certificado SSL Informatica padrão, mas os arquivos de truststore `infa_truststore.jks` e `infa_truststore.pem` padrão não estiverem no diretório padrão, será necessário especificar a localização dos arquivos e a senha do truststore.

## Banco de Dados do Repositório de Configuração de Domínio Seguro

O repositório de configuração de domínio Informatica armazena informações de configuração, privilégios e permissões de contas de usuário. Ao criar um domínio Informatica, você deve criar um repositório de configuração de domínio.

Você pode criar um repositório de configuração de domínio em um banco de dados protegido com o protocolo SSL. O protocolo SSL usa certificados SSL armazenados em um arquivo de truststore. O acesso ao banco de dados seguro requer um truststore que contenha os certificados para o banco de dados.

Você pode criar um banco de dados do repositório de configuração de domínio seguro durante a instalação dos serviços Informatica e a criação de um domínio. Para obter mais informações sobre a configuração de um repositório de configuração de domínio seguro durante a instalação, consulte os guias de instalação da Informatica.

Após a instalação, você poderá configurar um banco de dados do repositório de configuração de domínio seguro usando a linha de comando.

**Nota:** Antes de configurar um banco de dados do repositório de configuração de domínio seguro após a instalação, você deve ativar a comunicação segura no domínio.

Você pode criar um repositório de configuração de domínio seguro nos seguintes bancos de dados:

- Oracle
- Microsoft SQL Server
- IBM DB2



## Configurando um Banco de Dados do Repositório de Configuração de Domínio Seguro

Após a instalação, você poderá alterar o repositório de configuração de domínio para um banco de dados seguro. Você poderá usar um banco de dados do repositório de configuração de domínio seguro somente se ativar a comunicação segura no domínio.

Você deve desligar o domínio antes de alterar o banco de dados do repositório de configuração de domínio. Use o comando `infasetup` para fazer backup do banco de dados do repositório de configuração de domínio e restaurá-lo em um banco de dados seguro. Ao restaurar o repositório de configuração de domínio no banco de dados seguro, especifique os parâmetros de segurança do banco de dados seguro. Em seguida, atualize o nó de gateway com as informações do repositório de configuração de domínio.

Para fazer backup e restaurar o banco de dados do repositório e atualizar o nó de gateway, use os seguintes comandos:

### **infasetup BackupDomain**

Use a opção `BackupDomain` para fazer backup dos dados do banco de dados do repositório de configuração de domínio.

### **infasetup RestoreDomain**

Use a opção `RestoreDomain` para restaurar os dados do repositório de configuração de domínio para um banco de dados seguro.

### **infasetup UpdateGatewayNode**

Use a opção `UpdateGatewayNode` para atualizar as configurações do repositório de configuração de domínio nos nós de gateway do domínio.

Para alterar o repositório de configuração de domínio para um banco de dados seguro, conclua as seguintes etapas:

1. Verifique se a comunicação segura está ativada no domínio.  
O domínio deve ser protegido antes de usar um banco de dados seguro para o repositório de configuração de domínio.
2. Desligue o domínio.
3. Execute o comando `infasetup BackupDomain` e especifique as informações de conexão de banco de dados.  
  
Quando você executa o comando `BackupDomain`, o `infasetup` faz backup de grande parte das tabelas de banco de dados de configuração de domínio para o nome de arquivo especificado.  
  
**Nota:** Se o comando de backup ou restauração do `infasetup` falhar com um erro de memória Java, aumente a memória do sistema disponível para o `infasetup`. Para aumentar a memória do sistema, defina o valor `-Xmx` na variável de ambiente `INFA_JAVA_CMD_OPTS`.
4. Use o utilitário de backup do banco de dados para fazer backup manualmente de outra tabela do repositório que o comando `infasetup` não faz.  
  
Faça backup do conteúdo da seguinte tabela:
  - `ISP_RUN_LOG`
5. Para restaurar o repositório de configuração de domínio no banco de dados seguro, execute o comando `infasetup RestoreDomain` e especifique as informações de conexão de banco de dados.

Além disso, para as informações de conexão, especifique as seguintes opções necessárias para o banco de dados seguro:

Opção	Argumento	Descrição
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Obrigatório. Indica se o banco de dados no qual o repositório de configuração de domínio será restaurado é um banco de dados seguro. Defina essa opção como Verdadeiro.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Obrigatório. Caminho e nome do arquivo de truststore que contém o certificado SSL do banco de dados.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Obrigatório. A senha do arquivo de truststore do banco de dados seguro.

Na string de conexão, inclua os seguintes parâmetros de segurança:

**EncryptionMethod**

Obrigatório. Indica se os dados estão criptografados quando são transmitidos na rede. Esse parâmetro deve ser definido como `SSL`.

**ValidateServerCertificate**

Opcional. Indica se a Informatica valida o certificado enviado pelo servidor de banco de dados.

Se esse parâmetro for definido como `True`, a Informatica validará o certificado enviado pelo servidor de banco de dados. Se você especificar o parâmetro `HostNameInCertificate`, a Informatica também validará o nome do host no certificado.

Se esse parâmetro for definido como `False`, a Informatica não validará o certificado enviado pelo servidor de banco de dados. A Informatica ignora todas as informações de truststore especificadas.

O padrão é Verdadeiro.

**HostNameInCertificate**

Opcional. O nome do host da máquina que hospeda o banco de dados seguro. Se você especificar um nome de host, o Informatica validará o nome do host incluído na string de conexão em relação ao nome do host no certificado SSL.

**cryptoProtocolVersion**

Necessário. Especifica o protocolo de criptografia para usar na conexão com um banco de dados seguro. Você pode definir o parâmetro como `cryptoProtocolVersion=TLSv1.1` ou `cryptoProtocolVersion=TLSv1.2`, de acordo com o protocolo de criptografia usado pelo servidor de banco de dados.

6. Use o utilitário de restauração do banco de dados para restaurar as tabelas do repositório das quais você fez backup manualmente.  
Restaure a seguinte tabela:
  - `ISP_RUN_LOG`
7. Para atualizar os nós no domínio com informações sobre o repositório de configuração de domínio seguro, execute o comando `infasetup UpdateGatewayNode` e especifique as informações de conexão de banco de dados seguro.

Além disso, para as opções de nó, especifique as seguintes opções necessárias para o banco de dados seguro:

Opção	Argumento	Descrição
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Obrigatório. Indica se o banco de dados usado para o repositório de configuração de domínio é um banco de dados seguro. Defina essa opção como Verdadeiro.
-DatabaseConnectionString -cs	database_connection_string	Obrigatório. String de conexão a ser usada para conexão com o banco de dados seguro. A string de conexão deve incluir os parâmetros de segurança que você incluiu na string de conexão ao executar o comando <code>infasetup RestoreDomain</code> na etapa <a href="#">5</a>
-DatabaseTruststorePassword -dbtp	database_truststore_password	Obrigatório. A senha do arquivo de truststore do banco de dados seguro.

Se você tiver vários nós de gateway no domínio, execute o comando `infasetup UpdateGatewayNode` em cada nó de gateway.

8. Reinicie o domínio.

## Banco de Dados do Repositório do PowerCenter Seguro

Ao criar um Serviço do Repositório do PowerCenter, você pode criar o repositório do PowerCenter associado em um banco de dados protegido com o protocolo SSL.

O Serviço do Repositório do PowerCenter conecta-se ao banco de dados do repositório do PowerCenter usando conectividade nativa.

Ao criar um repositório do PowerCenter em um banco de dados seguro, verifique se os arquivos do cliente de banco de dados contêm as informações de conexão segura do banco de dados. Por exemplo, se você criar um repositório do PowerCenter em um banco de dados Oracle seguro, configure os arquivos do cliente de banco de dados Oracle `tnsnames.ora` e `sqlnet.ora` com as informações de conexão segura.

## Banco de Dados do Repositório do Modelo Seguro

Ao criar um Serviço de Repositório do Modelo, você pode criar o repositório do Modelo associado em um banco de dados protegido com o protocolo SSL.

O Serviço de Repositório do Modelo conecta-se ao banco de dados do repositório do Modelo usando drivers JDBC.

1. Configure um banco de dados protegido com o protocolo SSL.
2. Na ferramenta Administrator, crie um Serviço de Repositório do Modelo.
3. Na caixa de diálogo **Novo Serviço de Repositório do Modelo**, insira as propriedades gerais do Serviço de Repositório do Modelo e clique em **Avançar**.
4. Insira as propriedades do banco de dados e a string de conexão JDBC para o Serviço de Repositório do Modelo.

Para conectar-se a um banco de dados seguro, insira os parâmetros do banco de dados seguro no campo **Parâmetros JDBC Seguros**. O Informatica trata o valor do campo **Parâmetros JDBC Seguros** como dados confidenciais e armazena a string do parâmetro criptografada.

A seguinte lista descreve os parâmetros do banco de dados seguro:

#### **EncryptionMethod**

Obrigatório. Indica se os dados estão criptografados quando são transmitidos na rede. Esse parâmetro deve ser definido como `SSL`.

#### **ValidateServerCertificate**

Opcional. Indica se a Informatica valida o certificado enviado pelo servidor de banco de dados.

Se esse parâmetro for definido como `True`, a Informatica validará o certificado enviado pelo servidor de banco de dados. Se você especificar o parâmetro `HostNameInCertificate`, a Informatica também validará o nome do host no certificado.

Se esse parâmetro for definido como `False`, a Informatica não validará o certificado enviado pelo servidor de banco de dados. A Informatica ignora todas as informações de truststore especificadas.

O padrão é `Verdadeiro`.

#### **HostNameInCertificate**

Opcional. O nome do host da máquina que hospeda o banco de dados seguro. Se você especificar um nome de host, o Informatica validará o nome do host incluído na string de conexão em relação ao nome do host no certificado SSL.

#### **cryptoProtocolVersion**

Necessário. Especifica o protocolo de criptografia para usar na conexão com um banco de dados seguro. Você pode definir o parâmetro como `cryptoProtocolVersion=TLSv1.1` ou `cryptoProtocolVersion=TLSv1.2`, de acordo com o protocolo de criptografia usado pelo servidor de banco de dados.

#### **TrustStore**

Obrigatório. O caminho e o nome do arquivo truststore que contém o certificado SSL do banco de dados.

Se você não incluir o caminho para o arquivo de truststore, o Informatica procurará o arquivo no seguinte diretório padrão: `<InformaticaInstallationDirectory>/tomcat/bin`

#### **TrustStorePassword**

Obrigatório. A senha do arquivo truststore do banco de dados seguro.

**Nota:** O Informatica anexa os parâmetros JDBC seguros à string de conexão JDBC. Se você incluir os parâmetros JDBC seguros diretamente na string de conexão, não insira nenhum parâmetro no campo **Parâmetros JDBC Seguros**.

5. Teste a conexão com o banco de dados do repositório seguro para verificar se é válida.
6. Conclua o processo para criar um Serviço de Repositório do Modelo.

## Comunicação Segura para Fluxos de Trabalho e Sessões

Por padrão, quando você ativa a opção de comunicação segura no domínio, o Informatica protege a conexão entre o Serviço de Integração de Dados e o Serviço de Integração do PowerCenter e os processos do DTM.

Além disso, se você executar sessões do PowerCenter em uma grade, poderá ativar uma opção para proteger a comunicação de dados entre os processos do DTM.

Para ativar a comunicação de dados segura entre os processos do DTM nas sessões do PowerCenter, selecione a opção **Ativar Criptografia de Dados** para o Serviço de Integração do PowerCenter.

**Nota:** As sessões do PowerCenter exigem mais CPU e memória quando os processos do DTM são executados no modo seguro. Antes de ativar a comunicação de dados segura entre os processos do DTM para as sessões do PowerCenter, determine se os recursos do domínio são adequados à carga adicional.

## Ativando a Comunicação Segura para Processos do DTM do PowerCenter

Para proteger a conexão entre os processos do DTM nas sessões do PowerCenter executadas em uma grade, configure o Serviço de Integração do PowerCenter para ativar a criptografia de dados nos processos do DTM.

1. No Navegador da ferramenta Administrator, selecione o Serviço de Integração do PowerCenter.
2. No painel de conteúdo, clique na exibição Propriedades.
3. Vá para a seção Propriedades do Serviço de Integração do PowerCenter e clique em Editar.
4. Na janela **Editar Propriedades do Serviço de Integração do PowerCenter**, selecione **Ativar Criptografia de Dados**.
5. Clique em **OK**.

Quando você executar uma sessão do PowerCenter em uma grade, os processos do DTM enviarão dados criptografados ao se comunicarem com outros processos do DTM.

# Conexões Seguras com um Serviço de Aplicativo da Web

Para proteger dados que são transmitidos entre um serviço de aplicativo da Web e o navegador, proteja a conexão entre o serviço de aplicativo da Web e o navegador.

Você pode proteger as seguintes conexões:

### Conexões com a ferramenta Administrator

Você pode proteger a conexão entre a ferramenta Administrator e o navegador.

### Conexões com serviços de aplicativo da Web

Você pode proteger a conexão entre os seguintes serviços de aplicativo da Web e o navegador:

- Serviço Analyst
- Serviço do Metadata Manager
- Serviço do Hub de Operações REST
- Serviço do Test Data Manager
- Serviço de Console do Hub de Serviços da Web

## Requisitos para Conexões Seguras para Serviços de Aplicativo da Web

Antes de proteger a conexão com um serviço de aplicativo da Web, certifique-se de que os seguintes requisitos sejam atendidos:

**Você criou um CSR (Certificate Signing Request) e uma chave privada.**

Você pode usar o keytool ou o OpenSSL para criar o CSR e a chave privada.

Observe que a criptografia RSA requer mais de 512 bits.

**Você tem um certificado SSL assinado.**

O certificado pode ser autoassinado ou assinado pela CA. A Informatica recomenda um certificado assinado pela CA.

**Você importou o certificado para um armazenamento de chaves no formato JKS.**

Um armazenamento de chaves deve conter apenas um certificado. Se você usar um certificado exclusivo para cada serviço de aplicativo da Web, crie um armazenamento de chaves separado para cada certificado. Como alternativa, você pode usar um armazenamento de chaves e um certificado compartilhados.

Se você usar o certificado SSL gerado pelo instalador para a ferramenta Administrator, não será necessário importar o certificado para um armazenamento de chaves no formato JKS.

**O armazenamento de chaves está em um diretório acessível.**

O armazenamento de chaves deve estar em um diretório acessível para a ferramenta Administrator e os programas de linha de comando.

## Ativando Conexões Seguras para a Ferramenta Administrator

Após a instalação, você pode configurar conexões seguras para a ferramenta Administrator na linha de comando.

Você deve atualizar os nós de gateway no domínio com as propriedades de uma conexão segura entre o navegador e o serviço Informatica Administrator.

Para atualizar o nó de gateway com as propriedades da conexão segura, execute o seguinte comando:

```
infasetup UpdateGatewayNode
```

Inclua as seguintes opções:

Opção	Argumento	Descrição
-HttpsPort -hs	AdminConsole_https_port	Número de porta a ser usada para uma conexão segura com o serviço Informatica Administrator.
-KeystoreFile -kf	AdminConsole_Keystore_File	Caminho e nome do arquivo de armazenamento de chaves a serem usados na conexão HTTPS com o serviço Informatica Administrator.
-KeystorePass -kp	AdminConsole_Keystore_Password	Senha do arquivo de armazenamento de chaves.

Se você tiver vários nós de gateway no domínio, execute o comando em cada um deles.

## Serviços de Aplicativo da Web Informatica

Configure uma conexão segura para um serviço de aplicativo da Web ao criá-lo ou configurá-lo. Cada serviço de aplicativo tem propriedades específicas para a conexão HTTPS segura.

## Segurança para a Ferramenta Analyst

Ao criar o Serviço Analyst, você pode configurar as propriedades HTTPS seguras para a ferramenta Analyst.

Para proteger a conexão entre o navegador e o Serviço Analyst, configure as seguintes propriedades do Serviço Analyst:

Propriedade	Descrição
Ativar Comunicação Segura	Selecione para ativar uma conexão segura entre a ferramenta Analyst e o Serviço Analyst.
Porta HTTPS	O número de porta na qual o aplicativo da Web Informatica Analyst é executado quando você ativa o protocolo Transport Layer Security (TLS). Use um número de porta diferente do número de porta HTTP.
Arquivo de Armazenamento de Chaves	O diretório onde o arquivo de armazenamento de chaves que contém os certificados digitais é armazenado.
Senha do Armazenamento de Chaves	Senha contendo somente texto simples para o arquivo de armazenamento de chaves. Se esta propriedade não for definida, o Serviço Analyst usará a senha padrão <i>changeit</i> .
Protocolo SSL	A Informatica recomenda que você deixe este campo em branco. A versão do TLS ativada depende do valor. Um campo em branco permite que a versão mais recente do TLS esteja disponível. Se você inserir um valor, versões anteriores do TLS poderão ser ativadas. O comportamento é baseado na versão Java para seu ambiente.  Para obter mais informações, consulte a documentação sobre sua versão Java.

## Segurança para o Serviço do Hub de Operações REST

Ao usar o Serviço do Hub de Operações REST, você pode configurar as propriedades HTTPS seguras para o Hub de Operações REST.

Para proteger a conexão entre o navegador e o Serviço do Hub de Operações REST, configure as seguintes propriedades do Serviço do Hub de Operações REST:

Propriedade	Descrição
Porta HTTP	Número exclusivo de porta HTTP para o processo do Serviço do Hub de Operações REST quando o serviço usa o protocolo HTTP. O padrão é 6555.
Porta HTTPS	O número da porta na qual o Serviço do Hub de Operações REST é executado quando você ativa o protocolo Transport Layer Security (TLS). Use um número de porta que não seja o número da porta HTTP.
Habilitar TLS	Selecione para ativar uma conexão segura entre o Serviço do Hub de Operações REST e o cliente REST.
Arquivo de armazenamento de chaves	Diretório no qual é armazenado o arquivo de armazenamento de chaves que contém os certificados digitais.

Propriedade	Descrição
Senha do armazenamento de chaves	Senha contendo somente texto simples para o arquivo de armazenamento de chaves. Se essa propriedade não estiver configurada, o Serviço do Hub de Operações REST usará a senha padrão.
Protocolo SSL	Um campo em branco permite que a versão mais recente do TLS esteja disponível. A versão do TLS ativada depende do valor. Se você inserir um valor, versões anteriores do TLS poderão ser ativadas. O comportamento é baseado na versão Java para seu ambiente. Para obter mais informações, consulte a documentação sobre sua versão Java.

## Segurança para o Console do Hub de Serviços da Web

Ao criar o Serviço do Web Services Hub, você pode configurar as propriedades HTTPS seguras para o console do Hub de Serviços da Web.

Para proteger a conexão entre o navegador e o Serviço do Web Services Hub, configure as seguintes propriedades do Serviço do Web Services Hub:

Propriedade	Descrição
URLScheme	Indica o protocolo de segurança configurado para o Hub de Serviços da Web: <ul style="list-style-type: none"> <li>- HTTP. Executa o Hub de Serviços da Web somente em HTTP.</li> <li>- HTTPS. Executa o Hub de Serviços da Web somente em HTTPS.</li> <li>- HTTP e HTTPS. Executa o Hub de Serviços da Web nos modos HTTP e HTTPS.</li> </ul>
HubPortNumber (https)	Número da porta do Hub de Serviços da Web em HTTPS. Aparece quando o esquema de URL selecionado inclui HTTPS. Obrigatório, se você executar o Hub de Serviços da Web em HTTPS. O padrão é 7343.
Arquivo de Armazenamento de Chaves	Caminho e nome do arquivo de armazenamento de chaves que contém as chaves e os certificados necessários para uma conexão HTTPS.
Senha de Armazenamento de Chaves	Senha do arquivo de armazenamento de chaves. Se essa propriedade não for definida, o Hub de Serviços da Web usará a senha padrão <i>changeit</i> .



## Segurança do Metadata Manager

Ao criar o Serviço do Metadata Manager, você pode configurar as propriedades HTTPS seguras para o aplicativo da Web Metadata Manager.

Para proteger a conexão entre o navegador e o Serviço do Metadata Manager, configure as seguintes propriedades do Serviço do Metadata Manager:

Propriedade	Descrição
Ativar o Secure Sockets Layer	Indica que você deseja configurar uma conexão segura para o aplicativo da Web do Metadata Manager. <b>Nota:</b> Esta propriedade é exibida quando você cria um Serviço do Metadata Manager. Para proteger a conexão para um Serviço do Metadata Manager, defina a propriedade de configuração <b>Esquema de URL</b> como HTTPS.
Número de Porta	Número da porta em que o aplicativo Metadata Manager é executado. O padrão é 10250.
Arquivo de Armazenamento de Chaves	Arquivo de armazenamento de chaves que conterá as chaves e os certificados necessários se você configurar uma conexão segura para o aplicativo da Web do Metadata Manager. <b>Nota:</b> O Serviço do Metadata Manager usa criptografia RSA. Portanto, a Informatica recomenda o uso de um certificado de segurança que foi gerado com o algoritmo RSA.
Senha do Armazenamento de Chaves	Senha do arquivo de armazenamento de chaves.

## Pacotes de criptografia para o domínio Informatica

Você pode configurar os pacotes de criptografia que o domínio Informatica usa quando ele criptografa as conexões no domínio Informatica. As conexões do domínio Informatica para recursos fora do domínio não são afetadas pela configuração do pacote de criptografia.

Ao ativar a comunicação segura para o domínio Informatica ou as conexões seguras para os serviços de aplicativo da Web, o domínio Informatica usa os pacotes de criptografia para criptografar o tráfego.

A Informatica cria a lista efetiva de pacotes de criptografia usados por ela com base nas seguintes lista:

### Lista negra

Lista de pacotes de criptografia que você deseja que o domínio Informatica bloqueie. Quando você coloca um pacote de criptografia na lista negra, o domínio Informatica remove o pacote de criptografia da lista efetiva. Você pode adicionar pacotes de criptografia que estão na lista padrão à lista negra.

### Lista padrão

Lista de pacotes de criptografia que o domínio Informatica oferece suporte por padrão. Se você não configurar uma lista branca ou negra, o domínio Informatica usará a lista padrão como a lista efetiva.

Para obter mais informações, consulte [“Lista padrão de pacotes de criptografia” na página 98](#)

### Lista branca

Lista de pacotes de criptografia que você deseja que o domínio Informatica ofereça suporte. Quando você adiciona um pacote de criptografia à lista branca, o domínio Informatica adiciona o pacote de criptografia à lista efetiva. Você não precisa adicionar pacotes de criptografia que estão na lista padrão à lista branca.

A Informatica cria a lista efetiva ao adicionar pacotes de criptografia da lista branca à lista padrão e ao remover pacotes de criptografia que estão na lista negra da lista padrão.

Considere as seguintes diretrizes para a lista efetiva:

- Para usar uma lista efetiva personalizada para conexões seguras em clientes da Web, o domínio Informatica deve usar a comunicação segura no domínio. Se o domínio não usar a comunicação segura, a Informatica usará a lista padrão como a lista efetiva.
- A lista efetiva somente controla conexões no domínio Informatica. Conexões a fontes de dados não usam a lista efetiva.
- A lista efetiva deve conter pelo menos um pacote de criptografia com suporte no TLS v1.2 ou 1.3.
- A lista efetiva deve ser um pacote de criptografia válido para Windows, Java Runtime Environment e OpenSSL.

## Criar as listas de pacote de criptografia

Para configurar o domínio Informatica para usar conjuntos de criptografia específicos, crie uma lista de permissões especificando os pacotes de criptografia adicionais aos quais oferecer suporte. Você também pode criar uma lista negra especificando os pacotes de criptografia a serem bloqueados.

Trabalhe com seu administrador de segurança de rede para determinar os pacotes de criptografia adequados para o domínio Informatica.

A lista de pacotes de criptografia deve ser uma lista separada por vírgula. Use os nomes da IANA (Internet Assigned Numbers Authority) nos pacotes de criptografia na lista. Como alternativa, você pode usar uma expressão regular Java.

Você configurar a lista de permissões e a lista negra com infasetup. Você pode fornecer as listas diretamente nos parâmetros de comando ou especificar arquivos de texto simples que contêm listas separadas por vírgula.

O seguinte texto de amostra exibe uma lista com dois pacotes de criptografia:

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Você pode configurar as listas branca e negra dos pacotes de criptografia para o domínio Informatica ao criar o domínio. Use infasetup para criar o domínio Informatica, os nós de gateway e os nós de trabalho. Para obter mais informações sobre os comandos infasetup, consulte a *Referência de comandos da Informatica*.

Como alternativa, você pode configurar as listas branca e negra para um domínio Informatica existente.

## Lista padrão de pacotes de criptografia

Por padrão, o domínio Informatica usa os seguintes pacotes de criptografia para a comunicação segura no domínio e conexões seguras do cliente:

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_AES\_128\_CCM\_SHA256
- TLS\_AES\_128\_CCM\_8\_SHA256
- 
- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256

## Ativar o TLS 1.3

Atualize as criptografias para o TLS 1.3.

Se você atualizar as criptografias para um domínio recém-definido ou um domínio existente, execute as seguintes etapas:

1. Desligue o domínio.
2. Para atualizar as criptografias do domínio, execute o seguinte comando:  

```
./infasetup.sh updateDomainCiphers -cwl -cbl
```
3. Para atualizar o nó de gateway, execute o seguinte comando:  

```
./infasetup.sh updategatewaynode -cwl -cbl
```
4. Reinicie o domínio.

## Configure o domínio Informatica com uma nova lista efetiva de pacotes de criptografia

Para configurar os pacotes de criptografia usados pelo domínio Informatica, você deve atualizar o domínio Informatica, todos os nós de gateway e todos os nós do funcionário com as mesmas listas branca e negra.

**Nota:** Alterações na lista negra, na lista branca e na lista efetiva não são cumulativas. A Informatica cria uma nova lista efetiva com base na lista negra, na lista padrão e na lista branca quando você executa o comando. A nova lista efetiva substitui a lista anterior.

Para configurar um domínio Informatica existente com uma nova lista efetiva de pacotes de criptografia, realize as seguintes etapas:

1. Desative o domínio Informatica.
2. Opcionalmente, execute o comando `infasetup listDomainCiphers` para exibir a lista de pacotes de criptografia que um domínio ou nó oferece suporte ou bloqueia.  
  
Por exemplo, execute o seguinte comando para exibir todas as listas de pacotes de criptografia:  

```
infasetup listDomainCiphers -l ALL -dc true
```
3. Execute o comando `infasetup updateDomainCiphers` em um nó de gateway e especifique uma lista branca, uma lista negra, ou ambas.

Por exemplo, execute o seguinte comando para adicionar um pacote de criptografia à lista efetiva e remova dois pacotes de criptografia da lista efetiva:

```
infasetup updateDomainCiphers -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

4. Execute o comando `infasetup updateGatewayNode` em cada nó de gateway e especifique uma lista branca, uma lista negra, ou ambas.

Use a mesma lista branca e lista negra como o domínio.

Por exemplo, execute o seguinte comando:

```
infasetup updateGatewayNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

5. Atualize cada nó do funcionário com o mesmo conjunto de pacotes de criptografia como o domínio Informatica.

Use a mesma lista branca e lista negra como o domínio.

Por exemplo, execute o seguinte comando:

```
infasetup updateWorkerNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

6. Inicie o domínio Informatica.
7. Opcionalmente, execute o comando `infacmd isp listDomainCiphers` para exibir a lista de pacotes de criptografia usados por um domínio ou nó.  
  
Por exemplo, execute o seguinte comando para exibir a lista efetiva de pacotes de criptografia usada pelo domínio:

```
infacmd isp listDomainCiphers -l EFFECTIVE
```

## Origens e Destinos Seguros

O Informatica usa objetos de conexão para se conectar a bancos de dados relacionais como origem ou destino. Você pode criar um objeto de conexão com um banco de dados relacional protegido com um certificado SSL.

Crie objetos de conexão do PowerCenter no Workflow Manager. Crie conexões de Serviço de Dados, Qualidade de Dados ou Criação de Perfil na Developer tool ou na ferramenta Administrator.

Você pode criar uma conexão com uma origem ou destino seguro nos seguintes bancos de dados:

- Oracle
- Microsoft SQL Server
- IBM DB2

## Origens e Destinos do Serviço de Integração de Dados

Quando você cria um objeto de conexão para o Serviço de Integração de Dados para processar mapeamentos, perfis de dados, scorecards ou serviços de dados SQL, é possível definir uma conexão com um banco de dados protegido pelo protocolo SSL.

O Serviço de Integração de Dados conecta-se ao banco de dados de origem ou destino por meio de drivers JDBC. Ao configurar a conexão com um banco de dados do repositório seguro, você deve incluir os parâmetros da conexão segura na string de conexão JDBC.

1. Configure um banco de dados protegido com o protocolo SSL para usar como origem ou destino.
2. Na ferramenta Administrator, crie uma conexão.
3. Na caixa de diálogo **Nova Conexão**, selecione o tipo de conexão. Clique em **OK**.

Você pode criar uma conexão com um banco de dados seguro DB2, Microsoft SQL Server ou Oracle.

4. Na caixa de diálogo **Nova Conexão - Etapa 1 de 3**, insira as propriedades da conexão e clique em **Avançar**.

5. Na página **Nova Conexão - Etapa 2 de 3**, insira a string de conexão com o banco de dados.

Para conectar-se a um banco de dados seguro, insira os parâmetros do banco de dados seguro no campo **Opções de Segurança de JDBC Avançadas**. O Informatica trata o valor do campo **Opções de Segurança de JDBC Avançadas** como dados confidenciais e armazena a string do parâmetro criptografada.

A seguinte lista descreve os parâmetros do banco de dados seguro:

### **EncryptionMethod**

Obrigatório. Indica se os dados estão criptografados quando são transmitidos na rede. Esse parâmetro deve ser definido como `SSL`.

**ValidateServerCertificate**

Opcional. Indica se a Informatica valida o certificado enviado pelo servidor de banco de dados.

Se esse parâmetro for definido como True, a Informatica validará o certificado enviado pelo servidor de banco de dados. Se você especificar o parâmetro HostNameInCertificate, a Informatica também validará o nome do host no certificado.

Se esse parâmetro for definido como False, a Informatica não validará o certificado enviado pelo servidor de banco de dados. A Informatica ignora todas as informações de truststore especificadas.

O padrão é Verdadeiro.

**HostNameInCertificate**

Opcional. O nome do host da máquina que hospeda o banco de dados seguro. Se você especificar um nome de host, o Informatica validará o nome do host incluído na string de conexão em relação ao nome do host no certificado SSL.

**TrustStore**

Obrigatório. O caminho e o nome do arquivo truststore que contém o certificado SSL do banco de dados.

**TrustStorePassword**

Obrigatório. A senha do arquivo truststore do banco de dados seguro.

**Nota:** O Informatica anexa os parâmetros JDBC seguros à string de conexão. Se você incluir os parâmetros JDBC seguros diretamente na string de conexão, não insira nenhum parâmetro no campo **Opções de Segurança de JDBC Avançadas**.

6. Teste a conexão com o banco de dados seguro para verificar se é válida.
7. Conclua o processo para criar a conexão relacional.

## Origens e Destinos do PowerCenter

Ao criar um objeto de conexão em uma sessão do PowerCenter, você pode definir uma conexão com um banco de dados protegido com o protocolo SSL.

Você pode se conectar a origens e destinos relacionais do PowerCenter usando conectividade nativa ou drivers ODBC.

Se você se conectar a uma origem ou destino relacional seguro por conectividade nativa, verifique se o cliente de banco de dados contém as informações de conexão do banco de dados seguro. Por exemplo, se você se conectar a um destino do PowerCenter em um banco de dados Oracle seguro, configure o arquivo do cliente de banco de dados Oracle *tnsnames.ora* com as informações de conexão do banco de dados seguro.

Se você se conectar a uma origem ou destino relacional seguro usando drivers ODBC, verifique se o cliente de banco de dados contém as informações de conexão do banco de dados seguro e se a fonte de dados ODBC define corretamente a conexão com o banco de dados seguro.

# Secure Data Storage

Informatica encrypts sensitive data, such as passwords and secure connection parameters, before it stores the data in the domain configuration repository. Informatica uses an encryption key to encrypt sensitive data.

During installation, the installer generates the encryption key for the domain. All nodes in a domain must use the same encryption key. If you install on multiple nodes, the installer uses the same encryption key for all nodes in the domain. For more information about generating an encryption key for the domain during installation, see the Informatica installation guides.

After installation, you can change the encryption key for the domain. Run the `infasetup` command to generate an encryption key and change the encryption key for the domain. After you change the encryption key for the domain, you must upgrade the content of the repositories in the domain to update the encrypted data.

**Nota:** You must keep the encryption key file in a secure location. The encryption key is required when you change the encryption key for the domain or move a repository to another domain.

## Diretório Seguro no UNIX

Quando você instala a Informatica, o instalador cria um diretório para armazenar arquivos da Informatica que exigem acesso restrito, como o arquivo de chave de criptografia de domínio. No UNIX, o instalador atribui diferentes permissões para o diretório e os arquivos no diretório.

Por padrão, o instalador cria o seguinte diretório no diretório de instalação da Informatica para armazenar a chave de criptografia: `<INFA_HOME>/isp/config/keys`

O diretório `/keys` contém o arquivo de chave de criptografia do nó. Se você configurar o domínio para usar a autenticação Kerberos, o diretório conterá os arquivos de keytab Kerberos.

Durante a instalação, você pode especificar um diretório diferente para armazenar o arquivo de criptografia. O instalador atribui as mesmas permissões ao diretório especificado como diretório padrão.

O diretório `/keys` e os arquivos no diretório têm as seguintes permissões:

### Permissões de Diretório

O proprietário do diretório tem permissões `-wx` para o diretório, mas nenhuma permissão `r`. O proprietário do diretório é a conta de usuário usada para executar o instalador. O grupo ao qual o proprietário pertence também tem permissões `-wx` para o diretório, mas nenhuma permissão `r`.

Por exemplo, a conta de usuário `ediqa` possui o diretório e pertence ao grupo `infaadmin`. A conta de usuário `ediqa` e o grupo `infaadmin` têm as seguintes permissões: `-wx-wx---`

A conta de usuário `ediqa` e o grupo `infaadmin` podem gravar e executar arquivos no diretório. Eles não podem exibir a lista de arquivos no diretório, mas podem listar um determinado arquivo por nome.

Se você souber o nome de um arquivo no diretório, poderá copiar o arquivo do diretório para outra localização. Se você não souber o nome do arquivo, deverá alterar a permissão do diretório para incluir a permissão de leitura antes que possa copiar o arquivo. Você pode usar o comando `chmod 730` para conceder a permissão de leitura para o proprietário do diretório e dos subdiretórios.

Por exemplo, você precisa copiar o arquivo de chave de criptografia denominado `siteKey` para um diretório temporário para disponibilizá-lo para outro nó no domínio. Execute o comando `chmod 730` no diretório `<diretório de instalação do Informatica>/isp/config` para atribuir as seguintes permissões: `rwX-wX---`. Você pode copiar o arquivo de chave de criptografia do subdiretório `/keys` para outro diretório.

Depois de concluir a cópia dos arquivos, altere as permissões do diretório de volta para gravação e execute as permissões. Você pode usar o comando `chmod 330` para remover a permissão de leitura.

**Nota:** Não use a opção -R para alterar recursivamente as permissões do diretório e dos arquivos. O diretório e os arquivos no diretório têm permissões diferentes.

#### Permissões de Arquivo

O proprietário dos arquivos no diretório tem permissões `rwx` para os arquivos. O proprietário dos arquivos no diretório é a conta de usuário usada para executar o instalador. O grupo ao qual o proprietário pertence também tem permissões `rwx` para os arquivos no diretório.

O proprietário e o grupo têm acesso completo ao arquivo e podem exibir ou editar o arquivo no diretório.

**Nota:** Você deve saber o nome do arquivo para poder listá-lo ou editá-lo.

## Alterando a Chave de Criptografia da Linha de Comando

Após a instalação, você poderá alterar a chave de criptografia do domínio usando a linha de comando. Você deve desligar o domínio antes de alterar a chave de criptografia.

Use o comando `infasetup` para gerar uma chave de criptografia e configure o domínio para usar a nova chave de criptografia.

Os seguintes comandos `infasetup` geram e alteram a chave de criptografia:

#### **generateEncryptionKey**

Gera uma chave de criptografia em um arquivo denominado *sitekey*. Se o diretório especificado para a chave de criptografia tiver um arquivo denominado *sitekey*, o Informatica irá renomeá-lo como *siteKey\_old*.

#### **migrateEncryptionKey**

Altera a chave de criptografia usada para armazenar dados confidenciais no domínio Informatica.

Para alterar a chave de criptografia de um domínio, conclua as etapas a seguir:

1. Desligue o domínio.
2. Faça backup do domínio antes de alterar a chave de criptografia.  
Para garantir que você possa recuperar o domínio em caso de problemas ao alterar a chave de criptografia, faça backup do domínio antes de executar os comandos `infasetup`.
3. Para gerar uma chave de criptografia para o domínio, execute o comando `infasetup generateEncryptionKey`.

Especifique a opção `encryptionKeyLocation` para gerar uma chave de criptografia:

Opção	Argumento	Descrição
<code>-encryptionKeyLocation</code> <code>-kl</code>	<code>encryption_key_location</code>	Diretório que contém a chave de criptografia atual. O nome do arquivo de criptografia é <i>sitekey</i> .  O Informatica renomeia o arquivo <i>sitekey</i> atual para <i>sitekey_old</i> e gera uma chave de criptografia em um novo arquivo denominado <i>sitekey</i> no mesmo diretório.

**Nota:** O instalador cria uma chave de criptografia durante a instalação e a atualização. Você não precisa das opções de palavra-chave e nome de domínio ao gerar o arquivo de criptografia *sitekey*. Certifique-se de salvar uma cópia da chave exclusiva do site. Se você perder a chave do site, não poderá gerá-la novamente. Não compartilhe a chave exclusiva do site com outras pessoas.



4. Para alterar a chave de criptografia do domínio, execute o comando `infasetup migrateEncryptionKey` e especifique a localização da chave de criptografia antiga e nova.

Especifique as seguintes opções necessárias para alterar a chave de criptografia do domínio:

Opção	Argumento	Descrição
<code>-LocationOfEncryptionKeys</code> <code>-loc</code>	<code>location_of_encryption_keys</code>	<p>Diretório no qual o arquivo de chaves de criptografia antigo denominado <i>siteKey_old</i> e o arquivo de chaves de criptografia novo denominado <i>siteKey</i> estão armazenados.</p> <p>O diretório deve incluir os arquivos de chave de criptografia antigo e novo. Se os arquivos de chave de criptografia antigo e novo estiverem armazenados em diretórios diferentes, copie-os no mesmo diretório.</p> <p>Se o domínio tiver vários nós, esse diretório deverá estar acessível a qualquer nó no domínio em que você executar o comando <code>migrateEncryptionKey</code>.</p> <p>Quando você migra um domínio multinó, todos os nós do domínio devem usar a mesma chave de criptografia. Para alterar a chave de criptografia do domínio, execute o comando <code>infasetup migrateEncryptionKey</code> em todos os nós no domínio.</p> <p><b>Nota:</b> No UNIX, o nome de arquivo <i>siteKey_old</i> faz distinção entre maiúsculas e minúsculas. Se você renomear manualmente o arquivo de chave de criptografia anterior, verifique se o nome de arquivo apresenta a capitalização correta.</p>
<code>-IsDomainMigrated</code> <code>-mig</code>	<code>is_domain_migrated</code>	<p>Indica se o domínio foi atualizado para usar a chave de criptografia mais recente.</p> <p>Quando você executar o comando <code>migrateEncryptionKey</code> pela primeira vez, defina essa opção como <code>False</code> (Falso) para indicar que o domínio usa a chave de criptografia antiga.</p> <p>Após a primeira vez, quando você executar o comando <code>migrateEncryptionKey</code> para atualizar outros nós no domínio, defina essa opção como <code>True</code> (Verdadeiro) para indicar que o domínio foi atualizado para usar a chave de criptografia mais recente. Ou você pode executar o comando <code>migrateEncryptionKey</code> sem essa opção.</p> <p>O padrão é <code>Verdadeiro</code>.</p>

5. Execute o comando `infasetup` em cada nó no domínio.

Se o domínio tiver vários nós, execute o `infasetup migrateEncryptionKey` em cada nó. Execute o comando nos nós de gateway antes de executá-lo nos nós do funcionário. Você poderá omitir a opção `IsDomainMigrated` após executar o comando pela primeira vez.

6. Reinicie o domínio.

Você deve atualizar todos os serviços de repositório no domínio para atualizar e criptografar dados confidenciais nos repositórios com a nova chave de criptografia. Você também deve migrar a chave do site após atualizar o domínio.

7. Atualize todos os Serviços de Repositório do Modelo, os Serviços do Repositório do PowerCenter e os Serviços do Metadata Manager.

Você pode atualizar um Serviço de Repositório do Modelo e um Serviço do Repositório do PowerCenter na ferramenta Administrator ou no prompt de comando. Você pode atualizar um Serviço do Metadata Manager na ferramenta Administrator.

**Nota:** O Serviço do Metadata Manager deve ser desativado antes que você possa atualizá-lo.

Para atualizar um serviço na ferramenta Administrator, selecione **Gerenciar > Atualização** na área do cabeçalho. Se você selecionar vários serviços, a ferramenta Administrator os atualizará na ordem correta.

Para atualizar um serviço no prompt de comando, use os seguintes comandos:

Tipo de Serviço de Repositório	Comando
Serviço de Repositório do Modelo	<code>infacmd mrs UpgradeContents</code>
Serviço do Repositório do PowerCenter	<code>Atualização pmrep</code>

## Serviços de Aplicativo e Portas

Os serviços de domínio Informatica e os serviços de aplicativo no domínio Informatica têm portas exclusivas.

### Domínio Informatica

A seguinte tabela descreve as portas que você pode definir:

Porta	Descrição
Porta do Gerenciador de Serviços	Número de porta usado pelo Gerenciador de Serviços no nó. O Gerenciador de Serviços atende às solicitações de conexão de entrada nessa porta. Os aplicativos de cliente usam essa porta para comunicar-se com os serviços no domínio. Os programas de linha de comando Informatica usam essa porta para se comunicarem com o domínio. Essa também é a porta do driver JDBC/ODBC do serviço de dados SQL. O padrão é 6006.
Porta de Desligamento do Gerenciador de Serviços	Número de porta que controla a desativação do servidor para o Gerenciador de Serviços do domínio. O Gerenciador de Serviços escuta os comandos de desativação nessa porta. O padrão é 6007.
Porta do Informatica Administrator	Número de porta usado pelo Informatica Administrator. O padrão é 6008.
Porta HTTPS do Informatica Administrator	Nenhuma porta padrão. Insira o número da porta quando você criar o serviço. Definir essa porta como 0 desativa uma conexão HTTPS com a ferramenta Administrator.
Porta de desativação do Informatica Administrator	Número de porta que controla o desligamento do servidor do Informatica Administrator. O Informatica Administrator escuta os comandos de desativação nessa porta. O padrão é 6009.

Porta	Descrição
Número mínimo da porta	O número de porta mais baixo no intervalo de números de porta dinâmico que pode ser atribuído aos processos de serviço de aplicativo executados neste nó. O padrão é 6014.
Número máximo da porta	O número de porta mais alto no intervalo de números de porta dinâmico que pode ser atribuído aos processos de serviço de aplicativo executados neste nó. O padrão é 6114.

### Serviço Analyst

A seguinte tabela lista a porta padrão associada ao Serviço Analyst:

Tipo	Porta Padrão
Serviço Analyst (HTTP)	8085
Serviço Analyst (HTTPS)	Nenhuma porta padrão. Insira o número da porta quando você criar o serviço.

### Serviço do Gerenciamento de Conteúdo

A seguinte tabela lista a porta padrão associada ao Serviço do Gerenciamento de Conteúdo:

Tipo	Porta Padrão
Serviço do Gerenciamento de Conteúdo (HTTP)	8105
Serviço do Gerenciamento de Conteúdo (HTTPS)	Nenhuma porta padrão. Insira o número da porta quando você criar o serviço.

### Serviço de Integração de Dados

A seguinte tabela lista a porta padrão associada ao Serviço de Integração de Dados:

Tipo	Porta Padrão
Serviço de Integração de Dados (proxy HTTP)	8080
Serviço de Integração de Dados (HTTP)	8095
Serviço de Integração de Dados (HTTPS)	Nenhuma porta padrão. Insira o número da porta quando você criar o serviço.
Banco de Dados do Depósito de Criação de Perfil	Nenhuma porta padrão. Insira o número da porta de banco de dados.

### Serviço de Acesso a Metadados

A seguinte tabela lista a porta padrão associada ao Serviço de Acesso a Metadados:

Tipo	Porta Padrão
Serviço de Acesso a Metadados (HTTP)	7080 O Serviço de Acesso a Metadados usa números de porta consecutivos para se conectar a várias distribuições do Hadoop.
Serviço de Acesso a Metadados (HTTPS)	Nenhuma porta padrão. Insira o número da porta quando você criar o serviço. O Serviço de Acesso a Metadados usa números de porta consecutivos para se conectar a várias distribuições do Hadoop.

### Serviço do Metadata Manager

A seguinte tabela lista a porta padrão associada ao Serviço do Metadata Manager:

Tipo	Porta Padrão
Serviço do Metadata Manager (HTTP)	10250
Serviço do Metadata Manager (HTTPS)	Nenhuma porta padrão. Insira o número da porta quando você criar o serviço.

### Serviço do Ouvinte do PowerExchange®

Use o mesmo número de porta especificado na instrução SVCNODE do arquivo DBMOVER.

Se você definir mais de um Serviço do Ouvinte para ser executado em um nó, será necessário definir um número de porta SVCNODE exclusivo para cada serviço.

### Serviço do Agente de Log do PowerExchange

Use o mesmo número de porta especificado na instrução SVCNODE do arquivo DBMOVER.

Se você definir mais de um Serviço do Ouvinte para ser executado em um nó, será necessário definir um número de porta SVCNODE exclusivo para cada serviço.

### Serviço do Hub de Serviços da Web

A seguinte tabela lista a porta padrão associada ao Serviço do Hub de Serviços da Web:

Tipo	Porta Padrão
Serviço do Hub de Serviços da Web. (HTTP)	7333
Serviço do Hub de Serviços da Web. (HTTPS)	7343

## CAPÍTULO 7

# Gerenciamento de Segurança no Informatica Administrator

Este capítulo inclui os seguintes tópicos:

- [Usando a visão geral do Informatica Administrator, 109](#)
- [Segurança do Usuário, 110](#)
- [Guia Segurança, 112](#)
- [Gerenciamento de Senha, 116](#)
- [Gerenciamento de segurança do domínio, 117](#)
- [Gerenciamento de segurança do usuário, 117](#)

## Usando a visão geral do Informatica Administrator

O Informatica Administrator é a ferramenta que você usa para gerenciar o domínio Informatica e a segurança do Informatica.

Use a ferramenta Administrator para executar os seguintes tipos de tarefas:

- **Tarefas administrativas do domínio.** Gerencie logs, objetos de domínio, permissões de usuário e relatórios de domínio. Gere e faça upload de diagnóstico de nó. Monitore tarefas e aplicativos do Serviço de Integração de Dados. Os objetos de domínio incluem serviços de aplicativo, nós, grades, pastas, conexões de banco de dados, perfis de sistema operacional e licenças.
- **Tarefas administrativas de segurança.** Gerencie usuários, grupos, funções e privilégios.

A ferramenta Administrator possui as seguintes guias:

- **Gerenciar.** Exiba e edite as propriedades do domínio e dos objetos no domínio.
- **Monitorar.** Exiba o status de trabalhos de perfil, trabalhos de scorecard, trabalhos de visualização, trabalhos de mapeamento, serviços de dados SQL, serviços da Web e fluxos de trabalho para cada Serviço de Integração de Dados.
- **Monitorar.** Exiba o status de trabalhos de perfil, trabalhos de visualização, trabalhos de mapeamento, serviços de dados SQL e serviços da Web para cada Serviço de Integração de Dados.
- **Logs.** Exiba os eventos de log para o domínio e os serviços no domínio.
- **Relatórios.** Execute um Relatório de Serviços da Web ou um Relatório de Gerenciamento de Licenças.
- **Segurança.** Gerencie usuários, grupos, funções e privilégios.

- **Nuvem.** Exiba informações sobre sua organização do Informatica Cloud®.

A ferramenta Administrator possui os seguintes itens de cabeçalho:

- **Logout.** Faça logout da ferramenta Administrator.
- **Gerenciar.** Gerencie sua conta.
- **Ajuda.** Acesse a ajuda da guia atual e determine a versão do Informatica.

## Segurança do Usuário

O Gerenciador de Serviços e alguns serviços de aplicativo controlam a segurança do usuário em aplicativos clientes. Os aplicativos clientes incluem o Informatica Administrator, o Informatica Analyst, o Informatica Developer, o Metadata Manager e o Cliente do PowerCenter.

O Gerenciador de Serviços e os serviços de aplicativo controlam a segurança do usuário executando as seguintes funções:

### Criptografia

Quando você efetua login em um aplicativo cliente, o Gerenciador de Serviços criptografa a senha.

### Autenticação

Quando você efetua login no aplicativo cliente, o Gerenciador de Serviços autentica sua conta de usuário com base no nome e na senha do usuário ou no token de autenticação.

### Autorização

Quando você solicita um objeto em um aplicativo cliente, o Gerenciador de Serviços e alguns serviços de aplicativo autorizam a solicitação com base em seus privilégios, funções e permissões.

Também é possível usar HTTPS para conexão segura com o domínio e os serviços de aplicativo. Os seguintes serviços de aplicativo fornecem conexão HTTPS junto com o domínio Informatica:

- Serviço de Integração de Dados
- Serviço Analyst
- Serviço do Gerenciamento de Conteúdo
- Serviço de Acesso a Metadados
- Serviço do Metadata Manager
- Serviço Web Service Hub

## Encryption

Informatica encrypts passwords sent from application clients to the Service Manager. Informatica uses AES encryption with multiple 128-bit or 256-bit keys to encrypt passwords and stores the encrypted passwords in the domain configuration database. Configure HTTPS to encrypt passwords sent to the Service Manager from application clients.

## Autenticação

O Service Manager autentica os usuários que fazem login nos clientes de aplicativo.

Na primeira vez que você fizer logon no cliente do aplicativo, insira suas informações de nome de usuário, senha e domínio de segurança. Um domínio de segurança é uma coleção de contas de usuário e grupos em um domínio Informatica.

O domínio de segurança selecionado por você determina o método de autenticação usado pelo Service Manager para autenticar sua conta de usuário:

- **Nativo.** Quando você faz logon em um cliente de aplicativo como usuário nativo, o Service Manager autentica seu nome de usuário e senha em relação às contas de usuário no banco de dados de configuração do domínio.
- **Protocolo LDAP (Lightweight Directory Access Protocol)** Quando você faz logon no cliente de aplicativo como usuário LDAP, o Service Manager passa seu nome de usuário e senha para autenticação no serviço de diretório LDAP externo.

## Sign-On único

Depois de efetuar logon em um aplicativo cliente, o Gerenciador de Serviços permitirá ativar outro aplicativo cliente ou acessar vários repositórios no aplicativo cliente. Não é necessário efetuar logon no aplicativo cliente ou repositório adicional.

Na primeira vez em que o Gerenciador de Serviços autentica sua conta de usuário, ele cria um token de autenticação criptografado para sua conta e retorna o token de autenticação para o aplicativo cliente. O token de autenticação contém seu nome de usuário, domínio de segurança e um tempo de expiração. O Gerenciador de Serviços renova periodicamente o token de autenticação antes do tempo de expiração.

Quando você acessa vários repositórios em um aplicativo cliente, o aplicativo cliente envia o token de autenticação para o Gerenciador de Serviços para autenticação do usuário.

Quando você ativa um aplicativo Web cliente com base em outro, o aplicativo cliente transmite o token de autenticação ao próximo aplicativo cliente. O próximo aplicativo Web cliente envia o token de autenticação ao Gerenciador de Serviços para autenticação do usuário. Você deve fazer logout de cada aplicativo Web cliente separadamente. Por exemplo, se você abrir a ferramenta Analyst na ferramenta Administrator, deverá fazer logout dessas duas ferramentas separadamente.

**Nota:** Para usar o sign-on único entre a ferramenta Administrator, a ferramenta Analyst e a ferramenta Monitoring, você deve adicionar seus nomes de domínio totalmente qualificados ao arquivo host para cada nó.

Não é possível usar o single sign-on para conectar-se a um aplicativo Web cliente a partir de uma ferramenta cliente. Por exemplo, se você iniciar a ferramenta Administrator a partir da Developer tool, deverá fazer login na ferramenta Administrator.

## Autorização

O Gerenciador de Serviços autoriza solicitações do usuário para objetos de domínio. Solicitações podem vir da ferramenta Administrator. Os seguintes serviços de aplicativo autorizam solicitações do usuário para outros objetos:

- Serviço de Integração de Dados
- Serviço do Metadata Manager
- Serviço de Repositório do Modelo
- Serviço do Repositório do PowerCenter

Quando você cria usuários e grupos nativos ou importa usuários e grupos LDAP, o Gerenciador de Serviços armazena as informações no banco de dados de configuração do domínio nos seguintes repositórios:

- Repositório do Modelo
- Repositório do PowerCenter
- Repositório do PowerCenter para o Metadata Manager

O Gerenciador de Serviços sincroniza as informações de usuário e grupo entre os repositórios e o banco de dados de configuração do domínio quando ocorrerem os seguintes eventos:

- Você reinicia o Serviço do Metadata Manager, o Serviço de Repositório do Modelo ou o Serviço de Repositório do PowerCenter.
- Você adicionar ou remover usuários ou grupos nativos.
- O Gerenciador de Serviços sincroniza a lista de usuários e grupos LDAP no banco de dados de configuração do domínio com a lista de usuários e grupos do serviço de diretório LDAP.

Quando você atribui permissões a usuários e grupos em um aplicativo cliente, o serviço de aplicativos armazena as atribuições de permissão com as informações de usuários e grupos no repositório apropriado.

Quando você solicita um objeto em um aplicativo cliente, o serviço de aplicativos apropriado autoriza sua solicitação. Por exemplo, se você tentar editar um projeto no Informatica Developer, o Serviço de Repositório do Modelo autorizará sua solicitação com base em suas atribuições de privilégio, função e permissão.

## Guia Segurança

Administre a segurança do Informatica na guia Segurança da ferramenta Administrador.

A guia Segurança contém os seguintes componentes:

- Seção Pesquisa. Pesquise usuários, grupos ou funções por nome.
- Navegador. O Navegador é exibido no painel esquerdo e exibe grupos, usuários e funções.
- Painel de conteúdo. O painel de conteúdo exibe propriedades e opções com base no objeto selecionado no Navegador e na guia selecionada no painel de conteúdo.
- Menu Ações de Segurança. Contém opções para criar ou excluir um grupo, usuário ou função. Você pode gerenciar as configurações LDAP e os perfis de sistema operacional. Também é possível exibir usuários que tenham privilégios para um serviço.

## Usando a seção Pesquisa

Use a seção Pesquisa para pesquisar usuários, grupos e funções por nome. A pesquisa não diferencia maiúsculas e minúsculas.

1. Na seção Pesquisa, selecione se você deseja pesquisar usuários, grupos ou funções.
2. Digite o nome ou o nome parcial a ser pesquisado.

É possível incluir um asterisco (\*) em um nome para ser usado como curinga na pesquisa. Por exemplo, digite "ad\*" para todos os objetos que iniciam com "ad". Digite "\*ad" para pesquisar objetos que terminam com "ad".

3. Clique em Ir.

A seção Resultados da Pesquisa aparece e exibe no máximo 100 objetos. Se você pesquisar retornos superiores a 100 objetos, restrinja seus critérios de pesquisa para limitar os resultados.



4. Selecione um objeto na seção Resultados da Pesquisa para exibir informações sobre o objeto no painel de conteúdo.

## Usando o Navegador de Segurança

O Navegador aparece no painel de conteúdo da guia Segurança. Quando você seleciona um objeto no Navegador, o painel de conteúdo exibe informações sobre o objeto.

O Navegador na guia Segurança exibe uma das seguintes seções com base no que você está exibindo:

- Seção Grupos. Selecione um grupo para exibir suas propriedades, os usuários atribuídos ao grupo e as funções e os privilégios atribuídos ao grupo.
- Seção Usuários. Selecione um usuário para exibir suas propriedades, os grupos aos quais o usuário pertence e as funções e os privilégios atribuídos ao usuário.
- Seção Funções. Selecione uma função para exibir suas propriedades, os usuários e os grupos que receberam as atribuições da função e os privilégios atribuídos à função.
- Seção Perfis Operacionais. Selecione um perfil operacional para visualizar as propriedades do perfil do sistema operacional e as permissões atribuídas aos usuários e grupos que usam o perfil do sistema operacional.
- Seção Configuração do LDAP. Selecione uma configuração para exibir os detalhes da conexão do servidor LDAP, o domínio de segurança LDAP que contém usuários e grupos importados do serviço de diretório LDAP e o agendamento da sincronização do LDAP.

O Navegador fornece maneiras diferentes de concluir uma tarefa. É possível usar qualquer um dos seguintes métodos para gerenciar grupos, usuários e funções:

- Clique no menu **Ações**. Cada seção do Navegador inclui um menu Ações para gerenciar grupos, usuários, funções, perfis do sistema operacional ou configurações do LDAP.
- Clique com o botão direito do mouse em um objeto. Clique com o botão direito do mouse em um objeto no Navegador para exibir as opções disponíveis no menu Ações.
- Use os atalhos do teclado. Use os atalhos do teclado para se mover para diferentes seções do Navegador.

## Grupos

Um grupo é um conjunto de usuários e grupos que podem ter os mesmos privilégios, funções e permissões.

A seção Grupos do Navegador organiza grupos em pastas do domínio de segurança. Um domínio de segurança é uma coleção de contas de usuário e grupos em um domínio Informatica. A autenticação nativa usa o domínio de segurança nativa que contém os usuários e grupos criados e gerenciados na ferramenta Administrator. A autenticação LDAP usa domínios de segurança LDAP que contém usuários e grupos importados do serviço de diretório LDAP.

Quando você seleciona uma pasta do domínio de segurança na seção Grupos do Navegador, o painel de conteúdo exibe todos os grupos que pertencem ao domínio de segurança.

Quando você seleciona um grupo no navegador, o painel de conteúdo exibe as seguintes guias:

- Visão geral. Exibe propriedades gerais do grupo e de usuários atribuídos ao grupo.
- Privilégios. Exibe os privilégios e funções atribuídas ao grupo para o domínio e para serviços de aplicativo no domínio.
- Permissões. Exibe o nível de acesso que esses usuários no grupo têm para executar tarefas em objetos de domínio, incluindo nós, grades e serviços de aplicativo. Também exibe o nível de acesso que os usuários no grupo têm para executar tarefas em objetos de conexão e perfis do sistema operacional.

## Usuários

Um usuário com uma conta no domínio Informatica pode efetuar logon nos aplicativos clientes a seguir.

- Informatica Administrator
- Cliente do PowerCenter
- Informatica Developer
- Informatica Analyst
- Metadata Manager

A seção Usuários do Navegador organiza os usuários nas pastas do domínio de segurança. Um domínio de segurança é uma coleção de contas de usuário e grupos em um domínio Informatica. A autenticação nativa usa o domínio de segurança nativa que contém os usuários e grupos criados e gerenciados na ferramenta Administrator. A autenticação LDAP usa domínios de segurança LDAP que contém usuários e grupos importados do serviço de diretório LDAP.

Quando você seleciona uma pasta de domínio de segurança na seção Usuários do Navegador, o painel de conteúdo exibe todos os usuários pertencentes ao domínio de segurança.

Ao selecionar um usuário no Navegador, o painel de conteúdo exibe as seguintes guias:

- Visão geral. Exibe as propriedades gerais do usuário e todos os grupos aos quais o usuário pertence.
- Privilégios. Exibe os privilégios e funções atribuídos ao usuário para o domínio e para serviços de aplicativo no domínio.
- Permissões. Exibe o nível de acesso que o usuário tem para executar tarefas em objetos de domínio, incluindo nós, grades e serviços de aplicativo. Também exibe o nível de acesso que o usuário tem para executar tarefas em objetos de conexão e perfis de sistema operacional.

## Funções

Uma função é um conjunto de privilégios atribuídos a um usuário ou grupo. Os privilégios determinam as ações que os usuários podem executar. Você atribui uma função a usuários e grupos para o domínio e para serviços de aplicativo no domínio.

A seção Funções do navegador organiza funções nas seguintes pastas:

- Funções definidas pelo sistema. Contém funções que você não edita ou exclui. A função Administrador é definida pelo sistema.
- Funções personalizadas. Contém funções que você pode criar, editar e excluir. A ferramenta Administrador inclui algumas funções personalizadas que você pode editar e atribuir a usuários e grupos.

Quando você seleciona uma pasta na seção Funções do Navegador, o painel de conteúdo exibe todas as funções pertencentes à pasta.

Quando você seleciona uma função no Navegador, o painel de conteúdo exibe as seguintes guias:

- Visão geral. Exibe as propriedades gerais da função e os usuários e grupos que têm a função atribuída para o domínio e serviços de aplicativo.
- Privilégios. Exibe os privilégios atribuídos à função para o domínio e os serviços de aplicativo.

## Perfis do sistema operacional

Um perfil do sistema operacional é um mecanismo de segurança que o Serviço de Integração de Dados e o Serviço de Integração do PowerCenter usam para executar mapeamentos, fluxos de trabalho e tarefas de criação de perfil.

A seção Perfis do Sistema Operacional do Navegador lista os perfis do sistema operacional configurados no domínio.

Ao selecionar um perfil do sistema operacional no Navegador, o painel de conteúdo exibe as seguintes guias:

- **Propriedades.** Exibe as propriedades gerais do perfil do sistema operacional configurado para o Serviço de Integração de Dados, para o Serviço de Integração do PowerCenter ou para os dois serviços de aplicativo.
- **Permissões.** Exibe as permissões atribuídas a usuários e grupos que usam o perfil do sistema operacional. Também indica se o perfil do sistema operacional é o perfil padrão atribuído a um usuário ou grupo.

## Configuração do LDAP

Você pode configurar um domínio Informatica para permitir que usuários e grupos importados de um ou mais serviços de diretório LDAP efetuem login nos nós, serviços e clientes de aplicativos da Informatica.

A seção Configuração do LDAP do Navegador lista as configurações do LDAP usadas pelo domínio.

Quando você seleciona uma configuração do LDAP, as seguintes guias são exibidas na guia Configuração do LDAP:

- **Visão geral.** Lista os detalhes da conexão para o servidor LDAP que contém o serviço de diretório do qual você deseja importar usuários e grupos.
- **Domínios de segurança.** Lista os detalhes do domínio de segurança LDAP que contém usuários e grupos importados do serviço de diretório LDAP.
- **Agendamento.** Lista os detalhes da programação de sincronização que especifica quando o Gerenciador de Serviços atualiza o domínio de segurança com os usuários e grupos no serviço de diretório LDAP.

## Gerenciamento de conta

Para melhorar a segurança no domínio Informatica, você pode impor o bloqueio de contas de usuário e administrador após um número especificado de tentativas de login com falha.

A seção Configuração de Bloqueio de Conta da página Gerenciamento de Conta exibe se o bloqueio de conta está ativado para contas de usuário e contas de administrador. A seção também indica o número máximo de tentativas de login com falha permitidas.

A seção Usuários Nativos Bloqueados da página lista as contas de usuário bloqueadas no domínio de segurança nativo. Você pode desbloquear uma conta de usuário no domínio de segurança nativo.

A seção Usuários Nativos LDAP da página lista as contas de usuário bloqueadas no domínio de segurança LDAP. Você pode desbloquear uma conta de usuário no domínio Informatica. No entanto, o administrador do LDAP deve desbloquear a conta de usuário no servidor LDAP. O usuário só poderá fazer logon no domínio Informatica quando o administrador LDAP desbloquear a conta de usuário.

## Relatórios de Auditoria

Os relatórios de auditoria fornecem informações sobre usuários e grupos no domínio Informatica e sobre os privilégios, as funções e as permissões atribuídos a cada usuário ou grupo.

Selecione o relatório de auditoria a ser gerado no menu Selecionar Tipo de Relatório. Você pode gerar os seguintes relatórios de auditoria:

### **Informações Pessoais do Usuário**

Exibe as informações de contato e os detalhes de status de contas de usuário no domínio. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

### **Associação de Grupo de Usuários**

Exibe informações sobre usuários e os grupos aos quais eles pertencem. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

### **Privilégios**

Exibe as informações sobre os privilégios atribuídos a usuários e grupos no domínio. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

### **Funções**

Exibe as informações sobre as funções atribuídas a usuários e grupos no domínio. Você pode selecionar as funções para as quais deseja gerar o relatório.

### **Permissões em Objetos de Domínio**

Exibe as informações sobre os objetos de domínio nos quais os usuários e grupos têm permissão. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

## Gerenciamento de Senha

Você pode alterar a senha por meio do aplicativo Alterar Senha.

Você pode abrir o aplicativo Alterar Senha na ferramenta Administrator ou com a seguinte URL: `http://<fully qualified host name>:<port>/passwordchange/`

O Gerenciador de Serviços usa a senha de usuário associada a um nó do funcionário para autenticar o usuário do domínio. Se você alterar uma senha de usuário que esteja associada a um ou mais nós trabalhador, o Gerenciador de Serviços atualizará a senha em cada nó trabalhador. O Gerenciador de Serviços não pode atualizar nós que não estejam em execução. Nos nós que não estão em execução, o Gerenciador de Serviços atualiza a senha quando o nó é reiniciado.

**Nota:** Para uma conta de usuário LDAP, altere a senha no serviço de diretório LDAP.

Você pode ativar ou desativar as URLs internas ao alterar a senha do administrador do LDM na ferramenta Administrator configurada para balanceamento de carga.

Use a seguinte opção personalizada para URLs internos para gerenciamento de senhas:

### **enableChangePwdUrlProxyHost**

Exiba e acesse as URLs internas relacionadas ao gerenciamento de senhas. O padrão é "false".

Para uma conta de usuário no domínio que usa autenticação nativa, se você habilitar a complexidade da senha, use as seguintes diretrizes ao criar ou alterar uma senha:

- O comprimento da senha deve ser de pelo menos oito caracteres.

- Ela deve ser uma combinação de um caractere do alfabeto, um caractere numérico e um caractere não alfanumérico, como:

! \ " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ ] ^ \_ ` { | } ~

Quando você usa caracteres especiais em uma senha, o shell às vezes os interpreta de maneira diferente. Por exemplo, \$ é interpretado como uma variável. Nesse caso, use um caractere de escape para escapar o caractere especial.

## Alterando a senha

Altere a senha para uma conta de usuário nativo a qualquer momento. Para uma conta de usuário criada por outra pessoa, altere a senha na primeira vez que você fizer login na ferramenta Administrador.

1. Na área de cabeçalho da ferramenta Administrador, clique em **Gerenciar > Alterar Senha**.  
Para Alterar a Senha, o aplicativo é aberto em uma nova janela do navegador.
2. Insira a senha atual na caixa **Senha**, e a nova senha nas caixas **Nova Senha** e **Confirmar Senha**.
3. Clique em **Atualizar**.

## Gerenciamento de segurança do domínio

Você pode configurar o uso do protocolo SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) em componentes do domínio Informatica para criptografar conexões com outros componentes. Ao habilitar o SSL ou o TLS para componentes de domínio, você garante uma comunicação segura.

Você pode configurar a comunicação segura das seguintes formas:

### Entre serviços dentro do domínio

Você pode configurar a comunicação segura entre serviços dentro do domínio.

### Entre o domínio e componentes externos

Você pode configurar a comunicação segura entre componentes do domínio Informatica e navegadores da Web ou clientes de serviços Web.

Cada método de configuração da comunicação segura é independente dos outros. Ao configurar a comunicação segura para um conjunto de componentes, você não precisa configurá-la para nenhum outro conjunto.

**Nota:** Se você alterar um domínio seguro para um não seguro ou um domínio não seguro para um seguro, deverá excluir a configuração de domínio na ferramenta Developer e nas ferramentas de cliente do PowerCenter, e configurar o domínio novamente no cliente.

## Gerenciamento de segurança do usuário

Você gerencia a segurança do usuário no domínio com privilégios e permissões.

Os privilégios determinam as ações que os usuários podem concluir em objetos de domínio. As permissões definem o nível de acesso que um usuário tem a um objeto de domínio. Os objetos de domínio incluem o

domínio, pastas, nós, grades, licenças, conexões de banco de dados, perfis de sistema operacional e os serviços de aplicativo.

Mesmo que o usuário tenha o privilégio de domínio para concluir certas ações, talvez ele também precise de permissão para concluir ações em um objeto específico. Por exemplo, um usuário tem privilégio do domínio Gerenciar Serviços, que concede ao usuário a possibilidade de editar serviços de aplicativo. No entanto, o usuário também deve ter permissão para o serviço de aplicativo. Um usuário com privilégio e permissão para o domínio Gerenciar Serviços no Serviço de Repositório de Desenvolvimento, mas não no Serviço de Repositório de Produção, pode editar o Serviço de Repositório de Desenvolvimento mas não o Serviço de Repositório de Produção.

Para fazer logon na ferramenta Administrator, o usuário deve ter o privilégio de domínio Acesso ao Informatica Administrator. Se um usuário tiver privilégio e permissão de acesso ao Informatica Administrator em um objeto, mas não tiver o privilégio de domínio que concede a possibilidade de modificar o tipo de objeto, ele pode visualizar o objeto. Por exemplo, se um usuário tiver permissão para um nó, mas não tiver o privilégio para Gerenciar Nós e Grades, ele pode visualizar as propriedades do nó mas não pode configurar, encerrar nem remover o nó.

Se um usuário não tiver permissão para um objeto selecionado no Navegador, o painel de conteúdo exibe uma mensagem indicando que a permissão para o objeto foi negada.

## CAPÍTULO 8

# Usuários e grupos

Este capítulo inclui os seguintes tópicos:

- [Visão geral de usuários e grupos, 119](#)
- [Grupos Padrão, 120](#)
- [Entendendo as contas de usuário, 121](#)
- [Gerenciando usuários, 123](#)
- [Gerenciando grupos, 131](#)
- [Managing operating system profiles, 133](#)
- [Bloqueio de conta, 142](#)

## Visão geral de usuários e grupos

Para acessar os serviços de aplicativo e os objetos no domínio Informatica e usar os aplicativos clientes, você deve ter uma conta de usuário.

Durante a instalação, uma conta de usuário administrador é criada. Use a conta de administrador padrão para fazer logon no domínio Informatica e gerenciar serviços de aplicativo, objetos de domínio e outras contas de usuários. Ao efetuar logon no domínio Informatica após a instalação, altere a senha para garantir a segurança do domínio Informatica e aplicativos.

O gerenciamento de conta do usuário no Informatica envolve os seguintes componentes de chave:

- **Usuários.** É possível configurar diferentes tipos de contas de usuário no domínio Informatica. Os usuários podem realizar tarefas com base nas funções, nos privilégios e nas permissões atribuídos a eles.
- **Autenticação.** Quando um usuário efetua logon em um aplicativo cliente, o Gerenciador de Serviços autentica a conta do usuário no domínio Informatica e verifica se o usuário pode usar o aplicativo cliente. O domínio Informatica pode usar a autenticação nativa ou LDAP para autenticar usuários. O Gerenciador de Serviços organiza contas de usuário e grupos por domínio de segurança. Ele autentica os usuários com base no domínio de segurança ao qual o usuário pertence.
- **Grupos.** É possível configurar grupos de usuários e atribuir diferentes funções, privilégios e permissões a cada grupo. As funções, os privilégios e as permissões atribuídas ao grupo determinam as tarefas que os usuários no grupo podem executar no domínio Informatica.
- **Privilégios e funções.** Os privilégios determinam as ações que os usuários podem executar nos aplicativos clientes. Uma função é uma coleção de privilégios que você pode atribuir aos usuários e grupos. Você pode atribuir funções ou privilégios aos usuários e grupos do domínio e de cada serviços de aplicativo no domínio.

- Perfis do sistema operacional. Se você executar o Serviço de Integração no UNIX ou Linux, poderá configurar o Serviço de Integração para usar perfis do sistema operacional. Use perfis do sistema operacional para aumentar a segurança e isolar o ambiente de tempo de execução para os usuários. É possível criar e gerenciar perfis do sistema operacional na guia Segurança da ferramenta Administrador.
- Bloqueio de conta. Você pode configurar o bloqueio de conta para bloquear uma conta de usuário quando o usuário especificar um logon incorreto na ferramenta Administrador ou em quaisquer clientes do aplicativo, como a Developer tool e a ferramenta Analyst. Você também pode desbloquear uma conta de usuário.

## Grupos Padrão

O domínio Informatica tem um conjunto de grupos de usuários que são criados durante a instalação.

Por padrão, o domínio Informatica tem os seguintes grupos de usuários após a instalação:

- Administrador
- Todos
- Operador

### Grupo Administrador

O domínio Informatica inclui um grupo padrão chamado Administrador. A conta de administrador padrão criada durante a instalação pertence a esse grupo.

O grupo Administrador possui permissões e privilégios de administrador no domínio e em todos os serviços de aplicativo. Você pode adicionar ou remover usuários do grupo Administrador. Todos os usuários do grupo Administrador têm as mesmas permissões e privilégios que o administrador padrão criado durante a instalação.

Você não pode excluir a conta de administrador padrão do grupo Administrador e não pode excluir o grupo Administrador.

### Grupo Todos

O domínio Informatica inclui um grupo padrão chamado Todos. Todos os usuários do domínio pertencem ao grupo.

Por padrão, o grupo Todos não tem privilégios. É possível atribuir privilégios, funções e permissões ao grupo Todos para conceder o mesmo acesso a todos os usuários.

Você pode executar as seguintes tarefas no grupo Todos:

- Editar ou excluir o grupo Todos.
- Adicionar ou remover usuários do grupo Todos.
- Mover um grupo para o grupo Todos.



## Grupo Operador

O domínio Informatica inclui um grupo padrão denominado Operador.

Por padrão, o grupo Operador tem permissão em todos os objetos do domínio. Você pode atribuir a função de Operador ao grupo Operador e usá-lo para gerenciar os usuários Operadores no domínio.

É possível realizar as seguintes tarefas no grupo Operador:

- Atribuir privilégios e funções ao grupo.
- Adicionar ou remover usuários do grupo.
- Mover um grupo ao grupo.
- Editar ou excluir o grupo.

## Entendendo as contas de usuário

Um domínio Informatica pode ter os seguintes tipos de contas:

- Administrador padrão
- Administrador de domínio
- Administrador de cliente de aplicativo
- Usuário

### Administrador Padrão

Quando você instala serviços Informatica, o instalador cria o administrador padrão com um nome de usuário e uma senha especificados por você. É possível usar a conta de administrador padrão para fazer logon inicialmente na ferramenta Administrador.

O administrador padrão possui permissões e privilégios de administrador no domínio e em todos os serviços de aplicativo.

O administrador padrão pode executar as seguintes tarefas:

- Criar, configurar e gerenciar todos os objetos do domínio, incluindo nós, serviços de aplicativo, bem como contas de administrador e usuário.
- Configurar e gerenciar todos os objetos e contas de usuário criados por outros administradores de domínio e administradores do cliente do aplicativo.
- Faça logon em qualquer cliente do aplicativo.

Não é possível desativar nem modificar o nome de usuário ou os privilégios do administrador padrão. Você pode alterar a senha do administrador padrão.

### Administrador de domínio

Um administrador de domínio pode criar e gerenciar objetos no domínio.

O administrador de domínio pode efetuar logon na ferramenta Administrador e criar e configurar serviços de aplicativo no domínio. No entanto, por padrão, o administrador de domínio não pode efetuar logon nos clientes do aplicativo. O administrador padrão deve fornecer explicitamente a um administrador de domínio

permissões e privilégios completos para os serviços de aplicativo, de modo que ele possa efetuar login e executar tarefas administrativas nos clientes do aplicativo.

Para criar um administrador de domínio, atribua a um usuário a função Administrador de um domínio.

## Administrador de Cliente de Aplicativo

Um administrador de cliente de aplicativo pode criar e gerenciar objetos em um cliente de aplicativo. Crie contas de administrador para os clientes de aplicativo. Para limitar os privilégios do administrador e manter a segurança dos clientes de aplicativo, crie outra conta de administrador para cada cliente de aplicativo.

Por padrão, o administrador de cliente de aplicativo não tem permissões, nem privilégios no domínio. Sem as permissões ou privilégios no domínio, o administrador de cliente de aplicativo não pode fazer login na ferramenta Administrador para gerenciar o serviço de aplicativo.

Você pode configurar os seguintes administradores de cliente de aplicativo:

### **Administrador do Informatica Analyst**

Tem permissões e privilégios totais no Informatica Analyst. O administrador do Informatica Analyst pode fazer login no Informatica Analyst para criar e gerenciar os projetos e os objetos nos projetos e realizar todas as tarefas no cliente de aplicativo.

Para criar um administrador do Informatica Analyst, atribua a um usuário a função Administrador para um Serviço Analyst e para o Serviço de Repositório do Modelo associado.

### **Administrador do Informatica Developer**

Tem permissões e privilégios totais no Informatica Developer. O administrador do Informatica Developer pode fazer login no Informatica Developer para criar e gerenciar os projetos e os objetos nos projetos e realizar todas as tarefas no cliente de aplicativo.

Para criar um administrador do Informatica Developer, atribua a função Administrador a um usuário de um Serviço de Repositório do Modelo.

### **Administrador do Metadata Manager**

Tem permissões e privilégios totais no Metadata Manager. O administrador do Metadata Manager pode fazer login no Metadata Manager para criar e gerenciar os objetos do Metadata Manager e realizar todas as tarefas no cliente de aplicativo.

Para criar um administrador do Metadata Manager, atribua a um usuário a função Administrador de um Serviço do Metadata Manager.

### **Administrador do Test Data**

Tem privilégios e permissões totais no Test Data Manager. O administrador do Test Data Manager pode fazer login no Test Data Manager para criar e gerenciar os respectivos objetos e realizar todas as tarefas no cliente de aplicativo.

Para criar um administrador do Test Data, atribua a função Administrador a um usuário de um Serviço do Test Data Manager.

### **Administrador do Cliente do PowerCenter**

Tem privilégios e permissões totais para todos os objetos no Cliente do PowerCenter. O administrador do Cliente do PowerCenter pode fazer login no Cliente do PowerCenter para gerenciar os objetos do repositório do PowerCenter e realizar todas as tarefas no Cliente do PowerCenter. O administrador do Cliente do PowerCenter também pode realizar todas as tarefas nos programas de linha de comando pmrep e pmcmd.

Para criar um administrador de Cliente do PowerCenter, atribua a um usuário a função Administrador de um Serviço do Repositório do PowerCenter.

## Usuário

Um usuário com uma conta no domínio Informatica pode executar tarefas nos aplicativos clientes.

De modo geral, o administrador padrão ou um administrador de domínio cria e gerencia contas de usuário e atribui funções, permissões e privilégios ao domínio Informatica. Entretanto, qualquer usuário com os privilégios e permissões do domínio pode criar uma conta de usuário e atribuir funções, permissões e privilégios.

Os usuários podem executar tarefas nos aplicativos clientes com base nos privilégios e permissões atribuídos a eles.

## Gerenciando usuários

Você pode criar, editar e excluir usuários no domínio de segurança nativo. Não é possível excluir nem modificar as propriedades de contas de usuário nos domínios de segurança LDAP. Não é possível modificar as atribuições de usuário para grupos LDAP.

Você pode atribuir funções, permissões e privilégios a uma conta de usuário no domínio de segurança nativo ou um domínio de segurança LDAP. As funções, permissões e privilégios atribuídos ao usuário determinam as tarefas que o usuário pode executar no domínio Informatica.

Você também pode desbloquear uma conta de usuário.

## Criando usuários nativos

Adicionar, editar ou excluir usuários nativos na guia Segurança.

1. Na ferramenta Administrator, clique na guia Segurança.
2. No menu Ações de Segurança, clique em Criar Usuário.
3. Digite os seguintes detalhes do novo usuário:

Propriedade	Descrição
Nome de Logon	Nome de logon da conta de usuário. O nome de logon de uma conta de usuário deve ser exclusivo no domínio de segurança ao qual ele pertence. O nome não faz distinção entre maiúsculas e minúsculas e não pode exceder 128 caracteres. Ele não pode incluir tabulação, caractere de nova linha nem os seguintes caracteres especiais: , + " \ < > ; / * % ? & O nome pode incluir um caractere de espaço ASCII, exceto o primeiro e o último caracteres. Nenhum outro caractere de espaço é permitido.
Senha	Senha da conta de usuário. A senha pode ter de 1 a 80 caracteres.

Propriedade	Descrição
Confirmar Senha	Digite a senha novamente para confirmar. Você deve digitar novamente a senha. Não copie e cole a senha.
Nome Completo	Nome completo da conta de usuário. O nome completo não pode incluir os seguintes caracteres especiais: < > "
Descrição	Descrição da conta de usuário. A descrição não pode exceder 765 caracteres nem conter os seguintes caracteres especiais: < > "
E-mail	Endereço de e-mail do usuário. O endereço de e-mail não pode incluir os seguintes caracteres especiais: < > " Digite o endereço de e-mail no formato UserName@Dominio.
Telefone	Número de telefone do usuário. O número de telefone não pode incluir os seguintes caracteres especiais: < > "

4. Clique em OK para salvar a conta de usuário.

Depois de criar uma conta de usuário, o painel de detalhes exibe as propriedades da conta e os grupos aos quais o usuário foi atribuído.

## Editando Propriedades Gerais de Usuários Nativos

Não é possível alterar o nome de logon de um usuário nativo. Você pode alterar a senha e outros detalhes de uma conta de usuário nativo.

1. Na ferramenta Administrador, clique na guia Segurança.
2. Na seção Usuários do Navegador, selecione uma conta de usuário nativo e clique em Editar.
3. Para alterar a senha, selecione Alterar Senha.  
A guia Segurança limpa os campos Senha e Confirmar Senha.
4. Digite uma nova senha e confirme.
5. Modifique o nome completo, a descrição, o e-mail e o telefone, conforme o necessário.
6. Clique em OK para salvar as alterações.

## Atribuindo Usuários Nativos a Grupos Nativos

Atribua usuários nativos a grupos nativos na guia Segurança.

1. Na ferramenta Administrador, clique na guia Segurança.
2. Na seção Usuários do Navegador, selecione uma conta de usuário nativo e clique em **Editar**.
3. Clique na guia Grupos.
4. Para atribuir um usuário nativo a um grupo, selecione um nome do grupo na coluna Todos os Grupos e clique em **Adicionar**.

Se grupos aninhados não forem exibidos na coluna Todos os Grupos, expanda cada grupo para mostrar todos os grupos aninhados.

Você pode atribuir um usuário nativo a mais de um grupo. Use as teclas Ctrl ou Shift para selecionar vários grupos ao mesmo tempo.

5. Para remover um usuário nativo de um grupo, selecione um grupo na coluna Grupos Atribuídos e clique em **Remover**.
6. Clique em **OK** para salvar as atribuições do grupo.

## Atribuindo Usuários LDAP a Grupos Nativos

É possível atribuir contas de usuário LDAP a grupos nativos. Não é possível alterar a atribuição de contas de usuário LDAP a grupos de LDAP.

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Na seção Grupos do Navegador, selecione um grupo nativo e clique em **Editar**.
3. Clique na guia **Usuários**.
4. Para atribuir um usuário LDAP a um grupo, selecione esse usuário na coluna Todos os Usuários e clique em **Adicionar**.
5. Para remover um usuário LDAP de um grupo, selecione esse usuário na coluna Usuários Atribuídos e clique em **Remover**.
6. Clique em **OK** para salvar as atribuições de usuário.

## Ativando e desativando contas de usuário

Os usuários com contas ativas podem fazer logon nos clientes do aplicativo e executar tarefas com base nas suas permissões e privilégios. Se não desejar que os usuários acessem clientes do aplicativo temporariamente, você pode desativar suas contas. É possível ativar ou desativar contas de usuário no domínio de segurança LDAP ou nativo. Quando você desativa uma conta de usuário, o usuário não pode fazer logon nos clientes do aplicativo.

Para desativar uma conta de usuário, selecione-a na seção Usuários do Navegador e clique em Desativar. Quando você seleciona uma conta de usuário desativada, a guia Segurança exibe uma mensagem informando que a conta de usuário está desativada. Quando uma conta de usuário está desativada, o botão Ativar fica disponível. Para ativar a conta de usuário, clique em Ativar.

Não é possível desativar a conta de administrador padrão.

**Nota:** Quando o Service Manager importa uma conta de usuário do serviço de diretório LDAP, ele não importa o atributo LDAP que indica que uma conta de usuário está ativada ou desativada. O Service Manager importa todas as contas de usuário como ativadas. Você deve desativar uma conta de usuário LDAP na ferramenta Administrator se não desejar que o usuário acesse clientes do aplicativo. Durante a sincronização subsequente com o servidor LDAP, a conta de usuário retém o status ativado ou desativado definido na ferramenta Administrator.

## Excluindo usuários nativos

Para excluir uma conta de usuário nativo, clique com o botão direito do mouse no nome da conta de usuário na seção Usuários do Navegador e selecione Excluir Usuário. Confirme que você deseja excluir a conta de usuário.

Você não pode excluir a conta de administrador padrão. Quando você fizer logon na ferramenta Administrator, não poderá excluir sua conta de usuário.

## Excluindo usuários do PowerCenter

Ao excluir um usuário que possui objetos no repositório do PowerCenter, você remove qualquer propriedade que o usuário possua sobre pastas, objetos de conexão, grupos de implantação, rótulos ou consultas. Após excluir um usuário, o administrador padrão torna-se o proprietário de todos os objetos possuídos pelo usuário excluído.

Quando você exibe o histórico de um objeto com versão que pertencia a um usuário excluído, o nome do usuário excluído aparece com o prefixo "excluído".

## Excluindo Usuários do Metadata Manager

Quando você exclui um usuário que possui atalhos e pastas, o Metadata Manager move a pasta pessoal do usuário para uma pasta denominada Usuários Excluídos, de propriedade do administrador padrão. A pasta pessoal do usuário excluído contém todos os atalhos e pastas criados pelo usuário. Todas as pastas compartilhadas permanecem compartilhadas depois que você exclui o usuário.

Se a pasta Usuários Excluídos contiver uma pasta com o mesmo nome de usuário, o Metadata Manager nomeará a pasta adicional "Cópia (n) de <nomedousuário>".

## Usuários LDAP

Não é possível adicionar, editar nem excluir usuários LDAP na ferramenta Administrador. Você deve gerenciar contas de usuário LDAP no serviço de diretório LDAP.

## Desbloqueando uma conta de usuário

O administrador de domínio pode desbloquear uma conta de usuário que está bloqueada no domínio. Se o usuário for um usuário nativo, o administrador poderá solicitar que o usuário redefina a senha antes de fazer login novamente no domínio.

O usuário deve ter um endereço de e-mail válido configurado no domínio para receber notificações quando senha da sua conta for redefinida.

Se o usuário estiver bloqueado no servidor de autenticação LDAP, o administrador LDAP deverá desbloquear a conta de usuário no servidor LDAP.

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Clique em **Gerenciamento de conta**.

A página Gerenciamento de Conta exibe as seguintes listas de usuários bloqueados:

### **Usuários Nativos Bloqueados**

Inclui as contas de usuário que estão bloqueadas no domínio de segurança Nativo.

### **Usuários LDAP Bloqueados**

Inclui as contas de usuário que estão bloqueadas nos domínios de segurança LDAP.

3. Selecione os usuários que deseja desbloquear.
4. Selecione **Desbloquear o usuário e redefinir a senha** para gerar uma nova senha para o usuário depois que você desbloquear a conta.  
O usuário recebe a nova senha em um e-mail.
5. Clique no botão **Desbloquear usuários selecionados**.

## Aumentando a Memória do Sistema para Muitos Usuários

O tempo de processamento para uma reinicialização do domínio Informatica, para a sincronização de usuários LDAP e alguns comandos infacmd e infasetup, aumenta proporcionalmente com o número de usuários no domínio Informatica.

O número de usuários afeta o tempo de processamento dos seguintes comandos:

- infasetup BackupDomain, DeleteDomain e RestoreDomain
- infacmd isp ExportDomainObjects, ExportUsersandGroups, ImportDomainObjects e ImportUsersandGroups
- infacmd tools ExportObjects e ImportObjects

Você pode precisar aumentar a memória do sistema usada pelos Serviços Informatica, pelo infasetup e infacmd quando tiver um grande número de usuários no domínio. Para aumentar o tamanho máximo do heap, configure as seguintes variáveis de ambiente e especifique o valor em megabytes:

- INFA\_JAVA\_OPTS. Determina o tamanho máximo do heap usado pelos Serviços Informatica. Configure em cada nó onde Serviços Informatica estejam instalados.
- ICMD\_JAVA\_OPTS. Determina o tamanho máximo do heap usado pelo infacmd. Configure em cada máquina em que você execute o infacmd.
- INFA\_JAVA\_CMD\_OPTS. Determina o tamanho máximo do heap usado pelo infasetup. Configure em cada máquina em que você execute o infasetup.

Por exemplo, para configurar 2048 MB de memória do sistema no UNIX para a variável de ambiente INFA\_JAVA\_OPTS, use o seguinte comando:

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

No Windows, configure as variáveis como variáveis do sistema.

A tabela a seguir lista o requisito mínimo para as configurações de tamanho máximo do heap, com base no número de usuários e serviços no domínio:

Número de Usuários do Domínio	Tamanho Máximo do Heap (1 a 5 Serviços)	Tamanho Máximo do Heap (6-10 Serviços)
1.000 ou menos	512 MB (padrão)	1024 MB
5,000	2048 MB	3072 MB
10,000	3072 MB	5120 MB
20,000	5120 MB	6144 MB
30,000	5120 MB	6144 MB

**Nota:** As configurações do tamanho máximo do heap na tabela são baseadas no número de serviços de aplicativos no domínio.

Depois que você configurar essas variáveis de ambiente, reinicie o nó para que as alterações entrem em vigor.

## Exibindo a Atividade do Usuário

Use a guia Logs da ferramenta Administrator para exibir os logs de atividade do usuário. Exiba os logs de atividade do usuário para examinar as tentativas de logon dos aplicativos cliente da Informatica. Também é

possível exibir os logs para determinar quando um usuário criou, atualizou ou removeu serviços, nós, usuários, grupos ou funções.

Consulte o *Guia do Informatica Administrator* para obter mais informações sobre os logs de atividade do usuário e a guia Logs da ferramenta Administrator.

Também é possível usar o comando `infacmd isp getUserActivityLog` para exibir os dados do log de atividade do usuário. O comando `infacmd isp getUserActivityLog` usa a seguinte sintaxe:

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

O comando `infacmd isp getUserActivityLog` requer a função ou a associação de Administrador no grupo de Administradores. Para obter mais informações sobre o comando `isp getUserActivityLog`, consulte a *Referência de Comandos da Informatica*.

Os dados do log de atividade do usuário incluem tentativas de logon de usuário bem-sucedidas e malsucedidas de clientes da Informatica. Se o cliente definir propriedades personalizadas em solicitações de logon, os dados do log incluirão as propriedades personalizadas.

**Nota:** Os logs de atividade do usuário não incluem tentativas de logon do usuário em um domínio configurado para usar a autenticação Kerberos.

Os dados de atividade do usuário incluem as seguintes propriedades para cada tentativa de logon de um cliente da Informatica:

- Nome do aplicativo
- Versão do aplicativo
- Nome do host ou endereço IP do host do aplicativo

Você pode exibir eventos de log com base nos seguintes filtros opcionais:

- Nome de usuário
- Domínio de segurança
- Data e hora
- Ordem cronológica
- Código da atividade
- Texto da atividade

É possível exibir os eventos de log no prompt de comando ou gravar os eventos em um arquivo em um dos seguintes formatos:

- Binário
- Texto
- XML

Se você imprimir um log no formato binário, poderá usar o comando `infacmd isp convertUserActivityLog` para convertê-lo no formato de texto ou XML. Consulte a *Referência de Comandos da Informatica* para obter mais informações sobre como usar o comando `infacmd isp convertUserActivityLog`.

## Códigos de atividade do usuário

Os logs de atividade do usuário incluem códigos que indicam o sucesso ou a falha de cada atividade.

Os códigos de atividade válidos incluem o seguinte:

- CCM\_10437. Indica que uma atividade foi bem-sucedida.
- CCM\_10438. Indica que uma atividade falhou.



- CCM\_10778. Indica que uma tentativa de logon com propriedades personalizadas foi bem-sucedida.
- CCM\_10779. Indica uma falha na tentativa de logon com propriedades personalizadas.
- CCM\_10786. Indica que uma tentativa de logon sem propriedades personalizadas foi bem-sucedida.
- CCM\_10787. Indica uma falha na tentativa de logon sem propriedades personalizadas.

## Filtros de Log de Atividade do Usuário

Use um ou mais filtros para recuperar os eventos de log de usuários específicos, as datas ou os eventos.

Use um ou mais dos seguintes parâmetros do comando `infacmd isp getUserActivityLog` para filtrar os eventos de log:

### Usuários e domínios de segurança

Opcional. A lista dos usuários para os quais você deseja obter os eventos de log. Separe vários usuários com um espaço. Use o símbolo curinga (\*) para exibir logs para vários usuários em um único domínio de segurança ou todos os domínios de segurança. Por exemplo, as seguintes cadeias são os valores válidos para a opção:

```
user:Native
"user:*"
"user*"
"*_users_*"
"*:Native"
```

Adicione o seguinte parâmetro ao comando `getUserActivityLog` para filtrar eventos de log com base no usuário ou no domínio de segurança:

```
-usrs <UserName>:<SecurityDomain>
```

Por exemplo, adicione o seguinte parâmetro para recuperar a atividade do usuário de um usuário chamado User1 em todos os domínios de segurança:

```
-usrs "User1:*
```

### Data e hora

Opcional. O intervalo de datas que você deseja exibir eventos de log.

Se você digitar uma data de término anterior à data de início, o comando não retornará eventos de log.

Digite a data e a hora em um dos seguintes formatos:

- MM/dd/yyyy
- MM/dd/yyyy HH:mm:ss
- yyyy-MM-dd
- yyyy-MM-dd HH:mm:ss

Adicione o seguinte parâmetro ao comando `getUserActivityLog` para filtrar o log por data de início ou data de término:

```
-sd <start_date> -ed <end_date>
```

Por exemplo, adicione o seguinte parâmetro para recuperar a atividade do usuário entre 1º de janeiro de 2014 e 3 de fevereiro de 2014:

```
-sd 01/01/2014 -ed 02/03/2014
```

### Código da atividade

Opcional. Retorna os eventos de log com base no código da atividade.

Use o símbolo curinga (\*) para recuperar eventos de log de vários códigos da atividade. Códigos de atividade válidos incluem:

- CCM\_10437. Indica que uma atividade foi bem-sucedida.
- CCM\_10438. Indica que uma atividade falhou.
- CCM\_10778. Indica que uma tentativa de logon com propriedades personalizadas foi bem-sucedida.
- CCM\_10779. Indica uma falha na tentativa de logon com propriedades personalizadas.
- CCM\_10786. Indica que uma tentativa de logon sem propriedades personalizadas foi bem-sucedida.
- CCM\_10787. Indica uma falha na tentativa de logon sem propriedades personalizadas.

Adicione o seguinte parâmetro ao comando `getUserActivityLog` para filtrar por código da atividade:

```
-ac <activity_code>
```

Por exemplo, adicione o seguinte parâmetro para recuperar eventos de log que tiveram sucesso:

```
-ac CCM_10437
```

Se você usar o símbolo curinga, ponha o argumento entre aspas.

#### Texto da atividade

Opcional. Retorna eventos de log com base em uma cadeia encontrada no texto da atividade.

Adicione o seguinte parâmetro ao comando `getUserActivityLog` para filtrar por texto da atividade:

```
-atxt <activity_text>
```

Use o símbolo curinga (\*) para recuperar logs de vários eventos. Por exemplo, o seguinte parâmetro retorna todos os eventos de log que contêm a frase "Ativando serviço" em sua descrição:

```
-atxt "*Enabling service"
```

Se você usar o símbolo curinga, ponha o argumento entre aspas.

#### Ordem cronológica

Opcional. Imprime eventos de log em ordem cronológica inversa. Se você não especificar esse parâmetro, o comando exibirá eventos de log em ordem cronológica.

Adicione o seguinte parâmetro ao comando `getUserActivityLog` para imprimir o evento mais recente primeiro:

```
-ro true
```

## Gravar e Exibir Eventos de Log de Atividade do Usuário

Você pode gravar eventos de log de atividade do usuário para um arquivo ou exibi-los na linha de comando quando usa o comando `infacmd isp getUserActivityLog`. Grave os eventos de log de atividade do usuário no formato com base no modo como você planeja usar o arquivo de eventos de log exportado.

### Gravar e Exibir Arquivos de Log

Para gravar os eventos de log de atividade do usuário em um arquivo, execute o comando com o parâmetro `-lo` do arquivo de saída:

```
-lo output_file_name
```

Se você não especificar um formato de saída, o comando gravará os eventos de log em um arquivo de texto. Por exemplo, execute o seguinte comando para gravar eventos de log em um arquivo denominado `log.txt`:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo log.txt
```

Para especificar um formato de saída, execute o comando com o formato `-fm` do parâmetro:

```
-fm output_format_BIN_TEXT_XML
```

Os formatos válidos incluem:

- Bin (binário). Use o formato binário para fazer backup dos eventos de log no formato binário. Talvez você precise usar esse formato para enviar eventos de log ao Suporte Global a Clientes da Informatica
- Texto. Use um formato de texto se você desejar analisar os eventos de log em um editor de texto.
- XML. Use o formato XML se você desejar analisar os eventos de log em uma ferramenta externa que usa XML ou se desejar usar as ferramentas XML, como XSLT.

Se você especificar texto ou XML como o formato de saída, mas não especificar um arquivo de saída, o comando exibirá o log em texto ou em XML na linha de comando.

Se você especificar binário como o formato de saída, deverá fornecer um nome de arquivo de saída.

Por exemplo, execute o seguinte comando para imprimir eventos de log em um arquivo denominado `log.xml`:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm  
xml -lo log.xml
```

## Convertendo os Arquivos de Log

Se você usar o comando `getUserActivity` para gravar eventos de log em um arquivo binário, poderá converter o arquivo no formato de texto ou XML.

Execute o seguinte comando para converter um log binário recuperado no formato de texto ou XML:

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm  
output_format_TEXT_XML -lo output_file_name
```

Por exemplo, execute o seguinte comando para converter um arquivo de entrada binário denominado `log.bin` no formato XML e gere a saída em um arquivo denominado `convertedLog.xml`:

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

Para exibir o log na linha de comando, omita o nome do arquivo de saída.

Se você omitir o formato, o comando usará o formato de texto.

# Gerenciando grupos

Você pode criar, editar e excluir grupos no domínio de segurança nativo.

Você pode atribuir funções, permissões e privilégios a um grupo no domínio nativo ou em um domínio de segurança LDAP. Não é possível excluir ou modificar as propriedades de contas de grupo nos domínios de segurança de LDAP. As funções, as permissões e os privilégios atribuídos ao grupo determinam as tarefas que os usuários no grupo podem executar no domínio Informatica.

## Adicionando um Grupo Nativo

Adicione, edite ou remova grupos nativos na guia Segurança.

Um grupo nativo pode conter contas de usuário LDAP ou nativas, ou outros grupos nativos. É possível criar vários níveis de grupos nativos. Por exemplo, o grupo `Finanças` contém o grupo `AccountsPayable` que

contém o grupo OfficeSupplies. O grupo Finanças é o grupo pai do grupo AccountsPayable e o grupo AccountsPayable é o grupo pai do grupo OfficeSupplies. Cada grupo pode conter outros grupos nativos.

1. Na ferramenta Administrator, clique na guia Segurança.
2. No menu Ações de Segurança, clique em Criar Grupo.
3. Insira as seguintes informações para o grupo:

Propriedade	Descrição
Nome	Nome do grupo. O nome não diferencia letras maiúsculas de minúsculas e não pode exceder 128 caracteres. Não pode incluir uma guia, um caractere de nova linha nem os seguintes caracteres especiais: , + " \ < > ; / * % ? O nome pode incluir um caractere de espaço ASCII, exceto no primeiro e último caractere. Nenhum outro caractere de espaço é permitido.
Grupo Pai	Grupo ao qual o novo grupo pertence. Se você selecionar um grupo nativo antes de clicar em Criar Grupo, o grupo selecionado será o grupo pai. Caso contrário, o campo Grupo Pai exibirá Nativo, indicando que o novo grupo não pertence a um grupo.
Descrição	Descrição do grupo. A descrição do grupo não pode exceder 765 caracteres nem conter os seguintes caracteres especiais: < > "

4. Clique em Procurar para selecionar um grupo pai diferente.  
Você pode criar mais de um nível de grupos e subgrupos.
5. Clique em OK para salvar o grupo.

## Editando Propriedades de um Grupo Nativo

Depois de criar um grupo, é possível alterar a descrição do grupo e a lista de usuários no grupo. Não é possível alterar o nome do grupo nem o pai do grupo. Para alterar o pai do grupo, você deve mover o grupo para outro grupo.

1. Na ferramenta Administrator, clique na guia Segurança.
2. Na seção Grupos do Navegador, selecione um grupo nativo e clique em Editar.
3. Altere a descrição do grupo.
4. Para alterar a lista de usuários no grupo, clique na guia Usuários.  
A guia Usuários exibe a lista de usuários no domínio e a lista de usuários atribuída ao grupo.
5. Para atribuir usuários ao grupo, selecione uma conta de usuário na coluna Todos os Usuários e clique em Adicionar.
6. Para remover um usuário de um grupo, selecione uma conta de usuário na coluna Usuários Atribuídos e clique em Remover.
7. Clique em OK para salvar as alterações.

## Movendo um grupo nativo para outro grupo nativo

Para organizar os grupos de usuários no domínio de segurança nativa, é possível configurar grupos aninhados e mover um grupo para outro grupo.

Para mover um grupo nativo para outro grupo nativo, clique com o botão direito do mouse no nome de um grupo nativo na seção Grupos do Navegador e selecione Mover Grupo.

## Excluindo um grupo nativo

Para excluir um grupo nativo, clique com o botão direito do mouse no nome do grupo na seção Grupos do Navegador e selecione Excluir Grupo.

Quando você exclui um grupo, os usuários do grupo perdem sua associação no grupo e todas as permissões ou os privilégios herdados do grupo.

Quando você exclui um grupo, o Service Manager exclui todos os grupos e subgrupos que pertencem ao grupo.

## Grupos LDAP

Não é possível adicionar, editar ou excluir grupos LDAP ou modificar atribuições de usuário a grupos de LDAP na ferramenta Administrador. Você deve gerenciar atribuições de grupos e usuário no serviço de diretório do LDAP.

# Managing operating system profiles

Create and manage operating system profiles on the Security tab of the Administrator tool or from the command line. You can create, edit, and delete operating system profiles. You can assign or change the default operating system profile to users and groups.

If the Data Integration Service is configured to use operating system profiles, it runs mappings, profiles, and workflows with the operating system profile. If the PowerCenter Integration Service is configured to use operating system profiles, it runs workflows with the operating system profile.

Create, edit, and delete operating system profiles in the **Operating System Profiles** view of the **Security** tab.

Complete the following steps to create an operating system profile:

1. Enter an operating system profile name and a system user name.
2. Select the Integration Services and configure the operating system profile properties.
3. Optionally, assign permissions on the operating system profile.

You can assign users and groups to operating system profiles and assign a default profile to users and groups after you create an operating system profile.

## Propriedades do perfil do sistema operacional para o Serviço de Integração do PowerCenter

As variáveis do processo do serviço que são definidas nas propriedades da sessão e nos arquivos de parâmetro substituem as configurações de perfil do sistema operacional.

A seguinte tabela descreve as propriedades do perfil do sistema operacional para o Serviço de Integração do PowerCenter:

Propriedade	Descrição
Nome	Nome somente leitura do perfil do sistema operacional. O nome não pode exceder 128 caracteres. Ele não pode incluir espaços nem os seguintes caracteres especiais: \ / : * ? " < >   [ ] = + ; ,
Nome de usuário do sistema	Nome somente leitura de um usuário do sistema operacional que existe nas máquinas onde o Serviço de Integração do PowerCenter é executado. O Serviço de Integração do PowerCenter executa fluxos de trabalho usando o acesso do usuário do sistema definido para o perfil do sistema operacional.
\$PMRootDir	Diretório raiz acessível pelo nó. Esse é o diretório raiz de outras variáveis do processo do serviço. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   ,
\$PMSessionLogDir	Diretório dos logs de sessão. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/SessLogs.
\$PMBadFileDir	Diretório de arquivos rejeitados. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/BadFiles.
\$PMCacheDir	Diretório dos arquivos de cache de dados e de índice. Você pode aumentar o desempenho quando o diretório de cache for um local de unidade para o processo do Serviço de Integração do PowerCenter. Não use uma unidade mapeada ou montada para arquivos de cache. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/Cache.
\$PMTargetFileDir	Diretório dos arquivos de destino. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/TgtFiles.
\$PMSourceFileDir	Diretório dos arquivos de origem. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/SrcFiles.
\$PmExtProcDir	Diretório para procedimentos externos. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/ExtProc.
\$PMTempDir	Diretório dos arquivos temporários. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/Temp.
\$PMLookupFileDir	Diretório dos arquivos de pesquisa. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/LkpFiles.

Propriedade	Descrição
\$PMStorageDir	Diretório dos arquivos de tempo de execução. Arquivos de recuperação do fluxo de trabalho salvos no \$PMStorageDir configurado nas propriedades do Serviço de Integração do PowerCenter. Arquivos de recuperação de sessão salvos no \$PMStorageDir configurado no perfil do sistema operacional. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , O padrão é \$PMRootDir/Storage.
Variáveis de Ambiente	Nome e valor das variáveis de ambiente usadas pelo Serviço de Integração em tempo de execução. Se você especificar a variável de ambiente LD_LIBRARY_PATH nas propriedades de perfil do sistema operacional, o Serviço de Integração anexará o valor dessa variável à sua variável de ambiente LD_LIBRARY_PATH. O Serviço de Integração usa o valor da sua variável de ambiente LD_LIBRARY_PATH para definir as variáveis de ambiente dos processos filhos geradas para o perfil do sistema operacional. Se você não especificar a variável de ambiente LD_LIBRARY_PATH nas propriedades de perfil do sistema operacional, o Serviço de Integração usará sua variável de ambiente LD_LIBRARY_PATH.

## Propriedades do Perfil do Sistema Operacional para o Serviço de Integração de Dados

A seguinte tabela descreve as propriedades do perfil do sistema operacional para o Serviço de Integração de Dados:

Propriedade	Descrição
Nome	Nome somente leitura do perfil do sistema operacional. O nome não pode exceder 128 caracteres. Ele não pode incluir espaços ou os seguintes caracteres especiais: % * + \ / ? ; < >
Nome de usuário do sistema	Nome somente leitura de um usuário do sistema operacional existente nos sistemas em que o Serviço de Integração de Dados é executado. O Serviço de Integração de Dados executa mapeamentos, fluxos de trabalho e trabalhos de criação de perfil usando o acesso ao sistema do usuário do sistema operacional.
\$DISRootDir	Diretório raiz acessível pelo nó. Esse é o diretório raiz de outras variáveis do processo do serviço. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , [ ]
\$DISTempDir	Diretório para arquivos temporários criados quando os trabalhos são executados. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , [ ] O padrão é <diretório raiz>/disTemp. <b>Nota:</b> Se o Serviço de Integração de Dados estiver configurado para usar vários perfis do sistema operacional, especifique um diretório comum para todos os perfis porque um diretório separado para cada perfil resulta em uso excessivo de espaço em disco.
\$DISCacheDir	Diretório para arquivos de cache de dados e índice para transformações. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , [ ] O padrão é <diretório raiz>/cache.

Propriedade	Descrição
\$DISSourceDir	Diretório para arquivos simples de origem usados em um mapeamento. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , [ ] O padrão é <diretório raiz>/source.
\$DISTargetDir	Diretório para arquivos simples de destino usados em um mapeamento. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , [ ] O padrão é <diretório raiz>/target.
\$DISRejectedFilesDir	Diretório de arquivos rejeitados. Arquivos rejeitados contêm linhas que foram rejeitadas ao executar um mapeamento. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , [ ] O padrão é <diretório raiz>/reject.
\$DISLogDir	Diretório para logs. Ele não pode incluir os seguintes caracteres especiais: * ? < > "   , [ ] O padrão é <diretório raiz>/disLogs.
Ativar Propriedades de Representação do Hadoop	Indica que o Serviço de Integração de Dados usa o usuário de representação do Hadoop para executar mapeamentos, fluxos de trabalho e trabalhos de criação de perfil em um ambiente Hadoop.  O usuário de representação do Hadoop padrão é o usuário conectado. Para especificar um usuário de representação do Hadoop diferente, selecione <b>Usar o Usuário Especificado como Usuário de Representação do Hadoop</b> e insira um nome de usuário.
Variáveis de Ambiente	Nome e valor das variáveis de ambiente usadas pelo Serviço de Integração em tempo de execução.  Se você especificar a variável de ambiente LD_LIBRARY_PATH nas propriedades de perfil do sistema operacional, o Serviço de Integração anexará o valor dessa variável à sua variável de ambiente LD_LIBRARY_PATH. O Serviço de Integração usa o valor da sua variável de ambiente LD_LIBRARY_PATH para definir as variáveis de ambiente dos processos filhos geradas para o perfil do sistema operacional.  Se você não especificar a variável de ambiente LD_LIBRARY_PATH nas propriedades de perfil do sistema operacional, o Serviço de Integração usará sua variável de ambiente LD_LIBRARY_PATH.  <b>Nota:</b> No AIX, você deve definir a variável de ambiente LD_LIBRARY_PATH como INFA_HOME/services/shared/bin para o Serviço de Integração de Dados executar com êxito mapeamentos, perfis e fluxos de trabalho com perfis do sistema operacional.
Diretório de cache de arquivo simples	Diretório de cache de arquivo simples no qual a ferramenta Analyst armazena os arquivos simples carregados.  Se o Serviço Analyst conectar-se a um Serviço de Integração de Dados que usa perfis do sistema operacional, o usuário do sistema operacional especificado no perfil do sistema operacional deverá ter acesso a esse diretório de cache de arquivo simples. Quando você importa uma tabela de referência ou uma origem de arquivo simples, a ferramenta Analyst usa os arquivos desse diretório para criar uma tabela de referência ou um objeto de dados de arquivo simples. Reinicie o Serviço Analyst se você alterar a localização do arquivo simples.



## Propriedades do perfil do sistema operacional para o Serviço de Acesso a Metadados

A seguinte tabela descreve as propriedades do perfil do sistema operacional para o Serviço de Acesso a Metadados:

Propriedade	Descrição
Nome	Nome somente leitura do perfil do sistema operacional. O nome não pode exceder 128 caracteres. Ele não pode incluir espaços ou os seguintes caracteres especiais: % * + \ / ? ; < >
Nome de usuário do sistema	Nome somente leitura de um usuário do sistema operacional existente nos sistemas em que o Serviço de Acesso a Metadados é executado. O Serviço de Acesso a Metadados permite que a Developer tool acesse informações de conexão Hadoop para importar e visualizar metadados usando o acesso ao sistema do usuário do sistema operacional.
Ativar Propriedades de Representação do Hadoop	Indica que o Serviço de Acesso a Metadados usa o usuário de representação do Hadoop para importar e visualizar metadados. O usuário de representação do Hadoop padrão é o usuário conectado. Para especificar um usuário de representação do Hadoop diferente, selecione <b>Usar o Usuário Especificado como Usuário de Representação do Hadoop</b> e insira um nome de usuário.

## Criando um perfil do sistema operacional

Crie um perfil do sistema operacional e atribua-o a usuários e grupos para aumentar a segurança e isolar o ambiente do usuário em tempo de execução. Você pode criar um ou mais perfis do sistema operacional. O Serviço de Integração do PowerCenter usa o perfil do sistema operacional para executar fluxos de trabalho. O Serviço de Integração de Dados usa o perfil do sistema operacional para executar mapeamentos, perfis e fluxos de trabalho. O Serviço de Acesso a Metadados usa o perfil do sistema operacional para acessar informações de conexão Hadoop para importar e visualizar metadados.

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. No menu Ações de Segurança, clique em **Criar Perfil do Sistema Operacional**.  
A caixa de diálogo **Criar Perfil do Sistema Operacional - Etapa 1 de 3** é exibida.

3. Insira as seguintes propriedades gerais para o perfil do sistema operacional:

Propriedade	Descrição
Nome	Nome do perfil do sistema operacional. O nome não faz distinção entre maiúsculas e minúsculas, e deve ser exclusivo no domínio. Ele não pode ter mais de 128 caracteres, nem começar com @. Além disso, não pode conter os seguintes caracteres especiais: % * + \ / ? ; < > O nome pode conter um caractere de espaço ASCII, exceto para o primeiro e o último caracteres. Nenhum outro caractere de espaço é permitido.
Nome de usuário do sistema	Nome de um usuário do sistema operacional existente nas máquinas em que o Serviço de Integração é executado. O Serviço de Integração executa fluxos de trabalho ou trabalhos usando o acesso do usuário do sistema definido para o perfil do sistema operacional. <b>Nota:</b> Quando você criar perfis do sistema operacional, você não pode especificar o nome de usuário do sistema como raiz ou usar um usuário que não é raiz com uid==0.

4. Clique em **Avançar**.

A caixa de diálogo **Configurar Perfil do Sistema Operacional - Etapa 2 de 3** é exibida.

5. Selecione o serviço que usará o perfil do sistema operacional.
- Serviço de Integração do PowerCenter
  - Serviço de Integração de Dados
  - Serviço de Acesso a Metadados
6. Configure as propriedades do perfil do sistema operacional para os serviços selecionados. Para criar um perfil de sistema operacional para o Serviço de Acesso a Metadados, você também deve selecionar o Serviço de Integração de Dados junto com o Serviço de Acesso a Metadados e especificar a variável \$DISRootDir para o Serviço de Integração de Dados.
7. Se os serviços acessarem um ambiente do Hadoop em tempo de design ou em tempo de execução, configure as propriedades de representação do Hadoop da seguinte maneira:
- a. Selecione **Ativar Propriedades de Representação do Hadoop**.
  - b. Opte por usar o usuário conectado ou especifique um usuário de representação do Hadoop para executar trabalhos do Hadoop.
8. Opcionalmente, configure as variáveis de ambiente.
9. Se o Serviço Analyst conectar-se a um Serviço de Integração de Dados que usa perfis do sistema operacional, configure as propriedades do Serviço Analyst.
10. Clique em **Avançar**.
- A caixa de diálogo **Atribuir Grupos e Usuários ao Perfil do Sistema Operacional - Etapa 3 de 3** é exibida.
11. Na guia **Grupos**, atribua grupos ao perfil do sistema operacional, da seguinte maneira:
- a. Para atribuir grupos específicos ao perfil do sistema operacional, selecione um ou mais grupos e clique em **Adicionar**.
  - b. Para atribuir todos os grupos disponíveis ao perfil do sistema operacional, clique em **Adicionar Tudo**.
12. Opcionalmente, atribua o perfil do sistema operacional como o perfil padrão a um ou mais grupos. Para atribuir um perfil padrão, selecione **Perfil Padrão** para o grupo na lista Grupo(s) Selecionado(s).

13. Na guia **Usuários**, atribua usuários ao perfil do sistema operacional, da seguinte maneira:
  - a. Para atribuir usuários específicos ao perfil do sistema operacional, selecione um ou mais usuários e clique em **Adicionar**.
  - b. Para atribuir todos os usuários disponíveis ao perfil do sistema operacional, clique em **Adicionar Tudo**.
14. Opcionalmente, atribua o perfil do sistema operacional como o perfil padrão a um ou mais usuários. Para atribuir um perfil padrão, selecione **Perfil Padrão** para o usuário na lista Usuário(s) Selecionado(s).
15. Clique em **Concluir**.

Após a criação do perfil do sistema operacional, o painel de detalhes mostra as propriedades desse perfil e os grupos e usuários aos quais ele está atribuído.

## Editando um perfil do sistema operacional

É possível editar um perfil do sistema operacional para alterar as propriedades desse perfil.

Não é possível editar o nome ou o nome de usuário do sistema depois de criar um perfil do sistema operacional. Se não quiser usar o usuário do sistema operacional especificado no perfil do sistema operacional, exclua esse perfil.

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Selecione a exibição **Perfis do Sistema Operacional**.
3. Selecione o perfil do sistema operacional.
4. Na guia **Propriedades**, clique em **Editar**.

A caixa de diálogo **Editar Propriedades** é exibida.
5. Selecione o Serviço de Integração de Dados, o Serviço de Integração do PowerCenter ou o Serviço de Acesso a Metadados que você deseja configurar.
6. Edite as propriedades do serviço.
7. Clique em **OK**.

## Atribuindo um perfil do sistema operacional padrão a um usuário ou grupo

Quando um usuário ou grupo tem acesso a mais de um perfil do sistema operacional, atribua um perfil do sistema operacional padrão que o Serviço de Integração utiliza para executar trabalhos e fluxos de trabalho. É possível atribuir qualquer perfil do sistema operacional com permissões diretas como o perfil padrão para um usuário ou grupo. Um usuário ou grupo pode ter somente um perfil padrão de sistema operacional. No entanto, você pode atribuir o mesmo perfil do sistema operacional como o perfil padrão a mais de um usuário ou grupo.

1. Na guia Segurança, selecione a exibição **Usuários** ou **Grupos**.
2. No Navegador, selecione um usuário ou grupo.
3. No painel de conteúdo, selecione a exibição **Permissões**.
4. Clique na guia **Perfis do Sistema Operacional**.
5. Clique no botão **Atribuir ou Alterar o Perfil do Sistema Operacional Padrão**.

A caixa de diálogo **Atribuir ou Alterar o Perfil do Sistema Operacional** é exibida.

6. Selecione um perfil na lista **Perfil do Sistema Operacional Padrão**. Ou, selecione **Não atribuir um perfil do sistema operacional padrão** na lista para remover o perfil padrão que está atribuído a um usuário ou grupo.
7. Clique em **OK**.  
No painel de detalhes, a coluna **Perfil Padrão** exibe **Sim (Direto)** para o perfil do sistema operacional.

## Excluindo um perfil do sistema operacional

Para excluir um perfil do sistema operacional, clique com o botão direito do mouse no nome dele na seção Perfil do Sistema Operacional do Navegador e selecione **Excluir Perfil**.

Depois de excluir um perfil do sistema operacional, atribua outro aos usuários e grupos aos quais ele estava atribuído como o perfil padrão. Se o Serviço de Integração do PowerCenter usar perfis do sistema operacional, atribua outro perfil do sistema operacional às pastas de repositório e aos fluxos de trabalho aos quais esse perfil do sistema operacional estava atribuído.

## Working with Operating System Profiles in a Secure Domain

You can use operating system profiles in an Informatica domain that has secure communication enabled.

Consider the following rules and guidelines when you use operating system profiles in a domain that has secure communication enabled:

You must set the following environment variable for the operating system profile:

### **INFA\_TRUSTSTORE**

Set the value to the directory that contains the truststore files for the SSL certificates for the secure domain. The directory must contain a truststore file named `infa_truststore.pem`.

### **INFA\_TRUSTSTORE\_PASSWORD**

If you use a custom truststore, set the value to the password for the `infa_truststore.pem` that contains the SSL certificate for the secure domain. The password must be encrypted. Use the command line program `pmpasswd` to encrypt the password.

Additionally, if the PowerCenter Integration Service uses the Session on Grid option, you must set the following environment variable for the operating system profile:

### **INFA\_KEYSTORE**

Set the value to the directory that contains the keystore files for the SSL certificates for the secure domain. The directory must contain a keystore file named `infa_keystore.pem`.

You can set the environment variables for the operating system profile in the Administrator tool. To set the environment variables for the operating system profile, click **Security > Operating System Profiles**. Edit the properties of the operating system profile and set the environment variables.

# Trabalhando com Perfis do Sistema Operacional em um Domínio com Autenticação Kerberos

Você pode usar perfis do sistema operacional em um domínio Informatica que é executado em uma rede com autenticação Kerberos.

Considere as seguintes regras e diretrizes quando você usar perfis do sistema operacional em um domínio que é executado em uma rede com a autenticação Kerberos:

- A conta de usuário do perfil do sistema operacional deve ser uma entidade de segurança no serviço do Active Directory usado para a autenticação Kerberos e importado para um domínio de segurança LDAP no domínio Informatica.
- A conta de usuário deve ter um arquivo de cache de credenciais Kerberos que é acessível para a conta de usuário do perfil do sistema operacional. Cada conta de usuário do perfil do sistema operacional deve ter um arquivo de cache de credenciais.
- O arquivo de cache de credenciais da conta de usuário do perfil do sistema operacional deve ser encaminhável. Por exemplo, se você usar o utilitário *kinit* para criar o arquivo de cache de credenciais, você deve incluir a opção *-f*.
- O arquivo de cache de credenciais da conta de usuário do perfil do sistema operacional deve estar disponível quando você executa um fluxo de trabalho que usa um perfil do sistema operacional.
- O arquivo de cache de credenciais da conta de usuário do perfil do sistema operacional deve sempre ter as credenciais mais recentes. Você pode executar um utilitário de agendador de trabalho, como *cron*, para atualizar frequentemente as credenciais do usuário no arquivo de cache de credenciais.
- Você deve definir as seguintes variáveis de ambiente para o perfil do sistema operacional:

## **INFA\_OSPI\_SECURITY\_DOMAIN**

Defina o valor do nome do domínio de segurança que contém a conta de usuário do perfil do sistema operacional. Se a conta de usuário estiver no domínio de segurança do realm do usuário do Kerberos, você não precisará definir essa variável. O domínio de segurança do realm do usuário do Kerberos é o domínio de segurança criado durante a instalação que tem o mesmo nome do realm do usuário Kerberos.

## **KRB5\_CONFIG**

Defina a variável como o caminho e o nome do arquivo de configuração Kerberos. O nome do arquivo de configuração Kerberos é *krb5.conf*.

## **KRB5CCNAME**

Defina o valor para o caminho e o nome do arquivo de cache de credenciais Kerberos como a conta de usuário do perfil do sistema operacional.

You can set the environment variables for the operating system profile in the Administrator tool. To set the environment variables for the operating system profile, click **Security > Operating System Profiles**. Edit the properties of the operating system profile and set the environment variables.

# Bloqueio de conta

Para aumentar a segurança do domínio Informatica, um administrador pode impor o bloqueio de contas de usuário no domínio, inclusive de outros usuários administradores, após várias falhas de logon.

O administrador pode especificar o número de tentativas de logon com falha que um usuário pode fazer antes de bloquear sua conta. Se uma conta for bloqueada, o administrador poderá desbloqueá-la no domínio Informatica.

Quando o administrador desbloquear uma conta de usuário, ele poderá selecionar a opção "Desbloquear o usuário e redefinir a senha" para redefinir a senha do usuário. O administrador pode enviar um e-mail ao usuário para solicitar que ele altere a senha antes de fazer logon no domínio novamente. Para ativar o domínio para enviar e-mails aos usuários quando suas senhas forem redefinidas, configure as definições do servidor de e-mail para o domínio.

Se o usuário for bloqueado no domínio Informatica e no servidor LDAP, o administrador do Informatica poderá desbloquear a conta de usuário no domínio Informatica. O usuário só poderá fazer logon no domínio Informatica quando o administrador LDAP também desbloquear a conta de usuário no servidor LDAP.

**Nota:** Se o domínio Informatica usa a autenticação de rede Kerberos, você não pode configurar o bloqueio de contas de usuário. A exibição **Gerenciamento de Conta** não está disponível na guia **Segurança** da ferramenta Administrator.

## Configurando o bloqueio de conta

Selecione as opções de bloqueio de conta para bloquear contas de usuário no domínio Informatica após várias falhas de logon.

1. Na ferramenta Administrator, clique em **Segurança > Gerenciamento de Conta**.
2. Na seção **Configuração de Bloqueio de Conta**, clique em **Editar**.
3. Defina as seguintes propriedades:

Propriedade	Descrição
Ativar Bloqueio de Conta	Força o bloqueio de uma conta de usuário no domínio Informatica após um número especificado de logons com falha. Por padrão, essa opção não força o bloqueio de contas de usuário de administrador. Você deve selecionar a opção <b>Ativar Bloqueio de Conta de Administrador</b> para forçar o bloqueio de contas de usuário de administrador.
Ativar Bloqueio de Conta de Administrador	Força o bloqueio de uma conta de usuário de administrador no domínio Informatica após um número especificado de logons com falha. Você deve selecionar a opção <b>Ativar Bloqueio de Conta</b> para forçar o bloqueio de contas de usuário de administrador.
Máximo de Tentativas de Logon	Especifica o número máximo permitido de falhas de logon consecutivas para bloquear uma conta de usuário no domínio Informatica.

## Regras e diretrizes para o bloqueio de conta

Considere as seguintes regras e diretrizes na hora de impor o bloqueio de conta para os usuários do Informatica:

- Se um serviço de aplicativo é executado com uma conta de usuário e a senha errada é fornecida para o serviço de aplicativo, a conta de usuário pode se tornar bloqueada quando o serviço de aplicativo tenta iniciar. O Serviço de Integração de Dados, o Serviço do Web Services Hub e o Serviço de Integração do PowerCenter são serviços de aplicativo resilientes que usam um nome de usuário e senha para autenticar no Serviço de Repositório do Modelo ou no Serviço do Repositório do PowerCenter. Se o Serviço de Integração de Dados, o Serviço do Web Services Hub ou o Serviço de Integração do PowerCenter tentar reiniciar várias vezes após uma falha de logon, o domínio acabará bloqueando a conta de usuário associada.
- Se uma conta de usuário LDAP estiver bloqueada no domínio Informatica e no servidor de autenticação LDAP, o administrador do domínio Informatica poderá desbloqueá-la no domínio Informatica. O administrador do LDAP poderá desbloquear a conta de usuário no servidor LDAP.
- Se você ativar o bloqueio de conta no domínio Informatica e no servidor LDAP, configure o mesmo limite de falhas de logon no domínio Informatica e no servidor LDAP para evitar confusão em relação à diretiva de bloqueio de conta.
- Se o bloqueio de conta não estiver ativado no domínio Informatica, mas um usuário estiver bloqueado, verifique se o usuário não está bloqueado no servidor LDAP.

## CAPÍTULO 9

# Privilégios e funções

Este capítulo inclui os seguintes tópicos:

- [Privilégios, 144](#)
- [Funções, 145](#)
- [Privilégios do domínio, 146](#)
- [Privilégios do Serviço Analyst, 153](#)
- [Privilégios do Serviço do Gerenciamento de Conteúdo, 155](#)
- [Privilégios do Data Integration Service, 155](#)
- [Privilégio do Serviço de Ingestão em Massa, 156](#)
- [Privilégios do Serviço do Metadata Manager, 156](#)
- [Privilégios do Serviço de Repositório do Modelo, 159](#)
- [Privilégios do Serviço de Repositório do PowerCenter, 160](#)
- [Privilégios do Serviço do Ouvinte do PowerExchange, 175](#)
- [Privilégios do Serviço do Agente de Log do PowerExchange, 175](#)
- [Privilégios do Serviço de Agendador, 176](#)
- [Privilégios do Serviço do Test Data Manager, 177](#)
- [Gerenciando Funções, 180](#)
- [Atribuindo privilégios e funções aos usuários e grupos, 183](#)
- [Exibindo usuários com privilégios para um serviço, 185](#)
- [Solucionando problemas de privilégios e funções, 185](#)

## Privilégios

Os privilégios determinam as ações que os usuários podem executar nos aplicativos clientes. O Informatica inclui os seguintes privilégios:

- Privilégios de domínio. Determine as ações que os usuários podem executar no domínio Informatica usando a ferramenta Administrator e os programas de linha de comando infacmd e pmrep.
- Privilégio do Serviço Analyst. Determina ações que os usuários podem executar usando o Informatica Analyst.
- Privilégio do Serviço do Gerenciamento de Conteúdo. Determina ações que os usuários podem executar usando tabelas de referência na Informatica Developer tool e na ferramenta Informatica Analyst.



- Privilégio do Serviço de Integração de Dados. Determina ações que os usuários podem executar nos aplicativos usando a ferramenta Administrator e o programa de linha de comando infacmd. Este privilégio também determina se os usuários podem fazer uma busca detalhada e exportar os resultados do perfil.
- Privilégio do Serviço de Ingestão em Massa. Determina ações que os usuários podem realizar usando a ferramenta Ingestão em Massa.
- Privilégios do Serviço do Metadata Manager. Determina ações que os usuários podem executar usando o Metadata Manager.
- Privilégio do Serviço de Repositório do Modelo. Determina ações em projetos que os usuários podem executar usando o Informatica Analyst e Informatica Developer.
- Privilégios do Serviço do Repositório do PowerCenter. Determine as ações de repositório do PowerCenter que os usuários podem executar usando o Repository Manager, o Designer, o Workflow Manager, o Workflow Monitor e os programas de linha de comando pmrep e pmcmd.
- Privilégios do serviço de aplicativo do PowerExchange. Determine as ações que os usuários podem executar no Serviço do Ouvinte do PowerExchange e no Serviço do Agente de Log do PowerExchange usando comandos infacmd pwx.
- Os privilégios do Serviço do Agendador. Determine as ações que os usuários podem realizar usando o Serviço do Agendador.
- Privilégios do Serviço do Test Data Manager. Determinam as tarefas de descoberta, mascaramento, subconjunto e geração de dados de teste que os usuários podem executar usando o Test Data Manager.

Atribua privilégios a usuários e grupos para os serviços de aplicativo. Atribua diferentes privilégios a um usuário para cada serviço de aplicativo do mesmo tipo de serviço.

Atribua privilégios a usuários e grupos na **guia Segurança** da ferramenta Administrator.

A ferramenta Administrator organiza os privilégios em níveis. Um privilégio é listado abaixo do privilégio que ela inclui. Alguns privilégios incluem outros privilégios. Quando você atribui um privilégio a usuários e grupos, a ferramenta Administrator também atribui quaisquer privilégios incluídos.

## Grupos de Privilégio

Os privilégios do serviço de aplicativo e do domínio são organizados em grupos de privilégio. Um grupo de privilégio é uma organização de privilégios que define ações comuns do usuário. Por exemplo, os privilégios do domínio incluem os seguintes grupos de privilégio:

- Ferramentas. Inclui privilégios para fazer logon na ferramenta Administrator.
- Administração de segurança. Inclui privilégios para gerenciar usuários, grupos, funções e privilégios.
- Administração de Domínio. Inclui privilégios para gerenciar o domínio, pastas, nós, grades, licenças e serviços de aplicativo.

**Sugestão:** Quando você atribui privilégios a usuários e grupos de usuários, pode selecionar um grupo de privilégio para atribuir todos os privilégios no grupo.

## Funções

Uma função é um conjunto de privilégios atribuídos a um usuário ou grupo. Cada usuário de uma organização tem uma função específica, seja como desenvolvedor, administrador, usuário básico ou usuário avançado.

Por exemplo, a função de desenvolvedor do PowerCenter abrange todos os privilégios ou ações do Serviço do Repositório do PowerCenter, executados por um desenvolvedor.

Você atribui uma função a usuários e grupos para o domínio e para serviços de aplicativo no domínio.

**Sugestão:** Se você organizar usuários em grupos e, em seguida, atribuir funções e permissões para os grupos, poderá simplificar as tarefas de administração do usuário. Por exemplo, se um usuário mudar de cargo na organização, mova o usuário para outro grupo. Se um novo usuário entrar na organização, adicione o usuário a um grupo. Os usuários herdarão as funções e permissões atribuídas ao grupo. Não é necessário reatribuir privilégios, funções e permissões. Para obter mais informações, consulte o seguinte artigo da Biblioteca de Instruções da Informatica: [Using Groups and Roles to Manage Access Controls](#).

## Privilégios do domínio

Os privilégios de domínio determinam as ações que os usuários podem executar com a ferramenta Administrator e os programas de linha de comando infacmd e pmrep.

A tabela a seguir descreve cada grupo de privilégios de domínio:

Grupo de Privilégios	Descrição
Administração de Segurança	Inclui privilégios para gerenciar usuários, grupos, funções e privilégios.
Administração de Domínio	Inclui privilégios para gerenciar o domínio, pastas, nós, grades, licenças, serviços de aplicativo, conexões e configurações do cluster.
Monitoramento	Inclui privilégios para configurar as estatísticas e os relatórios de monitoramento, exibir o monitoramento dos objetos de integração e acessar o monitoramento.
Ferramentas	Inclui privilégios para fazer logon na ferramenta Administrator.
Administração de Nuvem	Inclui privilégios para adicionar organizações do Informatica Cloud na ferramenta Administrator e exibi-las.

### Grupo de privilégio Administração de segurança

Os privilégios no grupo de privilégio Administração de segurança e as permissões de objeto de domínio determinam as tarefas de gerenciamento de segurança que os usuários podem executar.

Algumas tarefas de gerenciamento de segurança são determinadas pela função Administrator, não por privilégios ou permissões. Um usuário que tenha recebido a função Administrator para o domínio pode executar as seguintes tarefas:

- Criar, editar e excluir perfis do sistema operacional.
- Conceder permissão para perfis do sistema operacional.

**Nota:** Para executar tarefas de gerenciamento de segurança na ferramenta Administrator, os usuários também devem ter o privilégio Acessar Informatica Administrator.

## O privilégio Conceder e privilégio de funções

Os usuários atribuídos ao privilégio Conceder e privilégios de funções pode atribuir privilégio e funções a usuários e grupos.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Conceder e privilégio de funções:

Permissão Ativada	Descrição
Domínio ou serviço de aplicativo	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Atribuir privilégios e funções para usuários e grupos do domínio ou serviço de aplicativo.</li><li>- Editar e remover as funções e os privilégios atribuídos a usuários e grupos.</li></ul>

## Privilégios Gerenciar usuários, grupos e funções

Os usuários atribuídos ao privilégio gerenciar usuários, grupos e funções pode configurar autenticação LDAP e gerenciar usuários, grupos e funções.

O privilégio Gerenciar usuários, grupos e funções inclui o privilégio Conceder Privilégios e Funções.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com privilégio gerenciar usuários, grupos e funções:

Permissão Ativada	Descrição
-	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Configurar a autenticação LDAP para o domínio.</li><li>- Criar, editar e excluir usuários, grupos e funções.</li><li>- Importar usuários e grupos LDAP.</li></ul>
Perfil do sistema operacional	O usuário é capaz de editar propriedades de perfil do sistema operacional.

## Grupo de Privilégios Administração de Domínio

As tarefas de gerenciamento de domínio que os usuários podem executar dependem de privilégios do grupo Administração de Domínio e de permissões sobre objetos de domínio.

Algumas tarefas de gerenciamento de domínio são determinadas pela função Administrador, não por privilégios nem por permissões. Um usuário que tenha recebido a função Administrador para o domínio pode executar as seguintes tarefas:

- Configurar propriedades do domínio.
- Definir as configurações de cluster.
- Conceder permissão no domínio.
- Gerenciar e limpar eventos de log.
- Receber alertas de domínio.
- Executar o Relatório da Licença.
- Exibir eventos de log de atividade do usuário.
- Desligar o domínio.
- Acesse o assistente de atualização de serviço.

Usuários que receberam a atribuição de permissões de objeto de domínio, mas não os privilégios, podem concluir algumas tarefas de gerenciamento de domínio. A tabela a seguir lista as ações que usuários podem executar quando eles são atribuídos somente a permissões de objeto de domínio:

Permissão Ativada	Descrição
Domínio	O usuário pode executar as seguintes ações: <ul style="list-style-type: none"><li>- Exibir propriedades do domínio e eventos de log.</li><li>- Configurar as definições de monitoramento.</li></ul>
Pasta	O usuário pode exibir as propriedades da pasta.
Serviço de aplicativo	O usuário pode exibir as propriedades do serviço de aplicativo e os eventos do log.
Objeto de licença	O usuário pode exibir as propriedades do objeto de licença.
Grade	O usuário pode exibir as propriedades de grade.
Nó	O usuário pode exibir as propriedades do nó.
Hub de Serviços da Web	O usuário pode executar o Relatório de Serviços da Web.

**Nota:** Para executar tarefas de gerenciamento de domínio na ferramenta Administrador, os usuários também devem ter privilégio de acesso de Informatica Administrator.

## Privilégio Gerenciar Execução de Serviço

Os usuários atribuídos ao privilégio Gerenciar Execução de Serviços pode ativar e desativar os serviços de aplicativo e receber alertas de serviços de aplicativo.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar Execução de Serviços:

Permissão Ativada	Descrição
Serviço de aplicativo	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Ativar e desativar serviços de aplicativo e processos de serviço. Para ativar e desativar um Serviço do Metadata Manager, os usuários também devem ter permissão para o Serviço de Integração do PowerCenter associado e para o Serviço de Repositório do PowerCenter.</li><li>- Receber alertas de serviços de aplicativo.</li></ul>

## Privilégio Gerenciar Serviços

Os usuários atribuídos ao privilégio Gerenciar Serviços pode criar, configurar, mover, remover e conceder permissão sobre serviços de aplicativo e objetos de licença.

O privilégio Gerenciar Serviços inclui o privilégio Gerenciar Execução de Serviços.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar Serviços:

Permissão Ativada	Descrição
Pasta pai ou de domínio	O usuário pode criar objetos de licença.
A pasta pai ou de domínio, o nó ou a grade onde é executado o serviço de aplicativo, o objeto de licença e qualquer serviço de aplicativo associado	O usuário pode criar serviços de aplicativo.
Serviço de aplicativo	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> <li>- Configurar serviços de aplicativo.</li> <li>- Conceder permissão para serviços de aplicativo.</li> </ul>
Pastas de origem e de destino	O usuário pode mover serviços de aplicativo ou objetos de licença de uma pasta para outra.
Pasta pai ou de domínio e serviço de aplicativo	O usuário pode remover serviços de aplicativo.
Serviço Analyst	O usuário pode criar e excluir tabelas de trilha de auditoria.
Serviço do Metadata Manager	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> <li>- Fazer backup do conteúdo de repositório do Metadata Manager.</li> <li>- Excluir o conteúdo de repositório do Metadata Manager.</li> <li>- Fazer upgrade do conteúdo do Serviço do Metadata Manager.</li> </ul> <p><b>Nota:</b> Para criar ou restaurar o conteúdo de repositório do Metadata Manager, o usuário deve pertencer ao grupo Administrador padrão.</p>
Serviço do Metadata Manager Serviço do Repositório do PowerCenter	O usuário pode restaurar o repositório do PowerCenter do Metadata Manager.
Serviço de Repositório do Modelo	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> <li>- Criar e excluir conteúdo do repositório do Modelo.</li> <li>- Criar, excluir e reindexar o índice de pesquisa.</li> <li>- Atualizar o conteúdo do Serviço de Repositório do Modelo do menu <b>Ações</b> ou da linha de comando. O usuário também deve ter os privilégios de Criar, Editar e Excluir Projetos no Serviço de Repositório do Modelo e permissão de gravação nos projetos.</li> </ul>
Serviço de Integração do PowerCenter	O usuário pode executar o Serviço de Integração do PowerCenter no modo de segurança.

Permissão Ativada	Descrição
Serviço do Repositório do PowerCenter	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Fazer backup, restauração e upgrade do repositório do PowerCenter.</li> <li>- Configurar linhagem de dados para o repositório do PowerCenter.</li> <li>- Copiar conteúdo de outro repositório do PowerCenter.</li> <li>- Fechar conexões do usuário e liberar bloqueios do repositório do PowerCenter.</li> <li>- Criar e excluir conteúdo do repositório do PowerCenter.</li> <li>- Criar, editar e excluir extensões reutilizáveis de metadados no Gerente de repositório do PowerCenter.</li> <li>- Ativar controle de versão para o repositório do PowerCenter.</li> <li>- Gerenciar um domínio de repositório do PowerCenter.</li> <li>- Executar uma limpeza avançada das versões de objeto no nível de repositório do PowerCenter Repository Manager.</li> <li>- Registrar e cancelar o registro de plug-ins do repositório do PowerCenter.</li> <li>- Executar o repositório do PowerCenter em modo exclusivo.</li> <li>- Enviar notificações de repositório do PowerCenter aos usuários.</li> <li>- Atualizar estatísticas do repositório do PowerCenter.</li> <li>- Atualizar o conteúdo do Serviço do Repositório do PowerCenter.</li> </ul>
Serviço do Test Data Manager	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Criar e excluir o conteúdo do repositório do Test Data Manager.</li> <li>- Atualizar o conteúdo do Serviço do Test Data Manager.</li> </ul>
Objeto de licença	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Editar objetos de licença.</li> <li>- Conceder permissão para objetos de licença.</li> </ul>
Objeto de licença e serviço de aplicativo	O usuário pode atribuir uma licença a um serviço de aplicativo.
Pasta pai ou de domínio e objeto de licença	O usuário pode remover objetos de licença.

## Privilégio Gerenciar nós e grades

Os usuários atribuídos ao privilégio Gerenciar nós e grades pode criar, configurar, mover, remove, desative e conceder permissão sobre nós e grades.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar nós e grades:

Permissão Ativada	Descrição
Pasta pai ou do domínio	O usuário é capaz de criar nós.
Pasta pai ou de domínio e nós atribuídos à grade	O usuário é capaz de criar grades.
Nó ou grade	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Configurar e encerrar nós e grades.</li> <li>- Conceder permissão para nós e grades.</li> </ul>
Pastas de origem e destino	O usuário é capaz de mover nós e grades de uma pasta para outra.
Pasta pai ou de domínio e nó ou grade	O usuário é capaz de remover nós e grades.

## Privilégio Gerenciar pastas do domínio

Os usuários atribuídos ao privilégio Gerenciar pastas do domínio pode criar, editar, mover, remover e conceder permissão em pastas do domínio.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar pastas do domínio:

Permissão Ativada	Descrição
Pasta pai ou do domínio	O usuário é capaz de criar pastas.
Pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Editar pastas.</li><li>- Conceder permissão para pastas.</li></ul>
Pastas de origem e destino	O usuário é capaz de mover pastas de uma pasta pai para outra.
Pasta pai ou de domínio e pasta sendo removida	O usuário é capaz de remover pastas.

## Privilégio Gerenciar conexões

Os usuários atribuídos ao privilégio Gerenciar conexões pode criar, editar e excluir conexões na ferramenta Administrator, a ferramenta Analyst, a ferramenta Desenvolvedor, e o programa de linha de comando infacmd. Os usuários também pode copiar conexões na ferramenta Desenvolvedor e pode conceder permissões em conexões na ferramenta Administrator e o programa de linha de comando infacmd.

Os usuários atribuídos ao privilégio Gerenciar Conexões também podem criar, atualizar e excluir as configurações do cluster, além de definir e limpar as propriedades de configuração na ferramenta Administrator e no programa de linha de comando infacmd.

Usuários com permissões de conexão, mas não o privilégio Gerenciar conexões pode executar as seguintes ações de gerenciamento de conexão:

- Exibir todos os metadados de conexão, exceto senhas. Requer permissão de leitura na conexão.
- Visualizar dados ou executar um mapeamento, scorecard ou perfil. Requer permissão de execução na conexão.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar conexões:

Permissão	Descrição
-	O usuário é capaz de criar conexões e configurações do cluster.
Gravar na conexão	O usuário é capaz de copiar, editar e excluir conexões.
Conceder na conexão	O usuário é capaz de conceder e revogar permissões nas conexões.
Gravar na configuração de cluster	O usuário é capaz de criar, atualizar e excluir configurações do cluster. O usuário é capaz de definir e limpar propriedades de configuração de cluster.

## Grupo de privilégio Monitoramento

Os privilégios no grupo de privilégio Monitoramento determinam quais usuários podem visualizar e configurar o monitoramento.

A seguinte tabela lista as permissões necessárias e as ações que os usuários podem realizar com os privilégios no grupo Gerenciar Monitoramento:

Privilégio pai	Privilégio	Permissão Ativada	Descrição
Gerenciar Monitoramento	Configuração de Monitoramento	Domínio	O usuário pode definir configurações de monitoramento.
Gerenciar Monitoramento	Configurações de Relatórios e Estatísticas	Domínio	O usuário pode configurar o monitoramento de estatísticas e relatórios.
Exibição	Exibir Trabalhos de Todos os Usuários nos Grupos aos quais o Usuário Pertence	Domínio	Um usuário em um grupo pode monitorar os trabalhos executados por outros usuários nesse grupo. Se o usuário pertencer a vários grupos, ele poderá ver os trabalhos de todos esses grupos.
Exibir Trabalhos de Todos os Usuários nos Grupos aos quais o Usuário Pertence	Exibir Trabalhos e Outros Usuários	Domínio	O usuário pode visualizar trabalhos de outros usuários.
Exibição	Exibir Estatísticas	Domínio	O usuário pode visualizar a exibição Estatísticas de Resumo e as estatísticas de objetos de domínio. <b>Nota:</b> Em um domínio que usa a autenticação Kerberos, os usuários também devem ter a função Administrador do Serviço de Repositório do Modelo de monitoramento para exibir a exibição Estatísticas de Resumo e as estatísticas dos objetos do domínio.
Exibição	Exibir Relatórios	Domínio	O usuário pode exibir relatórios para objetos de domínio.
Monitoramento de acesso	Acesso com a Ferramenta Analyst	Domínio	O usuário pode acessar o espaço de trabalho Status do Trabalho na ferramenta Analyst.
Monitoramento de acesso	Acesso com a Developer Tool	Domínio	O usuário pode acessar a ferramenta Monitoring na Developer tool.
Monitoramento de acesso	Acesso com a Ferramenta Administrador	Domínio	O usuário pode acessar a guia Monitor na ferramenta Administrator.
N/D	Executar Ações nas Tarefas	Domínio	O usuário pode executar as seguintes ações: - Anular trabalhos. - Reemitir trabalhos de mapeamento. - Visualizar logs de trabalho.

Os usuários não precisam do privilégio Acessar Informatica Administrator para acessar a ferramenta Monitoring.



## Grupo de privilégio Ferramentas

O privilégio no grupo Ferramentas do domínio determina quais usuários podem acessar a ferramenta Administrator.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio no grupo Ferramentas:

Privilégio	Descrição
Acessar Informatica Administrator	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"><li>- Efetue login na ferramenta Administrator.</li><li>- Gerencie a conta do usuário na ferramenta Administrator.</li><li>- Exporte eventos de log.</li></ul>

Os usuários devem ter o privilégio Acessar Informatica Administrator para concluir as tarefas na ferramenta Administrator. Os usuários não precisam do privilégio Acessar Informatica Administrator para executar comandos infacmd ou acessar a ferramenta Monitoramento.

## Grupo de Privilégio da Administração de Nuvem

Os privilégios no grupo Administração de Nuvem determinam quais usuários podem exibir e configurar as organizações do Informatica Cloud.

A seguinte tabela lista as permissões necessárias e as ações que os usuários podem executar com os privilégios no grupo Administração de Nuvem:

Privilégio	Permissão Ativada	Descrição
Exibir Organização	Domínio	O usuário pode exibir as organizações do Informatica Cloud, os Agentes Seguros e as conexões de nuvem associadas.
Gerenciar Organização	Domínio	O usuário pode adicionar organizações do Informatica Cloud na ferramenta Administrator.

## Privilégios do Serviço Analyst

O privilégio do Serviço Analyst determina ações que usuários licenciados podem executar em projetos usando a ferramenta Analyst.

A tabela a seguir lista os privilégios e permissões necessários para gerenciar projetos e objetos nos projetos:

Privilégio	Permissão	Descrição
Executar Perfis e Scorecards	Ler em projetos. Executar na conexão de fonte de dados relacionais.	O usuário pode executar perfis e scorecards para usuários licenciados na ferramenta Analyst.
Acessar Especificações de Mapeamento	Ler em projetos.	O usuário pode acessar as especificações de mapeamento de usuários licenciados na ferramenta Analyst.
Carregar Resultados da Especificação de Mapeamento	Gravar em projetos.	O usuário pode carregar os resultados de uma especificação de mapeamento de usuários licenciados em uma tabela ou arquivo simples. <b>Nota:</b> A seleção desse privilégio também concede o privilégio <b>Acessar Especificações de Mapeamento</b> por padrão.
Gerenciar Glossários	-	O usuário pode gerenciar o glossário comercial.
Exibir Glossários	-	O usuário é capaz de visualizar ativos publicados do Business Glossary no espaço de trabalho Biblioteca. Isso é equivalente a fornecer permissão de leitura para glossários e ativos de Glossário no espaço de trabalho Segurança do Glossário.
Acesso a Espaços de Trabalho	-	O usuário pode acessar os seguintes espaços de trabalho na ferramenta Analyst: - <b>Design</b> - <b>Descoberta</b> - <b>Glossário</b> - <b>Scorecards</b> <b>Nota:</b> A seleção desse privilégio também concede acesso aos projetos na ferramenta Analyst. Caso o usuário não tenha esse privilégio, ele deverá ter o privilégio <b>Espaço de Trabalho de Design</b> , <b>Espaço de Trabalho de Descoberta</b> , <b>Espaço de Trabalho de Glossário</b> ou <b>Espaço de Trabalho de Scorecards</b> para acessar projetos.
Espaço de Trabalho Design	-	O usuário pode acessar o espaço de trabalho <b>Design</b> .
Espaço de Trabalho Descoberta	-	O usuário pode acessar o espaço de trabalho <b>Descoberta</b> .
Espaço de Trabalho Glossário	-	O usuário pode acessar o espaço de trabalho <b>Glossário</b> .
Espaço de Trabalho Scorecards	-	O usuário pode acessar o espaço de trabalho <b>Scorecards</b> .

# Privilégios do Serviço do Gerenciamento de Conteúdo

Os privilégios do Serviço do Gerenciamento de Conteúdo determinam as ações que usuários licenciados podem executar em tabelas de referência.

A tabela a seguir lista os privilégios e as permissões necessárias para gerenciar as tabelas de referência:

Privilégio	Permissão	Descrição
Criar Tabelas de Referência	Gravação no projeto	<ul style="list-style-type: none"><li>- Crie uma tabela de referência nas ferramentas Analyst e Developer.</li><li>- Crie uma tabela de referência usando infacmd rtm import.</li><li>- Importe um objeto de tabela de referência para o repositório do Modelo.</li><li>- Copie uma tabela de referência nas ferramentas Analyst e Developer.</li><li>- Crie uma tabela de referência a partir de dados do perfil.</li></ul> <b>Nota:</b> O privilégio Criar também concede o privilégio Editar por padrão.
Editar Dados e Metadados da Tabela de Referência	Leitura do projeto	<ul style="list-style-type: none"><li>- Edite os valores dos dados de tabela de referência nas ferramentas Developer e Analyst.</li><li>- Adicione um perfil de dados a uma tabela de referência.</li><li>- Adicione ou exclua colunas em uma tabela de referência. Altere os metadados da tabela de referência, como nomes de coluna, descrições e valores padrão.</li></ul>

## Privilégios do Data Integration Service

O privilégio do Data Integration Service determina ações que os usuários podem executar nos aplicativos usando a ferramenta Administrador e o programa de linha de comando infacmd. Eles também determinam se os usuários podem fazer uma busca detalhada e exportar resultados de perfil usando as ferramentas Analyst e Desenvolvedor.

A seguinte tabela lista as ações que usuários podem realizar com o privilégio no grupo de privilégio Administração do Aplicativo:

Nome do privilégio	Descrição
Gerenciar aplicativos	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"><li>- Faça backup e restaure um aplicativo para um arquivo.</li><li>- Implantar um aplicativo em um Data Integration Service e resolver conflitos de nomes.</li><li>- Iniciar um aplicativo depois da implantação.</li><li>- Localizar um aplicativo.</li><li>- Inicie ou interrompa objetos em um aplicativo.</li><li>- Configurar propriedades do aplicativo.</li></ul>

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio no grupo de privilégio Administração de criação de perfil:

Nome do Privilégio	Permissão Ativada	Descrição
Buscar detalhadamente e exportar resultados	Leitura do projeto A execução na conexão da fonte de dados relacionais também é exigida para fazer uma busca detalhada nos dados ativos	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> <li>- Faça uma busca detalhada nos resultados da criação de perfil.</li> <li>- Exportar os resultados de criação de perfil.</li> </ul>

## Privilégio do Serviço de Ingestão em Massa

O privilégio do Serviço de Ingestão em Massa determina as ações que os usuários podem realizar usando a ferramenta Ingestão em Massa.

A tabela a seguir lista as ações que os usuários podem realizar com o privilégio do Serviço de Ingestão em Massa:

Privilégio	Descrição
Acesso à especificação de Ingestão em Massa	O usuário pode executar as seguintes ações: <ul style="list-style-type: none"> <li>- Procurar todas as especificações de ingestão em massa</li> <li>- Editar uma especificação de ingestão em massa</li> <li>- Executar uma especificação de ingestão em massa</li> <li>- Excluir uma especificação de ingestão em massa</li> </ul>

**Nota:** Um usuário que não tenha recebido o privilégio de acesso para especificação de Ingestão em Massa ou a função Administrador no domínio pode executar essas ações somente nas especificações de ingestão em massa que ele mesmo criar.

## Privilégios do Serviço do Metadata Manager

Os privilégios do Serviço do Metadata Manager determinam as ações que os usuários podem executar usando o Metadata Manager.

A tabela a seguir descreve cada grupo de privilégio do Metadata Manager:

Grupo de Privilégio	Descrição
Catálogo	Inclui privilégios para gerenciar objetos na página Procurar da interface do Metadata Manager.
Carregar	Inclui privilégios para gerenciar objetos na página Carregar da interface do Metadata Manager.
Modelo	Inclui privilégios para gerenciar objetos na página Modelo da interface do Metadata Manager.
Segurança	Inclui privilégios para gerenciar objetos na página Segurança da interface do Metadata Manager.

## Grupo de Privilégio Catálogo

Os privilégios no grupo de privilégio Catálogo determinam as tarefas que os usuários podem executar na guia **Procurar** do aplicativo do Metadata Manager. Um usuário com o privilégio para executar uma determinada ação também requer permissões para executar as ações em um objeto específico. Configure permissões na guia **Segurança** do aplicativo Metadata Manager.

A tabela a seguir lista os privilégios do grupo de privilégio Catálogo e as permissões necessárias para executar uma tarefa em um objeto:

Privilégio	Inclui Privilégios	Permissão	Descrição
Compartilhar Atalhos	n/d	Gravação	O usuário é capaz de compartilhar uma pasta que contém um atalho com outros usuários e grupos.
Exibir Linhagem	n/d	Leitura	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> <li>- Execute análise da linhagem de dados em objetos dos metadados, categorias e termos de negócios.</li> <li>- Execute a análise da linhagem de dados do PowerCenter Designer. Os usuários devem ter também permissão de leitura na pasta de repositório do PowerCenter.</li> </ul>
Exibir Catálogos Relacionados	n/d	Leitura	O usuário é capaz de exibir catálogos relacionados.
Exibir Resultados do Perfil	n/d	Leitura	O usuário é capaz de exibir informações de criação de perfil para objetos de metadados no catálogo de uma origem relacional.
Exibir Catálogo	n/d	Leitura	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> <li>- Exiba recursos e objetos de metadados no catálogo de metadados.</li> <li>- Pesquise o catálogo de metadados.</li> </ul>
Exibir Relacionamentos	n/d	Leitura	O usuário é capaz de exibir relacionamentos para objetos de metadados, categorias e termos comerciais.
Gerenciar Relacionamentos	Exibir Relacionamentos	Gravação	O usuário pode criar, editar e excluir relacionamentos de objetos de metadados personalizados, categorias e termos comerciais.
Exibir Comentários	n/d	Leitura	O usuário é capaz de exibir comentários para objetos de metadados, categorias e termos comerciais.
Publicar Comentários	Exibir Comentários	Gravação	O usuário é capaz de adicionar comentários para objetos de metadados, categorias e termos comerciais.
Excluir Comentários	<ul style="list-style-type: none"> <li>- Publicar Comentários</li> <li>- Exibir Comentários</li> </ul>	Gravação	O usuário é capaz de excluir comentários para objetos de metadados, categorias e termos comerciais.
Exibir Links	n/d	Leitura	O usuário é capaz de exibir links para objetos de metadados, categorias e termos comerciais.
Gerenciar Links	Exibir Links	Gravação	O usuário é capaz de criar, editar e excluir links para objetos de metadados, categorias e termos comerciais.

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Glossário	n/d	Leitura	O usuário pode realizar as seguintes ações: - Exiba glossários comerciais na exibição <b>Glossário</b> . - Pesquise glossários de negócios.
Gerenciar Objetos	n/d	Gravação	O usuário pode realizar as seguintes ações: - Edite objetos de metadados no catálogo. - Crie, edite e exclua objetos de metadados personalizados. Usuários devem ter também o privilégio Exibir Modelo. - Crie, edite e exclua recursos de metadados personalizados. Os usuários devem ter também o privilégio Gerenciar Recursos.

## Carregar grupo de privilégio

Os privilégios no grupo de privilégio Carregar determinam as tarefas que os usuários podem executar na guia **Carregar** do aplicativo Metadata Manager. Um usuário com o privilégio para executar uma determinada ação também requer permissões para executar as ações em um objeto específico. Configure permissões na guia **Segurança** do aplicativo Metadata Manager.

A seguinte tabela lista os privilégios e as permissões necessárias para gerenciar uma instância de um recurso no depósito do Metadata Manager:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Recurso	-	Leitura	O usuário pode realizar as seguintes ações: - Exibir recursos e propriedades dos recursos no depósito do Metadata Manager. - Exportar configurações de recurso. - Baixar o Instalador do Agente do Metadata Manager.
Carregar Recurso	Exibir Recurso	Gravação	O usuário pode realizar as seguintes ações: - Carregar metadados para um recurso no depósito do Metadata Manager.* - Criar links entre objetos nos recursos conectados para linhagem de dados. - Configurar indexação de pesquisa para recursos. - Importar configurações de recursos.
Gerenciar Agendamentos	Exibir Recurso	Gravação	O usuário pode realizar as seguintes ações: - Criar e editar agendamentos. - Adicionar agendamentos aos recursos.
Limpar Metadados	Exibir Recurso	Gravação	O usuário é capaz de remover metadados para um recurso do depósito do Metadata Manager.
Gerenciar Recurso	- Limpar Metadados - Exibir Recurso	Gravação	O usuário é capaz de criar, editar e excluir recursos.
* Para carregar metadados para os recursos do Business Glossary, os privilégios Carregar Recurso, Gerenciar Recurso e Exibir Modelo são necessários.			

## Grupo de privilégio Modelo

Os privilégios no grupo de privilégio Modelo determinam as tarefas que os usuários podem executar na guia **Modelo** do aplicativo Metadata Manager. Não é possível configurar as permissões em um modelo.

A tabela a seguir lista os privilégios necessários para gerenciar modelos:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Modelo	-	-	O usuário é capaz de abrir modelos e classes, e exibir propriedades de classe e modelo. Exiba relacionamentos e atributos de classes.
Gerenciar Modelo	Exibir Modelo	-	O usuário é capaz de criar, editar e excluir modelos personalizados. Adicionar atributos a modelos em pacote e universais.
Exportar/ Importar Modelos	Exibir Modelo	-	O usuário pode importar e exportar modelos personalizados. Importar e exportar modelos em pacote e universais modificados.

## Grupo de privilégio Segurança

Os privilégios no grupo de privilégio Segurança determinam as tarefas que os usuários podem executar na guia **Segurança** do aplicativo Metadata Manager.

Por padrão, o privilégio Gerenciar Permissões do Catálogo no grupo de privilégio Segurança é atribuído ao Administrador ou a um usuário com a função Administrador no Serviço do Metadata Manager. É possível atribuir o privilégio Gerenciar Permissões do Catálogo a outros usuários.

A seguinte tabela lista o privilégio e a permissão necessários para gerenciar a segurança do Metadata Manager:

Privilégio	Inclui Privilégios	Permissão	Descrição
Gerenciar Permissões do Catálogo	-	Controle completo	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"><li>- Atribua aos usuários e grupos permissões de recursos, objetos de metadados, categorias e termos comerciais.</li><li>- Edite permissões de recursos, objetos de metadados, categorias e termos comerciais.</li></ul>

## Privilégios do Serviço de Repositório do Modelo

Os privilégios do Serviço de Repositório do Modelo determinam as ações que os usuários podem executar nos projetos usando o Informatica Analyst e o Informatica Developer.

As permissões de objetos do repositório do Modelo determinam as tarefas que os usuários podem concluir nos objetos em projetos.

A tabela a seguir lista as permissões necessárias e as ações que os usuários podem executar com os privilégios do Serviço de Repositório do Modelo:

Privilégio	Permissão	Descrição
N/D	Leitura do projeto	O usuário pode visualizar projetos e objetos nos projetos.
N/D	Gravar no projeto	O usuário pode criar, editar e excluir objetos nos projetos.
N/D	Concessão no projeto	O usuário pode conceder e revogar permissões nos projetos aos usuários e grupos.
Acesso ao Analyst	N/D	O usuário pode acessar o repositório do Modelo na ferramenta Analyst.
Acesso ao Developer	N/D	O usuário pode acessar o repositório do Modelo na Developer tool.
Criar, Editar e Excluir Projetos	N/D	O usuário pode criar projetos.
Criar, Editar e Excluir Projetos	Gravar em projetos	O usuário pode executar as seguintes ações: <ul style="list-style-type: none"> <li>- Editar projetos.</li> <li>- Excluir projetos, se o usuário os tiver criado.</li> <li>- Atualizar o conteúdo do Serviço de Repositório do Modelo. Para atualizar o serviço no menu <b>Ações</b> ou na linha de comando, o usuário também deve ter o privilégio Gerenciar Serviço do domínio e a permissão no Serviço de Repositório do Modelo. Para atualizar o serviço usando o assistente de atualização de serviço, o usuário também deve ter a função Administrador do domínio.</li> </ul>
Gerenciar Domínios de Dados	N/D	O usuário pode criar, editar e excluir domínios de dados no glossário de domínio de dados. Esse privilégio faz parte do grupo de privilégio de <b>Administração de Domínio de Dados</b> .
Gerenciar Notificações	N/D	O usuário pode configurar notificações de scorecard. Esse privilégio faz parte do grupo de privilégio de <b>Administração de Perfil</b> .
Gerenciar Desenvolvimento Baseado em Equipe	N/D	O usuário pode gerenciar os estados bloqueados ou desbloqueados de objetos do repositório do Modelo. Se o repositório do Modelo estiver integrado com um sistema de controle de versão, o usuário poderá gerenciar os estados de check-out ou check-in dos objetos. O usuário também pode gerenciar a propriedade dos objetos com check-out.
Mostrar Detalhes de Segurança	N/D	O usuário pode visualizar os seguintes detalhes: <ul style="list-style-type: none"> <li>- Nomes de projetos para os quais os usuários não têm permissão de leitura.</li> <li>- Detalhes de mensagens de erro e de aviso.</li> </ul>

## Privilégios do Serviço de Repositório do PowerCenter

Os privilégios do Serviço de repositório do PowerCenter determinam as ações de repositório que os usuários podem executar usando o PowerCenter Repository Manager, Designer, Workflow Manager, Workflow Monitor, e os programas de linha de comando pmrep e pmcmd.



A tabela a seguir descreve cada grupo de privilégio para o Serviço de Repositório do PowerCenter:

Grupo de Privilégio	Descrição
Ferramentas	Inclui privilégios para acessar as ferramentas do Cliente do PowerCenter e programas de linha de comando.
Pastas	Inclui privilégios para gerenciar pastas de repositório.
Objetos de Design	Inclui privilégios para gerenciar os componentes comerciais, variáveis e parâmetros de mapeamento, mapeamentos, mapplets, transformações e funções definidas pelo usuário.
Origens e Destinos	Inclui privilégios para gerenciar cubos, dimensões, definições de origem e definições de destino.
Objetos de Tempo de Execução	Inclui privilégios para gerenciar objetos de configuração de sessão, tarefas, fluxos de trabalho e worklets.
Objetos Globais	Inclui privilégios para gerenciar objetos de conexão, grupos de implantação, rótulos e consultas.

Os usuários devem ter a permissão e o privilégio de domínio Gerenciar Serviços no Serviço de Repositório do PowerCenter para executar as ações a seguir no Repository Manager.

- Executar uma limpeza avançada de versões de objeto no nível de repositório do PowerCenter.
- Criar, editar e excluir extensões de metadados reutilizáveis.

## Grupo de privilégio Ferramentas

Os privilégios no grupo de privilégio Ferramentas do Serviço do Repositório do PowerCenter determinam as ferramentas do Cliente do PowerCenter e os programas de linha de comando que os usuários podem acessar.

A tabela a seguir lista as ações que os usuários podem executar para os privilégios no grupo Ferramentas:

Privilégio	Permissão	Descrição
Acessar o Designer	-	O usuário está conectado ao repositório do PowerCenter usando o Designer.
Acessar o Repository Manager	-	O usuário é capaz de executar as seguintes ações: - Conecte-se ao repositório do PowerCenter usando o Repository Manager. - Execute os comandos <i>pmrep</i> .
Acessar o Workflow Manager	-	O usuário é capaz de executar as seguintes ações: - Conecte-se ao repositório do PowerCenter usando o Workflow Manager. - Remova um Serviço de Integração do PowerCenter do Workflow Manager.
Acessar o Workflow Monitor	-	O usuário é capaz de executar as seguintes ações: - Conecte-se ao repositório do PowerCenter usando o Workflow Monitor. - Conecte-se ao Serviço de Integração do PowerCenter no Workflow Monitor.

**Nota:** Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço do Repositório do PowerCenter associado.

O privilégio apropriado no grupo de privilégio Ferramentas é necessário para todos os usuários concluírem as tarefas nas ferramentas do Cliente do PowerCenter e programas da linha de comando. Por exemplo, para criar pastas no Repository Manager, um usuário deve ter os privilégios Criar Pastas e Acessar Repository Manager.

Se os usuários tiverem um privilégio no grupo de privilégio Ferramentas e permissão sobre um objeto de repositório do PowerCenter, mas não o privilégio para modificar o tipo de objeto, eles poderão executar algumas ações no objeto. Por exemplo, um usuário possui o privilégio Acessar Repository Manager e a permissão de leitura em algumas pastas. O usuário não possui nenhum dos privilégios no grupo de privilégio Pastas. O usuário pode exibir objetos nas pastas e compará-las.

## Grupo de Privilégio Pastas

As tarefas de gerenciamento de pasta são determinadas pelos privilégios no grupo de privilégio Pastas, nas permissões de objeto de repositório do PowerCenter e nas permissões de objeto de domínio. Os usuários executam tarefas de gerenciamento de pasta no Repository Manager e com o programa de linha de comando pmrep.

Algumas tarefas de gerenciamento de pasta são determinadas pela propriedade da pasta e pela função Administrador, não por privilégios ou permissões. O proprietário da pasta ou um usuário que tenha a função Administrador no Serviço de Repositório do PowerCenter pode executar as seguintes tarefas de gerenciamento de pasta:

- Atribua perfis do sistema operacional às pastas se o Serviço de Integração do PowerCenter usar perfis do sistema operacional. Requer permissão no perfil do sistema operacional.
- Altere o proprietário da pasta.
- Configure permissões de pasta.
- Exclua a pasta.
- Designe a pasta a ser compartilhada.
- Edite o nome e a descrição da pasta.

Usuários com permissões de pasta, mas nenhum Privilégio pode executar algumas ações de gerenciamento de pasta. A tabela a seguir lista as ações que usuários podem executar quando eles tem atribuídos somente permissões de pasta:

Permissão	Descrição
Ler na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Compare pastas.</li><li>- Veja objetos em pastas.</li></ul>

**Nota:** Para executar ações em pastas, os usuários também devem ter o privilégio Acessar Repository Manager.

## Privilégio Criar Pastas

Os usuários atribuídos ao privilégio Criar Pastas pode criar pastas de repositório do PowerCenter.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Criar pastas:

Permissão	Descrição
-	O usuário é capaz de criar pastas.

## Copie as pastas privilégio

Os usuários atribuídos ao copiar pastas privilégio podem copiar pastas dentro de um repositório ou para outro repositório do PowerCenter.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Cópia pastas:

Permissão	Descrição
Ler na pasta	O usuário é capaz de copiar pastas dentro do mesmo repositório do PowerCenter ou para outro repositório do PowerCenter. Os usuários também devem ter o privilégio Criar Pastas no repositório de destino.

## Gerenciar Versões de pasta

Se você tem uma opção de desenvolvimento baseado em equipe, atribua aos usuários o privilégio Gerenciar Versões de pasta em um repositório do PowerCenter com versões. Os usuários podem alterar o status das pastas e execute uma limpeza avançada das versões de objeto no nível da pasta.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar Versões de pasta:

Permissão	Descrição
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Altere o status das pastas.</li><li>- Execute uma limpeza avançada das versões de objeto no nível da pasta.</li></ul>

## Grupo de privilégio Objetos de design

Os privilégios no grupo de privilégio Objetos de Design e as permissões do objeto de repositório do PowerCenter determinam as tarefas que os usuários podem concluir nos seguintes objetos de design:

- Componentes comerciais
- Parâmetros e variáveis de mapeamento
- Mapeamentos
- Maplets
- Transformações
- Funções definidas pelo usuário

Permissões de usuários atribuídos, mas sem privilégios pode executar algumas ações para objetos de design. A tabela a seguir lista as ações que usuários podem executar quando eles tem somente permissões atribuídas:

Permissão	Descrição
Ler na pasta	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Comparar os objetos de design.</li> <li>- Copiar os objetos de design como uma imagem.</li> <li>- Exportar os objetos de design.</li> <li>- Gerar código para transformação Personalizada e procedimentos externos.</li> <li>- Receber mensagens de notificação do repositório do PowerCenter.</li> <li>- Executar linhagem de dados nos objetos de design. Os usuários também devem ter o privilégio de Exibição de Linhagem para o Serviço do Metadata Manager e permissão de leitura nos objetos de metadados no catálogo do Metadata Manager.</li> <li>- Pesquisar objetos de design.</li> <li>- Exibir objetos de design, dependências de objeto de design e histórico de objeto de design.</li> </ul>
Leitura em pasta compartilhada Ler e Gravar na pasta de destino	O usuário é capaz de criar atalhos.

**Nota:** Para executar ações nos objetos de design, os usuários também devem ter privilégio apropriado no grupo de privilégio Ferramentas.

## Criar, Editar e Excluir Privilégio de Objetos de Design

Os usuários atribuídos ao criar, editar e excluir Privilégio de objetos de design pode criar, editar e excluir componentes comerciais, parâmetros de mapeamento, as variáveis de mapeamento, mapeamentos, mapplets, transformações e funções definidas pelo usuário.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com criar, editar e excluir Privilégio de objetos de design:

Permissão	Descrição
Ler na pasta original Ler e Gravar na pasta de destino	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Copiar objetos de design de uma pasta para outra.</li><li>- Copiar objetos de design para outro repositório do PowerCenter. Os usuários também devem ter privilégios para Criar, Editar e Excluir Objetos de Design no repositório de destino.</li></ul>
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Alterar comentários de um objeto de design com versão.</li><li>- Fazer check-in e desfazer um check-out de objetos de design cujo check-out tenha sido feito pela própria conta do usuário.</li><li>- Fazer check-out de objetos de design.</li><li>- Copiar e colar objetos de design na mesma pasta.</li><li>- Criar, editar e excluir perfis de dados e iniciar o Profile Manager. Os usuários também devem ter privilégios para Criar, Editar e Excluir Objetos em Tempo de Execução.</li><li>- Criar, editar e excluir objetos de design.</li><li>- Gerar e limpar programas SAP ABAP.</li><li>- Gerar mapeamentos de integração do conteúdo comercial. Os usuários também devem ter privilégios para Criar, Editar e Excluir Origens e Destinos.</li><li>- Importar objetos de design usando o Designer. Os usuários também devem ter privilégios para Criar, Editar e Excluir Origens e Destinos.</li><li>- Importar objetos de design usando o Repository Manager. Os usuários também devem ter privilégios para Criar, Editar e Excluir Objetos em Tempo de Execução e Criar, Editar e Excluir Origens e Destinos.</li><li>- Reverter para uma versão de objeto de design anterior.</li><li>- Validar funções de mapeamentos, mapplets e definidas pelo usuário.</li></ul>

## Gerenciar Versões do Objeto de Design

Se você tem uma opção de desenvolvimento baseado em equipe, atribua aos usuários o privilégio Gerenciar versões de objeto de design em um repositório do PowerCenter com versões. Os usuários podem alterar o status, recuperar e limpar versões de objeto de design. Os usuários também pode fazer check-in e desfazer check-outs feitos por outros usuários.

Gerenciar Versões de objeto de design inclui o privilégio Criar, editar e excluir objetos de design privilégio.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar versões de objeto de design:

Permissão	Descrição
Ler e Gravar na pasta	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Alterar o status dos objetos de design.</li> <li>- Fazer check-in e desfazer check-outs de objetos de design cujo check-out foi feito por outros usuários.</li> <li>- Limpar versões de objetos de design.</li> <li>- Recuperar objetos de design excluídos.</li> </ul>

## Grupo de privilégio Origens e destinos

Os privilégios no grupo de privilégio Origens e Destinos e as permissões do objeto de repositório do PowerCenter determinam as tarefas que os usuários podem concluir nos seguintes objetos de origem e destino:

- Cubos
- Dimensões
- Definições de origem
- Definições de destino

Permissões de usuários atribuídos, mas sem privilégios podem executar algumas ações para objetos de origem e destino. A tabela a seguir lista as ações que usuários podem executar quando eles tem atribuídos somente permissões:

Permissão	Descrição
Ler na pasta	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Compare os objetos de origem e destino.</li> <li>- Exporte os objetos de origem e destino.</li> <li>- Visualize os dados de origem e destino.</li> <li>- Receber mensagens de notificação do repositório do PowerCenter.</li> <li>- Execute a linhagem de dados nos objetos de origem e destino. Os usuários também devem ter o privilégio de Exibição de Linhagem para o Serviço do Metadata Manager e permissão de leitura nos objetos de metadados no catálogo do Metadata Manager.</li> <li>- Procure os objetos de origem e destino.</li> <li>- Exiba os objetos de origem e destino, dependências de objeto de origem e destino e histórico de objeto de origem e destino.</li> </ul>
Leitura em pasta compartilhada Ler e Gravar na pasta de destino	Criar atalhos.

**Nota:** Para executar ações nos objetos de origem e destino, os usuários também devem ter privilégio apropriado no grupo de privilégio Ferramentas.

## Criar, Editar e Excluir Privilégio de Origens e Destinos

Os usuários atribuídos ao Criar, Editar e Excluir privilégio de Origens e destinos pode criar, editar e excluir cubos, dimensões, definições de origem e definições de destino.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com Criar, Editar e Excluir privilégio de Origens e destinos:

Permissão	Descrição
Ler na pasta original Ler e Gravar na pasta de destino	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Copiar os objetos de origem e destino para outra pasta.</li><li>- Copiar os objetos de origem e destino para outro repositório do PowerCenter. Os usuários também devem ter privilégios para Criar, Editar e Excluir Objetos de Origens e Destinos no repositório de destino.</li></ul>
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Alterar comentários de um objeto de origem ou destino com versão.</li><li>- Fazer check-in e desfazer um check-out de objetos de origem e destino cujo check-out tenha sido feito pela própria conta do usuário.</li><li>- Fazer check-out dos objetos de origem e destino.</li><li>- Copiar e colar objetos de origem e destino na mesma pasta.</li><li>- Criar, editar e excluir objetos de origem e destino.</li><li>- Importar funções SAP.</li><li>- Importar objetos de origem e destino usando o Designer. Os usuários também devem ter o privilégio Criar, Editar e Excluir Objetos de Design.</li><li>- Importar objetos de origem e destino usando o Repository Manager. Os usuários também devem ter privilégios para Criar, Editar e Excluir Objetos de Design e Criar, Editar e Excluir Objetos de Tempo de Execução.</li><li>- Gerar e executar SQL para criar destinos em um banco de dados relacional.</li><li>- Reverter para uma versão de objeto de origem ou destino anterior.</li></ul>

## Privilégio Gerenciar Versões de Origem e Destino

Se você tem uma opção de desenvolvimento baseado em equipe, atribua aos usuários o privilégio Gerenciar Versões de origem e destino em um repositório do PowerCenter com versões. Os usuários podem alterar o status, recuperar e limpar versões de objetos de origem e destino. Os usuários também pode fazer check-in e desfazer check-outs feitos por outros usuários.

Privilégio Gerenciar Versões de origem e destino inclui Criar, Editar e Excluir privilégio de Origens e destinos.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar Versões de origem e destino:

Permissão	Descrição
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Alterar o status de objetos de origem e destino.</li><li>- Fazer check-in e desfazer check-outs de objetos de origem e destino cujo check-out foi feito por outros usuários.</li><li>- Limpar versões de objetos de origem e destino.</li><li>- Recuperar objetos de origem e destino excluídos.</li></ul>

## Grupo de privilégio de Objetos em Tempo de Execução

Os privilégios no grupo de privilégio de Objetos em Tempo de Execução, as permissões de objeto de repositório do PowerCenter e as permissões de objeto de domínio determinam as tarefas que os usuários podem executar nos seguintes objetos em tempo de execução:

- Objetos de configuração de sessão
- Tarefas
- Fluxos de Trabalho
- Worklets

Algumas tarefas de objeto de tempo de execução são determinadas pela função Administrador, não por privilégios nem por permissões. Um usuário atribuído à função Administrador para o Serviço de Repositório do PowerCenter pode excluir um Serviço de Integração do PowerCenter no Navegador do Workflow Manager.

Permissões de usuários atribuídos, mas sem privilégios pode executar algumas ações para objetos em tempo de execução. A tabela a seguir lista as ações que usuários podem executar quando eles tem atribuídos somente permissões:

Permissão	Descrição
Ler na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Comparar objetos em tempo de execução.</li><li>- Exportar objetos em tempo de execução.</li><li>- Receber mensagens de notificação do repositório do PowerCenter.</li><li>- Procurar objetos em tempo de execução.</li><li>- Usar parâmetros e variáveis de mapeamento em uma sessão.</li><li>- Exibir objetos em tempo de execução, dependências de objetos em tempo de execução e o histórico do objeto em tempo de execução.</li></ul>
Ler e Executar na pasta	Interromper e anular tarefas e fluxos de trabalho iniciados pela própria conta de usuário deles. Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.

**Nota:** Para executar ações em objetos em tempo de execução, os usuários também devem ter o privilégio apropriado no grupo de privilégio Ferramentas.



## Criar, Editar e Excluir Privilégio de Objetos de Tempo de Execução

Os usuários atribuídos ao criar, editar e excluir privilégio de objetos em tempo de execução privilégio pode criar, editar e excluir objetos de configuração de sessão, tarefas, fluxos de trabalho e worklets.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com criar, editar e excluir privilégio de objetos em tempo de execução:

Permissão	Descrição
Ler na pasta original Ler e Gravar na pasta de destino	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Copiar tarefas, fluxos de trabalho ou worklets de uma pasta para outra.</li><li>- Copiar tarefas, fluxos de trabalho ou worklets em outro repositório do PowerCenter. Os usuários também devem ter o privilégio Criar, Editar e Excluir Objetos em Tempo de Execução no repositório de destino.</li></ul>
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Atribuir um Serviço de Integração do PowerCenter a um fluxo de trabalho nas propriedades do fluxo de trabalho.</li><li>- Atribuir um nível de serviço a um fluxo de trabalho.</li><li>- Alterar os comentários de um objeto em tempo de execução com versão.</li><li>- Fazer check-in e desfazer um check-out de objetos em tempo de execução com check-out feito pela própria conta de usuário deles.</li><li>- Fazer check-out de objetos em tempo de execução.</li><li>- Copiar e colar tarefas, fluxos de trabalho e worklets na mesma pasta.</li><li>- Criar, editar e excluir perfis de dados e iniciar o Profile Manager. Os usuários também devem ter o privilégio Criar, Editar e Excluir Objetos de Design.</li><li>- Criar, editar e excluir objetos de configuração de sessão.</li><li>- Excluir e validar tarefas, fluxos de trabalho e worklets.</li><li>- Importar objetos em tempo de execução usando o Repository Manager. Os usuários também devem ter os privilégios Criar, Editar e Excluir Objetos de Design e Criar, Editar e Excluir Origens e Destinos.</li><li>- Importar objetos em tempo de execução usando o Workflow Manager.</li><li>- Reverter para uma versão do objeto anterior.</li></ul>
Ler e Gravar na pasta Ler no objeto de conexão	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"><li>- Criar e editar tarefas, fluxos de trabalho e worklets.</li><li>- Substituir uma conexão de banco de dados relacional por todas as sessões que usam a conexão.</li></ul>

## Privilégio Gerenciar Versões de objeto de tempo de execução

Se você tem uma opção de desenvolvimento baseado em equipe, atribua aos usuários o privilégio Gerenciar versões de objeto de tempo de execução em um repositório do PowerCenter com versões. Os usuários podem alterar o status, recuperar e limpar versões de objeto em tempo de execução. Os usuários também pode fazer check-in e desfazer check-outs feitos por outros usuários.

Privilégio Gerenciar Versões de objeto de tempo de execução inclui o privilégio Criar, Editar e Excluir privilégio de Objetos em tempo de execução.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar versões de objeto em tempo de execução:

Permissão	Descrição
Ler e Gravar na pasta	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Alterar o status de objetos em tempo de execução.</li> <li>- Fazer check-in e desfazer os check-outs de objetos em tempo de execução com check-out de outros usuários.</li> <li>- Limpar versões de objetos em tempo de execução.</li> <li>- Recuperar objetos em tempo de execução excluídos.</li> </ul>

## Privilégio Monitorar Objetos em tempo de execução

Os usuários atribuídos ao privilégio Monitorar Objetos de tempo de execução poderá monitorar fluxos de trabalho e tarefas no Workflow Monitor.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Monitorar Objetos de tempo de execução:

Permissão	Concede aos Usuários a Capacidade de
Ler na pasta	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Exibir as propriedades de objetos em tempo de execução no Workflow Monitor.*</li> <li>- Exibir os logs de sessão e fluxo de trabalho no Workflow Monitor.*</li> <li>- Exibir detalhes de objeto em tempo de execução e desempenho no Workflow Monitor.*</li> </ul> <p>Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.</p>

## Privilégio Executar de Objetos em tempo de execução

Os usuários atribuídos a execução de objetos em tempo de execução privilégio pode iniciar, inicialize a frio e recupere tarefas e fluxos de trabalho.

A execução de objetos em tempo de execução inclui o privilégio Monitorar Objetos de tempo de execução privilégio.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio executar Objetos em tempo de execução:

Permissão	Descrição
Ler e Executar na pasta	O usuário é capaz de atribuir um Serviço de Integração do PowerCenter para um fluxo de trabalho usando o menu Serviço ou Navegador.
Ler, Gravar e Executar na pasta Ler e Executar no objeto de conexão	<p>O usuário é capaz de depurar um mapeamento criando uma instância de sessão de depuração ou usando uma sessão reutilizável existente. Os usuários também devem ter privilégios para Criar, Editar e Excluir Objetos em Tempo de Execução.</p> <p>Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.</p>

Permissão	Descrição
Ler e Executar na pasta Ler e Executar no objeto de conexão	O usuário é capaz de depurar um mapeamento usando uma sessão não reutilizável existente. Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.
Ler e Executar na pasta Ler e Executar no objeto de conexão	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"> <li>- Iniciar, inicializar a frio e reiniciar tarefas e fluxos de trabalho.</li> <li>- Recuperar tarefas e fluxos de trabalho iniciados pela própria conta de usuário deles.</li> </ul> Se o Serviço de Integração do PowerCenter usar perfis de sistema operacional, os usuários devem ter permissão sobre o perfil do sistema operacional. Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.

## Privilegio Gerenciar Execução de objeto de tempo de execução

Os usuários atribuídos ao privilégio Gerenciar Execução de objeto de tempo de execução pode agendar e cancelar o agendamento de fluxos de trabalho. Os usuários também pode interromper, abortar e recupere tarefas e fluxos de trabalho iniciado por outros usuários.

Privilegio Gerenciar Execução de objeto de tempo de execução inclui o privilégio Executar objetos de tempo de execução e o privilégio Monitorar Objetos de tempo de execução.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar Execução de objeto de tempo de execução:

Permissão	Descrição
Ler e Executar na pasta	O usuário é capaz de truncar entradas de log de sessão e fluxo de trabalho.
Ler e Executar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"> <li>- Interromper e anular tarefas e fluxos de trabalho iniciados por outros usuários.</li> <li>- Interromper e anular tarefas que foram recuperadas automaticamente.</li> <li>- Cancelar agendamento de fluxos de trabalho.</li> </ul> Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.

Permissão	Descrição
Ler e Executar na pasta Ler e Executar no objeto de conexão	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Recuperar tarefas e fluxos de trabalho iniciados por outros usuários.</li> <li>- Recuperar tarefas que foram recuperadas automaticamente.</li> </ul> <p>Se o Serviço de Integração do PowerCenter usar perfis de sistema operacional, os usuários devem ter permissão sobre o perfil do sistema operacional.</p> <p>Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.</p>
Ler, Gravar e Executar na pasta Ler e Executar no objeto de conexão	<p>O usuário é capaz de executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>- Criar e editar um agendador reutilizável a partir do menu Fluxos de Trabalho &gt; Agendadores.</li> <li>- Editar um agendador não reutilizável a partir das propriedades do fluxo de trabalho.</li> <li>- Editar um agendador reutilizável a partir das propriedades de fluxo de trabalho. Os usuários também devem ter privilégios para Criar, Editar e Excluir Objetos em Tempo de Execução.</li> </ul> <p>Se o Serviço de Integração do PowerCenter usar perfis de sistema operacional, os usuários devem ter permissão sobre o perfil do sistema operacional.</p> <p>Quando o Serviço de Integração do PowerCenter for executado no modo de segurança, os usuários deverão ter a função Administrador para o Serviço de Repositório do PowerCenter associado.</p>

## Grupo de privilégio de objetos globais

Os privilégios no grupo de privilégio de Objetos Globais e as permissões de objeto de repositório do PowerCenter determinam as tarefas que os usuários podem concluir nos objetos globais a seguir:

- Objetos de conexão
- Grupos de implantação
- Rótulos
- Consultas

Algumas tarefas de objeto global são determinadas pela propriedade do objeto global e pela função Administrador, e não por privilégios ou permissões. O proprietário do objeto global ou um usuário que recebeu a função Administrador para o Serviço de Repositório do PowerCenter pode concluir as seguintes tarefas de objeto global:

- Configurar permissões de objeto global.
- Alterar o proprietário do objeto global.
- Excluir o objeto global.

Permissões de usuários atribuídos, mas sem privilégios podem executar algumas ações para objetos globais. A tabela a seguir lista as ações que usuários podem executar quando eles tem somente permissões atribuídas:

Permissão	Descrição
Ler no objeto de conexão	O usuário é capaz de exibir objetos de conexão.
Ler no grupo de implantação	O usuário é capaz de exibir grupos de implantação.

Permissão	Descrição
Ler no rótulo	O usuário é capaz de exibir rótulos.
Ler na consulta	O usuário é capaz de exibir consultas de objeto.
Ler e gravar no objeto de conexão	O usuário é capaz de editar objetos de conexão.
Ler e gravar no rótulo	O usuário é capaz de editar e bloquear rótulos.
Ler e gravar na consulta	O usuário é capaz de editar e validar consultas de objeto.
Ler e executar na consulta	O usuário é capaz de executar consultas de objeto.
Ler na pasta Ler e executar no rótulo	O usuário é capaz de aplicar rótulos e remover referências de rótulo.

**Nota:** Para executar ações nos objetos globais, os usuários também devem ter o privilégio adequado no grupo de privilégio Ferramentas.

## Criar Conexões privilégio

Os usuários atribuídos ao privilégio Criar conexões pode criar objetos de conexão.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Criar conexões:

Permissão	Descrição
-	O usuário é capaz de criar e copiar objetos de conexão.

## Privilégio Gerenciar Grupos de Implantação

Se você tem uma opção de desenvolvimento baseado em equipe, os usuários com atribuição do privilégio Gerenciar grupos de implantação em um repositório do PowerCenter pode criar, editar, copiar e reverter grupos de implantação. Em um repositório sem versão, os usuários podem criar, editar e copiar grupos de implantação.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Gerenciar grupos de implantação:

Permissão	Descrição
-	O usuário é capaz de criar grupos de implantação.
Ler e gravar no grupo de implantação	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"> <li>- Editar grupos de implantação.</li> <li>- Remover objetos de um grupo de implantação.</li> </ul>
Ler na pasta original Ler e gravar no grupo de implantação	O usuário é capaz de adicionar objetos a um grupo de implantação.

Permissão	Descrição
Ler na pasta original Ler e Gravar na pasta de destino Ler e executar no grupo de implantação	O usuário é capaz de copiar grupos de implantação.
Ler e Gravar na pasta de destino	O usuário é capaz de reverter grupos de implantação.

## Privilégio Executar Grupos de Implantação

Os usuários atribuídos ao privilégio Executar Grupos de Implantação podem copiar um grupo de implantação sem permissão de gravação nas pastas de destino.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Executar Grupos de implantação:

Permissão	Descrição
Ler na pasta original Executar no grupo de implantação	O usuário é capaz de copiar grupos de implantação.

## Privilégio Criar rótulos

Se você tiver uma opção de desenvolvimento baseado em equipe, os usuários que receberam o privilégio Criar rótulos em um repositório do PowerCenter vcom versão pode criar rótulos.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Criar rótulos:

Permissão	Descrição
-	O usuário é capaz de criar rótulos.

## Privilégio Criar consultas

Os usuários atribuídos ao privilégio criar consultas pode criar consultas de objeto.

A tabela a seguir lista as permissões necessárias e as ações que usuários podem executar com o privilégio Criar consultas:

Permissão	Descrição
-	O usuário é capaz de criar consultas de objeto.

# Privilégios do Serviço do Ouvinte do PowerExchange

Os privilégios do Serviço do Ouvinte do PowerExchange determinam os comandos `infacmd pwx` que os usuários podem executar.

A tabela a seguir descreve o privilégio de Serviço do Ouvinte do PowerExchange no grupo de privilégio comandos de informações:

Nome do Privilégio	Descrição
listtask	Execute o comando <code>infacmd pwx ListTaskListener</code> .

A tabela a seguir descreve cada privilégio do Serviço do Ouvinte do PowerExchange no grupo de privilégio de gerenciamento de comandos:

Nome do Privilégio	Descrição
fechar	Execute o comando <code>infacmd pwx CloseListener</code> .
closeforce	Execute o comando <code>infacmd pwx CloseForceListener</code> .
stoptask	Execute o comando <code>infacmd pwx StopTaskListener</code> .

# Privilégios do Serviço do Agente de Log do PowerExchange

Os privilégios do Serviço do Agente de Log do PowerExchange determinam os comandos `infacmd pwx` que os usuários podem executar.

A tabela a seguir descreve cada privilégio de Serviço do Agente de Log do PowerExchange no grupo de privilégio comandos de informações:

Nome do Privilégio	Descrição
displayall	Execute o comando <code>infacmd pwx DisplayAllLogger</code> .
displaycpu	Execute o comando <code>infacmd pwx DisplayCPULogger</code> .
displaycheckpoints	Execute o comando <code>infacmd pwx DisplayCheckpointsLogger</code> .
displayevents	Execute o comando <code>infacmd pwx DisplayEventsLogger</code> .
displaymemory	Execute o comando <code>infacmd pwx DisplayMemoryLogger</code> .
displayrecords	Execute o comando <code>infacmd pwx DisplayRecordsLogger</code> .
displaystatus	Execute o comando <code>infacmd pwx DisplayStatusLogger</code> .

A tabela a seguir descreve cada privilégio de Serviço do Agente de Log do PowerExchange no grupo de privilégio comandos de gerenciamento:

Nome do Privilégio	Descrição
condense	Execute o comando <code>infacmd pwx CondenseLogger</code> .
fileswitch	Execute o comando <code>infacmd pwx FileSwitchLogger</code> .
shutdown	Execute o comando <code>infacmd pwx ShutDownLogger</code> .

## Privilégios do Serviço de Agendador

Privilégios do Serviço de Agendador determinam as ações que os usuários podem realizar em agendamentos e trabalhos agendados.

A seguinte tabela descreve os privilégios e as permissões necessárias do Serviço de Agendador:

Privilégio	Descrição	Requer permissão em
Criar Agendamento	O usuário pode criar agendamentos. Para criar um agendamento, o usuário também deve ter o privilégio Administração de Aplicativos no Serviço de Integração de Dados.	<ul style="list-style-type: none"> <li>- Serviço de Agendador</li> <li>- O Serviço de Integração de Dados que executa os trabalhos que o usuário deseja agendar</li> </ul>
Editar Agendamento	O usuário pode editar, pausar e retomar agendamentos. Para editar um agendamento, o usuário também deve ter o privilégio Administração de Aplicativos no Serviço de Integração de Dados.	<ul style="list-style-type: none"> <li>- Serviço de Agendador</li> <li>- O Serviço de Integração de Dados que executa os trabalhos que o usuário deseja agendar</li> </ul>
Excluir Agendamento	O usuário pode excluir agendamentos.	Serviço de Agendador
Exibir Agendamentos	O usuário pode visualizar a exibição <b>Agendamentos</b> e os agendamentos.	Serviço de Agendador



# Privilégios do Serviço do Test Data Manager

Os privilégios do Serviço do Test Data Manager determinam as ações que os usuários podem realizar usando o Test Data Manager. Configure os privilégios na guia **Segurança** da ferramenta Administrator.

A tabela a seguir descreve cada grupo de privilégio do Test Data Manager:

Grupo de Privilégios	Descrição
Administração	Inclui privilégios para criar e gerenciar conexões, códigos de acesso, funções e atribuir privilégios a usuários e grupos de usuários do Informatica Administrator, gerenciar repositórios, adicionar licenças e configurar atributos de fluxo de trabalho e de projeto. <b>Nota:</b> Antes que você crie usuários e grupos, o usuário administrador padrão do Informatica deve atribuir privilégios de Administração de Segurança ao usuário Administrador de Dados de Teste.
Domínios de Dados	Inclui privilégios para exibir e gerenciar domínios de dados no Test Data Manager.
Mascaramento de Dados	Inclui privilégios para exibir e gerenciar regras de mascaramento e atribuições de diretivas no Test Data Manager.
Diretivas	Inclui privilégios para exibir e gerenciar diretivas no Test Data Manager.
Projetos	Inclui privilégios para exibir e gerenciar projetos, auditar e importar metadados e executar planos e fluxos de trabalho no Test Data Manager.

## Grupo de Privilégios Administração

Os privilégios no grupo de privilégios Administração determinam as tarefas de administração que os Administradores de Test Data podem executar.

A seguinte tabela lista os privilégios do grupo de privilégios Administração e as permissões necessárias para executar uma tarefa em um objeto:

## Grupo de Privilégio Conexões

Os privilégios do grupo de privilégio Conexões determinam as tarefas que os usuários podem executar na página Conexões do TDM Workbench. A tabela a seguir lista os privilégios do grupo de privilégio Conexões e as permissões necessárias para executar uma tarefa em um objeto:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Conexões	-	Ler	O usuário pode exibir e testar conexões no TDM Workbench.
Gerenciar Conexões	Exibir Conexões	Gravar	O usuário pode executar as seguintes ações na página Conexões do TDM Workbench: <ul style="list-style-type: none"><li>- Criar conexões.</li><li>- Editar conexões.</li><li>- Excluir conexões.</li><li>- Exibir conexões.</li><li>- Testar conexões.</li></ul>

## Grupo de Privilégio Domínios de Dados

Os privilégios no grupo de privilégio Domínios de Dados determinam as tarefas que os usuários podem realizar em domínios de dados na página Diretivas do Test Data Manager.

A seguinte tabela lista os privilégios do grupo de privilégio Domínios de Dados e as permissões necessárias para executar uma tarefa em um objeto:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Domínios de Dados	-	Ler	O usuário pode exibir domínios de dados no Test Data Manager.
Gerenciar Domínios de Dados	Exibir Domínios de Dados	Gravar	O usuário pode realizar as seguintes ações em domínios de dados no Test Data Manager: <ul style="list-style-type: none"><li>- Criar domínios de dados.</li><li>- Editar domínios de dados.</li><li>- Excluir domínios de dados.</li><li>- Exibir domínios de dados.</li></ul>

## Grupo de Privilégio Mascaramento de Dados

Os privilégios no grupo de privilégio Mascaramento de Dados determinam as tarefas que os usuários podem realizar na exibição Projeto | Definir | Mascaramento de Dados do Test Data Manager. Você pode atribuir regras e diretivas às colunas de tabela por meio dessa exibição.

A seguinte tabela lista os privilégios do grupo de privilégio Mascaramento de Dados e as permissões necessárias para executar uma tarefa em um objeto:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Mascaramento de Dados	-	Ler	O usuário pode exibir atribuições de mascaramento de dados no Test Data Manager.
Gerenciar Mascaramento de Dados	Exibir Mascaramento de Dados	Gravar	O usuário pode realizar as seguintes ações de atribuição de mascaramento de dados no Test Data Manager: <ul style="list-style-type: none"><li>- Adicionar atribuições de regra e diretiva.</li><li>- Excluir atribuições de regra e diretiva.</li><li>- Substituir as propriedades de regra.</li><li>- Exibir atribuições de mascaramento de dados.</li></ul>

## Grupo de Privilégios Subconjunto de Dados

Os privilégios no grupo de privilégio Subconjunto de Dados determinam as tarefas que os usuários podem realizar em objetos de subconjunto de dados no Test Data Manager.

A seguinte tabela lista os privilégios do grupo de privilégio Subconjunto de Dados e as permissões necessárias para executar uma tarefa em um objeto:

## Grupo de Privilégio Diretivas

Os privilégios no grupo de privilégio Diretivas determinam as tarefas que os usuários podem realizar em Diretivas no Test Data Manager.

A seguinte tabela lista os privilégios do grupo de privilégio Diretivas e as permissões necessárias para executar uma tarefa em um objeto:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Diretivas	-	Ler	O usuário pode exibir diretivas no Test Data Manager.
Gerenciar Diretivas	Exibir Diretivas	Gravar	O usuário pode realizar as seguintes ações em diretivas no Test Data Manager: <ul style="list-style-type: none"><li>- Criar diretivas.</li><li>- Editar diretivas.</li><li>- Excluir diretivas.</li><li>- Exibir diretivas.</li></ul>

## Grupo de Privilégios Projetos

Os privilégios no grupo de privilégios Projetos determinam as tarefas que os usuários podem realizar em Projetos no Test Data Manager.

A seguinte tabela lista os privilégios do grupo de privilégios Projetos e as permissões necessárias para executar uma tarefa em um objeto:

**Nota:** Um usuário com o privilégio Gerenciar Projeto deve ter pelo menos os níveis de privilégios a seguir para poder criar um plano com cada componente.

- Exibir conexão do grupo de privilégios Administração. Para criar um plano.
- Exibir um subconjunto de dados do grupo de privilégios Subconjunto de Dados. Para criar um plano com os componentes de subconjunto.
- Exibir regras de mascaramento do grupo de privilégios Regras. Para criar um plano com componentes de mascaramento.

## Grupo de Privilégios Regras

A seguinte tabela lista os privilégios do grupo de privilégio Mascaramento de Dados e as permissões necessárias para executar uma tarefa em um objeto:

## Grupo de Privilégio Geração de Dados

Os privilégios no grupo de privilégio Geração de Dados determinam as tarefas de geração de dados de teste que os usuários podem realizar no Test Data Manager.

A tabela a seguir lista os privilégios do grupo de privilégio Geração de Dados e as permissões necessárias para executar uma tarefa em um objeto:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Geração de Dados	-	Ler	O usuário pode exibir atribuições de regras de geração de dados no Test Data Manager.
Gerenciar Geração de Dados	Exibir Geração de Dados	Gravar	O usuário pode realizar as seguintes ações de geração de dados no Test Data Manager: <ul style="list-style-type: none"><li>- Exibir atribuições de regra de geração de dados.</li><li>- Adicionar atribuições de regra de geração de dados.</li><li>- Excluir atribuições de regra de geração de dados.</li><li>- Substituir atribuições de regra de geração de dados.</li></ul>

## Gerenciando Funções

Uma função é uma coleção de privilégios que você pode atribuir aos usuários e grupos. Você pode atribuir os seguintes tipos de funções:

- Definidas pelo sistema. Funções que não podem ser editadas nem excluídas.
- Personalizar. Funções que é possível criar, editar ou excluir.

Uma função inclui privilégios para o domínio ou um tipo de serviço de aplicativo. Você atribui funções a usuários ou grupos ao domínio ou a cada serviço de aplicativo no domínio. Por exemplo, é possível criar uma função Desenvolvedor que inclua privilégios para o Serviço do Repositório do PowerCenter. Um domínio pode conter vários Serviços de Repositório do PowerCenter. Você pode atribuir a função Desenvolvedor a um usuário do Serviço do Repositório do PowerCenter de Desenvolvimento. Você pode atribuir uma função diferente a esse usuário no Serviço do Repositório do PowerCenter de Produção.

Quando seleciona uma função na seção Funções do Navegador, você pode exibir todos os usuários e grupos que receberam diretamente a função para o domínio e os serviços de aplicativo. É possível exibir as atribuições de função por usuários e grupos ou por serviços. Para navegar para um usuário ou grupo listado na seção Atribuições, clique com o botão direito do mouse no item desejado e selecione Navegar até o Item.

Você pode procurar funções definidas pelo sistema e personalizadas.

## Funções definidas pelo sistema

Uma função definida pelo sistema não pode ser editada nem excluída. A função Administrador é definida pelo sistema.

Quando você atribui a função de Administrador a um usuário ou grupo para o domínio, o Serviço Analyst, o Serviço de Integração de Dados, o Serviço de Ingestão em Massa, o Serviço do Metadata Manager, o Serviço de Repositório do Modelo ou o Serviço do Repositório do PowerCenter, o usuário ou grupo recebe todos os privilégios do serviço. A função de Administrador ignora a verificação de permissão. Usuários com a função de administrador podem acessar todos os objetos gerenciados pelo serviço.

## Função Administrador

Quando você atribui a função Administrador a um usuário ou grupo no domínio, Serviço de Integração de Dados ou Serviço do Repositório do PowerCenter, o usuário ou grupo podem realizar algumas tarefas, determinadas pela função Administrador e não por privilégios ou permissões.

Você pode atribuir a um usuário ou grupo todos os privilégios do domínio, Serviço de Integração de Dados ou do Serviço do Repositório do PowerCenter e depois conceder ao usuário ou grupo permissão total em todos os objetos de repositório do domínio ou do PowerCenter. No entanto, esse usuário ou grupo não pode executar as tarefas determinadas pela função Administrador.

Por exemplo, um usuário atribuído com a função Administrador no domínio pode configurar propriedades do domínio na ferramenta Administrator. Um usuário atribuído com todos os privilégios e permissões do domínio não pode configurar propriedades do domínio.

A tabela a seguir relaciona as tarefas determinadas pela função Administrador do domínio, do Serviço de Integração de Dados, do Serviço de Ingestão em Massa e do Serviço do Repositório do PowerCenter:

Serviço	Tarefas
Domínio	<ul style="list-style-type: none"><li>- Configure as propriedades do domínio.</li><li>- Defina as configurações de cluster.</li><li>- Criar perfis do sistema operacional.</li><li>- Excluir perfis do sistema operacional.</li><li>- Conceder permissão nos perfis de domínio e sistema operacional.</li><li>- Gerenciar e limpar eventos de log.</li><li>- Receber alertas de domínio.</li><li>- Executar o Relatório da Licença.</li><li>- Exibir eventos de log de atividade do usuário.</li><li>- Desligar o domínio.</li><li>- Acesse o assistente de atualização de serviço.</li></ul>
Serviço de Integração de Dados	<ul style="list-style-type: none"><li>- Atualizar o Serviço de Integração de Dados usando o menu Ações.</li></ul>
Serviço de Ingestão em Massa	<ul style="list-style-type: none"><li>- Procure todas as especificações de ingestão em massa.</li><li>- Edite uma especificação de ingestão em massa.</li><li>- Execute uma especificação de ingestão em massa.</li><li>- Exclua uma especificação de ingestão em massa.</li></ul>
Serviço do Repositório do PowerCenter	<ul style="list-style-type: none"><li>- Atribua perfis de sistema operacional a pastas de repositório se o Serviço de Integração do PowerCenter usar perfis de sistema operacional.*</li><li>- Altere o proprietário de pastas e objetos globais.*</li><li>- Configure permissões de pasta e objeto global.*</li><li>- Conectar ao Serviço de Integração do PowerCenter a partir do Cliente do PowerCenter ao executar o Serviço de Integração do PowerCenter em modo de segurança.</li><li>- Exclua um Serviço de Integração do PowerCenter no navegador do Workflow Manager.</li><li>- Exclua pastas e objetos globais.*</li><li>- Designe pastas a serem compartilhadas.*</li><li>- Edite o nome e a descrição de pastas.*</li></ul> <p>*O proprietário da pasta de repositório do PowerCenter ou o proprietário do objeto global também pode concluir essas tarefas.</p>

## Funções personalizadas

Uma função personalizada é uma função que você pode editar ou excluir.

Por padrão, a ferramenta Administrator inclui as seguintes funções personalizadas:

- Função personalizada do Serviço Analyst
- Funções personalizadas do Serviço do Metadata Manager
- Função personalizada do operador
- Funções personalizadas do Serviço do Repositório do PowerCenter
- Funções personalizadas do Serviço do Test Data Manager

Você pode editar os privilégios dessas funções ou excluí-las. Você também pode criar suas próprias funções personalizadas.

### Criando Funções Personalizadas

Quando você cria uma função personalizada, atribui privilégios à função para o domínio ou para um tipo de serviço de aplicativo. Uma função inclui privilégios para um ou mais serviços.

1. Na ferramenta Administrator, clique na guia Segurança.
2. No menu Ações de Segurança, clique em Criar Função.  
A caixa de diálogo Criar Função é exibida.
3. Insira as seguintes propriedades para a função:

Propriedade	Descrição
Nome	Nome da função. O nome da função não faz distinção entre letras maiúsculas e minúsculas e não pode ter mais que 128 caracteres. Não pode incluir uma guia, um caractere de nova linha nem os seguintes caracteres especiais: , + " \ < > ; / * % ?  O nome pode incluir um caractere de espaço ASCII, exceto no primeiro e último caractere. Nenhum outro caractere de espaço é permitido.
Descrição	Descrição da função. A descrição não pode exceder 765 caracteres, nem incluir uma guia, um caractere de nova linha nem os seguintes caracteres especiais: < > "

4. Clique na guia Privilégios.
5. Expanda o domínio ou um tipo de serviço de aplicativo.
6. Selecione os privilégios a serem atribuídos à função para o tipo de domínio ou de serviço de aplicativo.
7. Clique em OK.

### Editando Propriedades para Funções Personalizadas

Quando edita uma função personalizada, você pode alterar a descrição da função. Não é possível alterar o nome da função.

1. Na ferramenta Administrator, clique na guia Segurança.
2. Na seção Funções do Navegador, selecione uma função.
3. Clique em Editar.
4. Altere a descrição da função e clique em OK.

## Editando Privilégios Atribuídos a Funções Personalizadas

Você pode alterar os privilégios atribuídos a uma função personalizada para o domínio e para cada tipo de serviço de aplicativo.

1. Na ferramenta Administrator, clique na guia Segurança.
2. Na seção Funções do Navegador, selecione uma função.
3. Clique na guia Privilégios.
4. Clique em Editar.  
A caixa de diálogo Editar Funções e Privilégios é exibida.
5. Expanda o domínio ou um tipo de serviço de aplicativo.
6. Para atribuir privilégios à função, selecione os privilégios do tipo de domínio ou de serviço de aplicativo.
7. Para remover os privilégios da função, desmarque-os para o domínio ou o tipo de serviço de aplicativo.
8. Repita as etapas para alterar os privilégios para cada tipo de serviço.
9. Clique em OK.

## Excluindo funções personalizadas

Quando você exclui uma função personalizada, ela e todos os privilégios que inclui são removidos de qualquer usuário ou grupo atribuído à função.

Para excluir uma função personalizada, clique com o botão direito do mouse na seção Funções do Navegador e selecione Excluir função. Confirme se deseja excluir a função.

# Atribuindo privilégios e funções aos usuários e grupos

Determine as ações que usuários podem executar atribuindo os seguintes itens aos usuários e grupos:

- Privilégios. Um privilégio determina as ações que os usuários podem executar em clientes de aplicativo.
- Funções. Uma função é um conjunto de privilégios. Quando você atribui uma função a um usuário ou grupo, atribui o conjunto de privilégios pertencentes à função.

Use as funções e diretrizes a seguir quando atribuir privilégios e funções a usuários e grupos:

- Você atribui privilégios e funções a usuários e grupos para o domínio e para cada serviço de aplicativo que está em execução no domínio.  
Você não pode atribuir privilégios nem funções a usuários e grupos para um Serviço do Metadata Manager ou um Serviço de Repositório do PowerCenter nas seguintes situações:
  - O serviço de aplicativo está desativado.
  - O Serviço do Repositório do PowerCenter está sendo executado em modo exclusivo.
- Você pode atribuir privilégios e funções diferentes a um usuário ou grupo para cada serviço de aplicativo do mesmo tipo de serviço.
- Uma função inclui privilégios para os tipos de serviço de domínio e de vários aplicativos. Quando você atribui a função a um usuário ou grupo para um serviço de aplicativo, os privilégios para esse tipo de serviço de aplicativo são atribuídos ao usuário ou grupo.

Se você alterar os privilégios ou as funções atribuídos a um usuário, as alterações terão efeito no próximo login do usuário.

**Nota:** Não é possível editar os privilégios ou funções atribuídos por padrão à conta de usuário do Administrador.

## Privilégios herdados

Um usuário ou grupo pode herdar privilégios dos seguintes objetos:

- Grupo. Quando você atribui privilégios a um grupo, todos os subgrupos e usuários pertencentes ao grupo herdam os privilégios.
- Função. Quando você atribui uma função a um usuário, o usuário herda os privilégios pertencentes à função. Quando você atribui uma função a um grupo, o grupo e todos os subgrupos e usuários pertencentes ao grupo herdam os privilégios pertencentes à função. Os subgrupos e usuários não herdam a função.

Não é possível revogar privilégios herdados de um grupo ou função. Você pode atribuir privilégios adicionais a um usuário ou grupo que não tenha sido herdado de um grupo ou função.

A guia Privilégios para um usuário ou grupo exibe todas as funções e os privilégios atribuídos ao usuário ou grupo para o domínio e para cada serviço de aplicativo. Expanda o serviço de domínio ou aplicativo para exibir as funções e os privilégios atribuídos para o domínio ou serviço. Clique nos itens a seguir para exibir mais informações sobre as funções e os privilégios atribuídos:

- Nome de uma função atribuída. Exibe os detalhes da função no painel de detalhes.
- Ícone de informações para uma função atribuída. Realça todos os privilégios herdados com essa função.

Privilégios que são herdados de uma função ou grupo exibem um ícone de herança. A dica de ferramenta para um privilégio herdado exibe de qual função ou grupo o usuário herdou o privilégio.

## Atribuindo Privilégios e Funções a um Usuário ou Grupo por Navegação

1. Na ferramenta Administrador, clique na guia Segurança.
2. No navegador, selecione um usuário ou grupo.
3. Clique na guia Privilégios.
4. Clique em Editar.

A caixa de diálogo Editar Funções e Privilégios é exibida.

5. Para atribuir funções, expanda o domínio ou um serviço de aplicativo na guia Funções.
6. Para conceder funções, selecione-as para atribuir ao usuário ou grupo para o serviço de domínio ou aplicativo.

Você pode selecionar qualquer função que inclua privilégios para o tipo de domínio ou serviço de aplicativo selecionado.

7. Para revogar funções, limpe as funções atribuídas ao usuário ou grupo.
8. Repita as etapas [5](#) a [7](#) para atribuir funções para outro serviço.
9. Para atribuir privilégios, clique na guia Privilégios.
10. Expanda o domínio ou serviço de aplicativo.
11. Para conceder privilégios, selecione-os para atribuir ao usuário ou grupo para domínio ou serviço de aplicativo.



12. Para revogar privilégios, limpe os privilégios atribuídos ao usuário ou grupo.  
Você não pode revogar privilégios herdados de uma função ou um grupo.
13. Repita as etapas [10](#) a [12](#) para atribuir privilégios para outro serviço.
14. Clique em OK.

## Exibindo usuários com privilégios para um serviço

É possível exibir todos os usuários que possuem privilégios para o domínio ou um serviço de aplicativo.

1. Na ferramenta Administrador, clique na guia Segurança.
2. No menu Ações de Segurança, clique em Privilégios do Usuário do Serviço.  
A caixa de diálogo Serviços é exibida.
3. Selecione o domínio ou um serviço de aplicativo.  
O painel de detalhes exibe todos os usuários que possuem privilégios para o domínio ou serviço de aplicativo.
4. Clique com o botão direito do mouse em um nome de usuário e clique em Navegar até o Item para navegar até o usuário.

## Solucionando problemas de privilégios e funções

**Eu não consigo atribuir privilégios nem funções aos usuários para um Serviço do Metadata Manager ou ao Serviço de Repositório do PowerCenter.**

Você não pode atribuir privilégios nem funções a usuários e grupos para um Serviço do Metadata Manager ou um Serviço de Repositório do PowerCenter existente nas seguintes situações:

- O serviço de aplicativo está desativado.
- O Serviço do Repositório do PowerCenter está sendo executado em modo exclusivo.

**Eu removi um privilégio de um grupo. Por que alguns usuários no grupo ainda possuem esse privilégio?**

É possível usar alguns dos seguintes métodos para atribuir privilégios a um usuário:

- Atribuir um privilégio diretamente a um usuário.
- Atribuir uma função a um usuário.
- Atribuir um privilégio ou função a um grupo ao qual o usuário pertence.

Se você remover um privilégio de um grupo, os usuários pertencentes a esse grupo poderão receber diretamente o privilégio ou herdá-lo de uma função atribuída.

**Eu recebi todos os privilégios de domínio e permissão sobre todos os objetos do domínio, mas eu não consigo concluir todas as tarefas na ferramenta Administrador.**

Algumas das tarefas da ferramenta Administrador são determinadas pela função Administrador, não pelos privilégios ou pelas permissões. Você pode receber todos os privilégios para o domínio e as permissões

completas em todos os objetos de domínio. Entretanto, você não pode concluir as tarefas determinadas pela função Administrador.

### Eu recebi a função Administrador para um serviço de aplicativo, mas eu não consigo configurar o serviço de aplicativo na ferramenta Administrador.

Quando possui a função Administrador para um serviço de aplicativo, você é um administrador de aplicativo cliente. Um administrador de aplicativo cliente possui todas as permissões e privilégios em um aplicativo cliente.

Entretanto, um administrador de aplicativo cliente não possui permissões nem privilégios no domínio Informatica. Um administrador de aplicativo cliente não pode efetuar login na ferramenta Administrador para gerenciar o serviço para o aplicativo cliente para o qual ele possui privilégios de administrador.

Para gerenciar um serviço de aplicativo na ferramenta Administrador, você deve ter os privilégios e permissões de domínio apropriados.

### Eu recebi a função Administrador para o Serviço do Repositório do PowerCenter, mas eu não consigo usar o Repository Manager para executar uma limpeza de objetos ou criar extensões de metadados reutilizáveis.

Você deve ter o privilégio e a permissão do domínio do Gerenciar Serviços no Serviço do Repositório do PowerCenter na ferramenta Administrador para executar as seguintes ações no Repository Manager:

- Executar uma limpeza avançada de versões de objeto no nível de repositório do PowerCenter.
- Criar, editar e excluir extensões de metadados reutilizáveis.

### Meus privilégios indicam que eu posso editar objetos em um aplicativo cliente, mas eu não consigo editar metadados.

Talvez você não tenha as permissões do objeto necessárias no cliente de aplicativo. Mesmo que você tenha o privilégio para executar determinadas ações, talvez também necessite de permissão para executar a ação em um objeto específico.

### Eu não consigo usar pmrep para me conectar a um novo Serviço do Repositório do PowerCenter em execução no modo exclusivo.

O Gerenciador de Serviços pode não ter sincronizado a lista de usuários e grupos no repositório do PowerCenter com a lista no banco de dados de configuração de domínio. Para sincronizar a lista de usuários e grupos, reinicie o Serviço do Repositório do PowerCenter.

### Eu recebi todos os privilégios no grupo de privilégios Pastas para o Serviço do Repositório do PowerCenter e possuo permissão de leitura, gravação e execução em uma pasta. Entretanto, eu não consigo configurar as permissões para a pasta.

Somente o proprietário da pasta ou um usuário com a função Administrador para o Serviço do Repositório do PowerCenter pode concluir as seguintes tarefas de gerenciamento:

- Atribua perfis do sistema operacional às pastas se o Serviço de Integração do PowerCenter usar perfis do sistema operacional. Requer permissão no perfil do sistema operacional.
- Altere o proprietário da pasta.
- Configure permissões de pasta.
- Exclua a pasta.
- Designe a pasta a ser compartilhada.
- Edite o nome e a descrição da pasta.

Eu recebi a função Administrador do Serviço do Metadata Manager, mas não posso criar ou restaurar o repositório do Metadata Manager.

Para criar ou restaurar o repositório do Metadata Manager, você deve estar no grupo Administrador padrão. Os usuários no grupo Administrador padrão têm mais privilégios que os usuários que recebem a função Administrador de um serviço de aplicativo.

Eu recebi o privilégio Carregar recursos para o Serviço do Metadata Manager, mas recebo a mensagem de erro "privilégios insuficientes" quando tento carregar os recursos do Business Glossary.

Para carregar os recursos do Business Glossary, os privilégios Carregar Recurso, Gerenciar Recurso e Exibir Modelo são necessários. Você também precisa de permissão de gravação em qualquer recurso de glossário comercial que você queira carregar.

# CAPÍTULO 10

## Permissões

Este capítulo inclui os seguintes tópicos:

- [Visão geral de permissões, 188](#)
- [Permissões do Objeto de Domínio, 190](#)
- [Permissões de Conexão, 194](#)
- [Permissões de configuração de cluster, 197](#)
- [Permissões de aplicativos e objetos de aplicativo, 197](#)
- [Permissões de Serviço de Dados SQL, 199](#)
- [Permissões do serviço da Web, 203](#)

## Visão geral de permissões

Você gerencia a segurança do usuário com privilégios e permissões. Permissões definem o nível de acesso que usuários e grupos têm a um objeto.

Mesmo que um usuário tenha o privilégio para executar determinadas ações, ele também poderá precisar de permissão para executar a ação em um objeto específico.

Por exemplo, um usuário tem a permissão e o privilégio do domínio Gerenciar Serviços no Serviço do Repositório do PowerCenter de Desenvolvimento, mas não no Serviço do Repositório do PowerCenter de Produção. O usuário pode editar ou remover o Serviço do Repositório do PowerCenter de Desenvolvimento, mas não o serviço de Repositório do PowerCenter de Produção. Para gerenciar um serviço de aplicativo, um usuário deve ter a permissão e o privilégio do domínio Gerenciar Serviços e no serviço de aplicativo.

Você usa ferramentas diferentes para configurar permissões nos seguintes objetos:

Tipo de objeto	Ferramenta	Descrição
Aplicativos e objetos de aplicativo	Ferramenta Administrator	É possível atribuir permissões em aplicativos e objetos de aplicativo, como mapeamentos e fluxos de trabalho.
Objetos de conexão	Ferramenta Administrator Ferramenta Analyst Developer tool	É possível atribuir permissões em conexões definidas na ferramenta Administrator, na ferramenta Analyst ou na Developer tool. Essas ferramentas compartilham as permissões de conexão.

Tipo de objeto	Ferramenta	Descrição
Objetos de domínio	Ferramenta Administrator	Você pode atribuir permissões nos seguintes objetos de domínio: domínio, pastas, nós, grades, licenças, serviços de aplicativo e perfis do sistema operacional.
Objetos de catálogo do Metadata Manager	Metadata Manager	Você pode atribuir permissões em pastas e objetos de catálogo do Metadata Manager.
Projetos do repositório do Modelo	Ferramenta Analyst Developer tool	Você pode atribuir permissões em projetos definidos na ferramenta Analyst e na Developer tool. Essas ferramentas compartilham as permissões do projeto.
Objetos de repositório do PowerCenter	Cliente do PowerCenter	Você pode atribuir permissões em pastas do PowerCenter, grupos de implantação, rótulos, consulta e objetos de conexão.
Objetos de serviço de dados SQL	Ferramenta Administrator	Você pode atribuir permissões em objetos de dados SQL, como serviços de dados SQL, esquemas virtuais, tabelas virtuais e procedimentos armazenados virtuais.
Objetos de serviços da Web	Ferramenta Administrator	Você pode atribuir permissões em serviços da Web ou operações de serviço da Web.

## Tipos de Permissões

Os usuários e os grupos podem ter os seguintes tipos de permissões em um domínio:

### Permissões diretas

Permissões que são atribuídos diretamente a um usuário ou um grupo. Quando os usuários e os grupos têm permissão sobre um objeto, eles podem executar tarefas administrativas nesse objeto quando também têm o privilégio apropriado. Você pode editar permissões diretas.

### Permissões herdadas

Permissões que os usuários herdam. Quando os usuários têm permissão em um domínio ou pasta, eles herdam a permissão em todos os objetos no domínio ou na pasta. Quando os grupos têm permissão em um objeto de domínio, todos os subgrupos e usuários pertencentes ao grupo herdam a permissão no objeto do domínio. Por exemplo, um domínio tem uma pasta denominada Nós que contém vários nós. Se você atribuir uma permissão de grupo na pasta, todos os subgrupos e usuários pertencentes ao grupo herdam a permissão na pasta e em todos os nós na pasta .

Não é possível revogar as permissões herdadas. Também é possível revogar permissões de usuários ou grupos atribuídos à função de Administrador. A função de Administrador ignora a verificação de permissão. Usuários com a função de administrador podem acessar todos os objetos.

Você pode negar permissões herdadas em alguns tipos de objeto. Quando você nega permissões, configura exceções para as permissões que usuários e grupos possam já ter.

### Permissões efetivas

Superconjunto de todas as permissões para um usuário ou grupo. Inclui permissões diretas e herdadas.

Quando exibe detalhes de permissão, você pode exibir a origem de permissões efetivas. Detalhes das permissões exibem permissões diretas atribuídas ao usuário ou grupo, permissões diretas atribuídas a grupos pai e permissões herdadas de objetos pai. Além disso, detalhes da permissão exibem se o usuário ou grupo tem a função de administrador que ignora a verificação de permissão.

## Filtros de pesquisa de permissão

Ao atribuir permissões, exibir detalhes de permissão ou editar permissões para um usuário ou grupo, você pode usar filtros de pesquisa para procurar um usuário ou grupo.

Ao gerenciar permissões para um usuário ou grupo, você pode usar os seguintes filtros de pesquisa:

### Domínio de segurança

Selecione o domínio de segurança para procurar usuários ou grupos.

### String padrão

Digite uma string para procurar usuários ou grupos. A ferramenta Administrador retorna todos os nomes que contêm a string de pesquisa. A string não diferencia maiúsculas de minúsculas. Por exemplo, a string "DA" pode retornar "iasdaemon", "daphne", e "DA\_AdminGroup".

Você também pode classificar a lista de usuários ou grupos. Clique com o botão direito em um nome de coluna para classificá-la em ordem crescente ou decrescente.

## Permissões do Objeto de Domínio

Você configura privilégios e permissões para gerenciar a segurança do usuário no domínio. As permissões definem o nível de acesso que um usuário tem a um objeto de domínio. Para fazer login na ferramenta Administrador, o usuário deve ter permissão em pelo menos um objeto de domínio. Se o usuário tiver permissão em um objeto, mas não tiver o privilégio do domínio que concede a capacidade de modificar o tipo de objeto, só poderá exibir o objeto.

Por exemplo, se um usuário tiver permissão para um nó, mas não tiver o privilégio para Gerenciar Nós e Grades, ele pode exibir as propriedades do nó, mas não pode configurar, encerrar nem remover o nó.

Você pode configurar permissões nos seguintes tipos de objetos de domínio:

Tipo de Objeto de Domínio	Descrição de Permissão
Domínio	Permite que os usuários da ferramenta Administrator acessem todos os objetos no domínio. Quando os usuários têm permissão em um domínio, eles herdam a permissão em todos os objetos no domínio.
Pasta	Permite que os usuários da ferramenta Administrator acessem todos os objetos da pasta na ferramenta Administrator. Quando os usuários têm permissão em uma pasta, eles herdam a permissão em todos os objetos da pasta.
Nó	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades do nó. Sem permissão, um usuário não pode usar o nó ao definir um serviço de aplicativo ou criar uma grade.
Grade	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades da grade. Sem permissão, um usuário não pode atribuir a grade para um Serviço de Integração de Dados ou o Serviço de Integração do PowerCenter.
Licença	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades da licença. Sem permissão, um usuário não pode usar a licença ao criar um serviço de aplicativo.

Tipo de Objeto de Domínio	Descrição de Permissão
Serviço de Aplicativo	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades de serviço de aplicativo.
Perfil do Sistema Operacional	Permite que desenvolvedores, analistas e operadores do Informatica associados ao perfil do sistema operacional executem mapeamentos, perfis e fluxos de trabalho. Permite que os usuários do PowerCenter executem fluxos de trabalho associados com o perfil do sistema operacional. Se o usuário que executa um fluxo de trabalho não tiver permissão no perfil do sistema operacional atribuído ao fluxo de trabalho, o fluxo de trabalho falhará.

Você pode usar os seguintes métodos para gerenciar permissões de objeto de domínio:

- Gerenciar permissões por objeto de domínio. Use a exibição **Permissões** de um objeto de domínio para atribuir e editar permissões no objeto para vários usuários ou grupos.
- Gerenciar permissões por usuário ou grupo. Use a caixa de diálogo **Gerenciar permissões** para atribuir e editar permissões em objetos de domínio para determinado usuário ou grupo.

**Nota:** Você configura permissões em um perfil do sistema operacional de forma diferente da que você configura permissões em outros objetos de domínio.

## Permissões do objeto de domínio

Use a exibição **Permissões** de um objeto de domínio para atribuir, exibir e editar permissões no objeto de domínio para vários usuários ou grupos.

### Atribuindo Permissões em um Objeto de Domínio

Ao atribuir permissões em um objeto de domínio, você concede acesso de usuários e grupos para o objeto.

1. Na guia **Gerenciar**, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione o objeto de domínio.
3. No painel de conteúdo, selecione a exibição **Permissões**.
4. Clique na guia **Grupos** ou **Usuários**.
5. Clique em **Ações > Atribuir Permissão**.  
A caixa de diálogo **Atribuir permissões** exibe todos os usuários ou grupos que não têm permissão no objeto.
6. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
7. Selecione um usuário ou grupo e clique em **Próximo**.
8. Selecione **Permitir** e clique em **Concluir**.

### Exibindo Detalhes de Permissão em um Objeto de Domínio

Ao exibir detalhes de permissão, você pode exibir a origem de permissões efetivas.

1. Na guia **Gerenciar**, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione o objeto de domínio.
3. No painel de conteúdo, selecione a exibição **Permissões**.
4. Clique na guia **Grupos** ou **Usuários**.

5. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
6. Selecione um usuário ou grupo e clique em **Ações > Exibir Detalhes de Permissão**.  
A caixa de diálogo **Detalhes da Permissão** é exibida. A caixa de diálogo exibe permissões diretas atribuídas ao usuário ou grupo, permissões diretas atribuídas a grupos pai e permissões herdadas de objetos pai. Além disso, detalhes da permissão exibem se o usuário ou grupo tem a função de administrador que ignora a verificação de permissão.
7. Clique em **Fechar**.
8. Ou clique em **Editar Permissões** para editar permissões diretas.

## Editando permissões em um objeto de domínio

Você pode editar permissões diretas em um objeto de domínio para um usuário ou grupo. Não é possível revogar permissões herdadas nem suas próprias permissões.

**Nota:** Se você revogar permissões diretas em um objeto, o usuário ou grupo ainda assim poderá herdar permissões de um grupo ou objeto pai.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione o objeto de domínio.
3. No painel de conteúdo, selecione a exibição **Permissões**.
4. Clique na guia **Grupos** ou **Usuários**.
5. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
6. Selecione um usuário ou grupo e clique em **Ações > Editar Permissões Diretas**.  
A caixa de diálogo **Editar Permissões** é exibida.
7. Para atribuir permissões no objeto, selecione **Permitir**.
8. Para revogar permissões no objeto, selecione **Revogar**.  
Você pode clicar em **Exibir Detalhes da Permissão** para ver se a permissão foi diretamente atribuída ou herdada.
9. Clique em **OK**.

## Permissões por usuário ou grupo

Use a caixa de diálogo **Gerenciar Permissões** para exibir, atribuir e editar permissões de objeto de domínio para um usuário ou grupo específico.

### Exibindo Detalhes de Permissão de um Usuário ou Grupo

Ao exibir detalhes de permissão, você pode exibir a origem de permissões efetivas.

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Clique na guia **Grupos** ou **Usuários**.
3. Selecione um usuário ou grupo.
4. Clique na guia **Permissões**.



## Atribuindo e editando permissões para um usuário ou grupo

Quando você edita permissões de objeto de domínio para um usuário ou grupo, você pode atribuir permissões existentes e editar permissões diretas. Você não pode revogar permissões herdadas ou as próprias permissões.

Você pode clicar em **Exibir Detalhes da Permissão** para ver se a permissão foi diretamente atribuída ou herdada. Se você revogar uma permissão no objeto, o usuário ou grupo ainda assim poderá herdar essa permissão de um grupo ou objeto pai.

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Clique na guia **Grupos** ou **Usuários**.
3. Selecione um usuário ou grupo.
4. Clique na guia **Permissões**.
5. Selecione um objeto de domínio e clique em **Editar Permissões Diretas**.
6. Para atribuir uma permissão no objeto, selecione **Permitir**.
7. Para revogar permissões no objeto, selecione **Revogar**.
8. Clique em **OK**.

## Permissões do perfil do sistema operacional

Atribuir, exibir e editar permissões em perfis do sistema operacional na página Segurança da ferramenta Administrator.

O grupo Administrador tem permissões em todos os perfis do sistema operacional.

### Atribuindo Permissões em um Perfil do Sistema Operacional

Quando você atribui permissões em um perfil do sistema operacional, os usuários do Informatica executam mapeamentos, perfis e fluxos de trabalho com esse perfil do sistema operacional. Os usuários do PowerCenter executam fluxos de trabalho atribuídos ao perfil do sistema operacional.

1. Na ferramenta Administrator, clique na guia **Segurança**.
2. Clique na guia **Perfis do Sistema Operacional**.
3. Selecione um perfil do sistema operacional e clique na guia **Permissões**.
4. Clique na guia **Grupos** ou **Usuários** e selecione **Editar Permissões Diretas**.
5. Selecione um objeto de domínio e clique em **Editar Permissões Diretas**.
6. Para atribuir uma permissão no objeto, selecione **Permitir**.
7. Para revogar permissões no objeto, selecione **Revogar**.
8. Clique em **OK**.

### Exibindo detalhes de permissões em um perfil do sistema operacional

Ao exibir detalhes de permissão, você pode exibir a origem de permissões efetivas.

1. Na guia **Segurança**, selecione a exibição **Perfis do Sistema Operacional**.
2. Selecione o perfil do sistema operacional e clique na guia **Permissões**.
3. Selecione a exibição **Grupos** ou **Usuários**.
4. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.

5. Selecione um usuário ou grupo e clique em **Exibir Detalhes da Permissão**.

A caixa de diálogo **Detalhes da Permissão** é exibida. A caixa de diálogo exibe permissões diretas atribuídas ao usuário ou grupo, permissões diretas atribuídas a grupos pai e permissões herdadas de objetos pai. Além disso, detalhes da permissão exibem se o usuário ou grupo tem a função de administrador que ignora a verificação de permissão.

6. Clique em **Fechar**.
7. Ou clique em **Editar Permissões** para editar permissões diretas.

## Editando permissões em um perfil do sistema operacional

Você pode editar permissões diretas em um perfil do sistema operacional para um usuário ou grupo. Não é possível revogar permissões herdadas nem suas próprias permissões.

**Nota:** Se você revogar permissões diretas em um objeto, o usuário ou grupo ainda assim poderá herdar permissões de um grupo ou objeto pai.

1. Na guia **Segurança**, selecione a exibição **Perfis do Sistema Operacional**.
2. Selecione o perfil do sistema operacional e clique na guia **Permissões**.
3. Selecione a exibição **Grupos** ou **Usuários**.
4. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
5. Selecione um usuário ou grupo e clique em **Editar Permissões Diretas**.

A caixa de diálogo **Editar Permissões** é exibida.

6. Para atribuir permissões no perfil do sistema operacional, selecione **Permitir**.
7. Para revogar permissões no perfil do sistema operacional, selecione **Revogar**.

Você pode clicar em **Exibir Detalhes da Permissão** para ver se a permissão foi diretamente atribuída ou herdada.

8. Clique em **OK**.

## Permissões de Conexão

As permissões controlam o nível de acesso que um usuário ou grupo possuem na conexão.

Você pode configurar permissões em uma conexão na ferramenta Analyst, na ferramenta Desenvolvedor, ou na ferramenta Administrador.

Qualquer permissão de conexão que seja atribuída a um usuário ou grupo em uma ferramenta também se aplica em outras ferramentas. Por exemplo, você concedeu permissão ao GroupA sobre o ConnectionA na ferramenta Desenvolvedor. O GrupoA tem permissão sobre a ConexãoA na ferramenta Analyst e na ferramenta Administrador também.

Qualquer permissão de conexão que seja atribuída a um usuário ou grupo em uma ferramenta também se aplica em outras ferramentas. Por exemplo, você concedeu permissão ao GroupA sobre o ConnectionA na ferramenta Desenvolvedor. O GrupoA também tem permissão para a ConexãoA na ferramenta Administrador.

Os seguintes componentes da Informatica usam as permissões de conexão:

- Ferramenta Administrador. Impõe permissões de leitura, gravação e execução nas conexões.
- Ferramenta Analyst. Impõe permissões de leitura, gravação e execução nas conexões.

- Interface de linha de comando da Informatica. Impõe permissões de leitura, gravação e concede permissões nas conexões.
- Ferramenta Desenvolvedor. Impõe permissões de leitura, gravação e execução nas conexões. Para serviço de dados SQL, a ferramenta Desenvolvedor não impõe permissões de conexão. Ao contrário, ela impõe segurança de passagem e em nível de coluna para restringir o acesso aos dados.
- Serviço de Integração de Dados. Impõe permissões de execução quando um usuário tenta visualizar dados ou executar um mapeamento, scorecard ou perfil.

**Nota:** Você não pode atribuir permissões nas seguintes conexões: depósito de criação de perfil, banco de dados de cache do objeto de dados ou repositório do Modelo.

## Tipos de permissões de conexão

Você pode atribuir diferentes tipos de permissão a usuários para executar as seguintes ações:

Ação	Tipos de Permissão
Exibir todos os metadados de conexão, exceto senhas, como nome, tipo, descrição da conexão, strings de conexão e nomes de usuários.	Ler
Editar todos os metadados de conexão, incluindo senhas. Excluir a conexão. Usuários com permissão de Gravar herdam permissão de leitura.	Gravar
Acesse os dados físicos da fonte de dados subjacente definida pela conexão. Os usuários podem visualizar dados, executar mapeamentos, executar mapeamentos em fluxos de tarefa de mapeamento, executar scorecards ou executar perfis que usam a conexão.	Executar
Conceder e revogar permissões em conexões.	Conceder

## Permissões de Conexão Padrão

O administrador de domínio tem todas as permissões em todas as conexões. O usuário que cria uma conexão tem permissão de leitura, gravação, execução e concessão sobre a conexão. Por padrão, todos os usuários têm permissão para executar as seguintes ações nas conexões:

- Exibir metadados básicos de conexão, como o nome, descrição e tipo de conexão.
- Usar a conexão em mapeamentos na ferramenta Desenvolvedor.
- Criar perfis na ferramenta Analyst em objetos na conexão.

## Atribuindo Permissões sobre uma Conexão

Ao atribuir permissões em uma conexão, você define o nível de um usuário ou grupo para a conexão.

1. Na guia Gerenciar, selecione a exibição **Conexões**.
2. No Navegador, selecione a conexão.
3. No painel de conteúdo, selecione a exibição **Permissões**.
4. Clique na guia **Grupos** ou **Usuários**.
5. Clique em **Ações > Atribuir Permissão**.

A caixa de diálogo **Atribuir Permissões** exibe todos os usuários ou grupos que não têm permissão sobre a conexão.

6. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
7. Selecione um usuário ou grupo e clique em **Próximo**.
8. Selecione **Permitir** para cada tipo de permissão que você deseja atribuir.
9. Clique em **Concluir**.

## Exibindo detalhes de permissão em uma conexão

Ao exibir detalhes de permissão, você pode exibir a origem de permissões efetivas.

1. Na guia Gerenciar, selecione a exibição **Conexões**.
2. No Navegador, selecione a conexão.
3. No painel de conteúdo, selecione a exibição **Permissões**.
4. Clique na guia **Grupos** ou **Usuários**.
5. Selecione um usuário ou grupo e clique em **Ações > Exibir Detalhes de Permissão**.

A caixa de diálogo **Exibir Detalhes da Permissão** é exibida. A caixa de diálogo exibe permissões diretas atribuídas ao usuário ou grupo e permissões diretas atribuídas a grupos pai. Além disso, detalhes da permissão exibem se o usuário ou o grupo está atribuído à função de Administrador que ignora a verificação de permissão.

6. Clique em **Fechar**.
7. Ou clique em **Editar Permissões** para editar permissões diretas.

## Editando permissões em uma conexão

Você pode editar permissões diretas em uma conexão para um usuário ou grupo. Não é possível revogar permissões herdadas nem suas próprias permissões.

**Nota:** Se você revogar permissões diretas em um objeto, o usuário ou grupo ainda assim poderá herdar permissões de um grupo ou objeto pai.

1. Na guia Gerenciar, selecione a exibição **Conexões**.
2. No Navegador, selecione a conexão.
3. No painel de conteúdo, selecione a exibição **Permissões**.
4. Clique na guia **Grupos** ou **Usuários**.
5. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
6. Selecione um usuário ou grupo e clique em **Ações > Editar Permissões Diretas**.

A caixa de diálogo **Editar Permissões** é exibida.

7. Escolha se quer conceder ou revogar permissões.
  - Selecione **Permitir** para atribuir uma permissão.
  - Desmarque **Permitir** para revogar uma única permissão.
  - Selecione **Revogar** para revogar todas as permissões.

Você pode clicar em **Exibir Detalhes da Permissão** para ver se a permissão foi diretamente atribuída ou herdada.

8. Clique em **OK**.

# Permissões de configuração de cluster

As permissões controlam o nível de acesso que um usuário ou grupo tem em uma configuração de cluster.

É possível configurar as permissões em uma configuração de cluster na ferramenta Administrator e na interface de linha de comando da Informatica.

Um usuário ou grupo pode ter as seguintes permissões em uma configuração de cluster:

- Ler. Os membros do usuário ou grupo podem exibir a configuração de cluster.
- Gravar. Os membros do usuário ou grupo podem editar a configuração de cluster. Inclui permissão de leitura.
- Executar. Os membros do usuário ou grupo podem executar mapeamentos no ambiente Hadoop.
- Conceder. Os membros do usuário ou grupo podem conceder permissão na configuração de cluster para outros usuários e grupos. Inclui permissão de leitura.
- Todos. O usuário herda todas as permissões permitidas.

Por padrão, todos os usuários têm permissão para exibir o nome da configuração de cluster.

## Permissões de aplicativos e objetos de aplicativo

As permissões controlam o nível de acesso de um usuário ou grupo em aplicativos e objetos de aplicativo, como mapeamentos e fluxos de trabalho.

Você pode configurar permissões de aplicativos e objetos de aplicativo na ferramenta Administrator ou da linha de comando.

### Tipos de permissões de aplicativos e objetos de aplicativo

Você pode atribuir permissões para exibição, concessão e execução a usuários e grupos.

As seguintes permissões podem ser atribuídas a usuários e grupos:

#### **Permissão para exibição**

Exibir aplicativos e objetos de aplicativo.

#### **Permissão para concessão**

Permissões para concessão e revogação em aplicativos e objetos de aplicativo.

#### **Permissão para execução**

Executar aplicativos e objetos de aplicativo.

**Nota:** Para executar operações de aplicativo, como iniciar, interromper ou fazer backup na ferramenta Administrator ou a partir da linha de comando, o usuário deve ter permissão de execução e o privilégio de Gerenciar Aplicativos no aplicativo.

### Atribuindo permissões em um aplicativo ou objeto de aplicativo

Ao atribuir permissões em um aplicativo ou objeto de aplicativo, você define o nível de acesso de um usuário ou grupo ao aplicativo ou objeto de aplicativo.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.

2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione um aplicativo, um mapeamento ou um fluxo de trabalho.
5. No painel de detalhes, selecione a exibição **Permissões do Grupo** ou **Permissões de Usuário**.
6. Clique no botão **Atribuir Permissão**.  
A caixa de diálogo **Atribuir Permissões** exibe todos os usuários ou grupos que não têm permissão no aplicativo ou no objeto de aplicativo.
7. Insira as condições de filtro para procurar usuários e grupos, e clique no botão **Filtro**.
8. Selecione um usuário ou grupo e clique em **Próximo**.
9. Selecione **Permitir** para cada tipo de permissão que você deseja atribuir.
10. Clique em **Concluir**.

## Exibindo detalhes de permissões em um aplicativo ou objeto de aplicativo

Ao exibir detalhes de permissão, você pode exibir a origem de permissões efetivas.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o aplicativo, mapeamento ou fluxo de trabalho.
5. No painel de detalhes, selecione a exibição **Permissões do Grupo** ou **Permissões de Usuário**.
6. Insira as condições de filtro para procurar usuários e grupos, e clique no botão **Filtro**.
7. Selecione um usuário ou grupo e clique em **Exibir Detalhes de Permissão**.

A caixa de diálogo **Detalhes da Permissão** é exibida. A caixa de diálogo exibe permissões diretas atribuídas ao usuário ou grupo, permissões diretas atribuídas a grupos pai e permissões herdadas de objetos pai. Além disso, detalhes da permissão exibem se o usuário ou grupo tem a função de administrador que ignora a verificação de permissão.

8. Clique em **Fechar**.
9. Ou clique em **Editar Permissões** para editar permissões diretas.

## Editando permissões em um aplicativo ou objeto de aplicativo

É possível editar permissões diretas em um aplicativo ou objeto de aplicativo para um usuário ou grupo. Não é possível revogar permissões herdadas nem suas próprias permissões.

**Nota:** Se você revogar permissões diretas em um objeto, o usuário ou grupo ainda assim poderá herdar permissões de um grupo ou objeto pai.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o aplicativo ou objeto de aplicativo.
5. No painel de detalhes, selecione a exibição **Permissões do Grupo** ou **Permissões de Usuário**.
6. Insira as condições de filtro para procurar usuários e grupos, e clique no botão **Filtro**.

7. Selecione um usuário ou grupo e clique no botão **Editar Permissões Diretas**.

A caixa de diálogo **Editar Permissões Diretas** é exibida.

8. Escolha se quer conceder ou revogar permissões.

- Selecione **Permitir** para atribuir uma permissão.
- Desmarque **Permitir** para revogar uma única permissão.
- Selecione **Revogar** para revogar todas as permissões.

Você pode clicar em **Exibir Detalhes da Permissão** para ver se a permissão foi diretamente atribuída ou herdada.

9. Clique em **OK**.

## Negando permissões em um aplicativo ou objeto de aplicativo

É possível negar explicitamente permissões de aplicativos e objetos de aplicativo. Quando você nega uma permissão, está aplicando uma exceção à permissão efetiva.

## Permissões de Serviço de Dados SQL

Os usuários finais podem conectar-se a um serviço de dados SQL por meio de uma ferramenta de cliente JDBC ou ODBC. Depois da conexão, os usuários podem executar as consultas SQL em relação às tabelas virtuais em um serviço de dados SQL ou podem executar um procedimento armazenado virtual em um serviço de dados SQL. As permissões controlam o nível de acesso que um usuário tem a um serviço de dados SQL.

É possível atribuir permissões aos usuários e grupos nos seguintes objetos do serviço de dados SQL:

- serviço de dados SQL
- Tabela virtual
- Procedimento armazenado virtual

Quando você atribui permissões em um objeto de serviço de dados SQL, o usuário ou grupo herda as mesmas permissões sobre todos os objetos pertencentes ao objeto de serviço de dados SQL. Por exemplo, você atribui uma permissão de seleção de usuário em um serviço de dados SQL. O usuário herda a permissão selecionar em todas as tabelas virtuais no serviço de dados SQL.

Você pode negar permissões para usuários e grupos em alguns objetos de serviço de dados SQL. Quando você nega permissões, configura exceções para as permissões que usuários e grupos possam já ter. Por exemplo, você não pode atribuir permissões para uma coluna em uma tabela virtual, mas pode negar que um usuário execute uma instrução SQL SELECT que inclui a coluna.

## Tipos de Permissões de Serviço de Dados SQL

Você pode atribuir as seguintes permissões a usuários e grupos:

- Permissão de concessão. Os usuários podem conceder e revogar permissões nos objetos do serviço de dados SQL usando a ferramenta Administrador ou usando o programa de linha de comando *infacmd*.
- Permissão de execução. Os usuários podem executar procedimentos virtuais armazenados no serviço de dados SQL usando uma ferramenta de cliente do JDBC ou ODBC.

- Permissão de seleção. Os usuários podem executar instruções SQL SELECT em tabelas virtuais no serviço de dados SQL usando uma ferramenta de cliente do JDBC ou ODBC.

Algumas permissões não são aplicáveis para todos os objetos do serviço de dados SQL.

A tabela a seguir descreve as permissões para cada objeto de serviço de dados SQL:

Objeto	Permissão de Concessão	Permissão de Execução	Permissão de Seleção
serviço de dados SQL	Conceda e revogue permissões no serviço de dados SQL e todos os objetos no serviço de dados SQL.	Execute todos os procedimentos armazenados virtuais no serviço de dados SQL.	Execute as instruções SQL SELECT em todas as tabelas virtuais no serviço de dados SQL.
Tabela virtual	Conceda e revogue permissões na tabela virtual.	-	Execute instruções SQL SELECT na tabela virtual.
Procedimento armazenado virtual	Conceda e revogue permissões no procedimento armazenado virtual.	Execute o procedimento armazenado virtual.	-

## Atribuindo Permissões em um serviço de dados SQL

Ao atribuir permissões em um objeto de serviço de dados SQL, você define o nível de acesso de um usuário ou grupo para o objeto.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o objeto de serviço de dados SQL.
5. No painel de detalhes, selecione a exibição **Permissões de Grupo** ou **Permissões de Usuário**.
6. Clique no botão **Atribuir Permissão**.

A caixa de diálogo **Atribuir Permissões** exibe todos os usuários ou grupos que não têm permissão no objeto de serviço de dados SQL.

7. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
8. Selecione um usuário ou grupo e clique em **Próximo**.
9. Selecione **Permitir** para cada tipo de permissão que você deseja atribuir.
10. Clique em **Concluir**.

## Exibindo Detalhes de Permissão em um Serviço de Dados SQL

Ao exibir detalhes de permissão, você pode exibir a origem de permissões efetivas.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o objeto de serviço de dados SQL.
5. No painel de detalhes, selecione a exibição **Permissões de Grupo** ou **Permissões de Usuário**.
6. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
7. Selecione um usuário ou grupo e clique em **Exibir Detalhes de Permissão**.



A caixa de diálogo **Detalhes da Permissão** é exibida. A caixa de diálogo exibe permissões diretas atribuídas ao usuário ou grupo, permissões diretas atribuídas a grupos pai e permissões herdadas de objetos pai. Além disso, detalhes da permissão exibem se o usuário ou grupo tem a função de administrador que ignora a verificação de permissão.

8. Clique em **Fechar**.
9. Ou clique em **Editar Permissões** para editar permissões diretas.

## Editando permissões em um Serviço de Dados SQL

Você pode editar permissões diretas em um serviço de dados SQL para um usuário ou grupo. Não é possível revogar permissões herdadas nem suas próprias permissões.

**Nota:** Se você revogar permissões diretas em um objeto, o usuário ou grupo ainda assim poderá herdar permissões de um grupo ou objeto pai.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o objeto de serviço de dados SQL.
5. No painel de detalhes, selecione a exibição **Permissões de Grupo** ou **Permissões de Usuário**.
6. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
7. Selecione um usuário ou grupo e clique no botão **Editar Permissões Diretas**.

A caixa de diálogo **Editar Permissões** é exibida.

8. Escolha se quer conceder ou revogar permissões.
  - Selecione **Permitir** para atribuir uma permissão.
  - Desmarque **Permitir** para revogar uma única permissão.
  - Selecione **Revogar** para revogar todas as permissões.

Você pode clicar em **Exibir Detalhes da Permissão** para ver se a permissão foi diretamente atribuída ou herdada.

9. Clique em **OK**.

## Negando Permissões em um Serviço de Dados SQL

Você pode claramente negar permissões em alguns objetos de serviço de dados SQL. Quando você negar uma permissão de um objeto em um serviço de dados SQL, está aplicando uma exceção à permissão efetiva.

Para negar permissões, use um dos seguintes comandos infacmd:

- `infacmd sql SetStoredProcedurePermissions`. Nega permissões Executar ou Conceder no nível de procedimento armazenado.
- `infacmd sql SetTablePermissions`. Nega permissões Selecionar ou Conceder no nível de tabela virtual.
- `infacmd sql SetColumnPermissions`. Nega permissões Selecionar no nível de coluna.

Cada comando tem opções para aplicar permissões (-ap) e negar permissões (-dp). O comando `SetColumnPermissions` não contém a opção de aplicar permissões.

**Nota:** Você não pode negar permissões a partir da ferramenta Administrador.

O Data Integration Service verifica as permissões antes de executar consultas e procedimentos armazenados no SQL em relação ao banco de dados virtual. O Data Integration Service valida as permissões para os usuários ou grupos começando pelo nível de serviço de dados SQL. Quando as permissões se aplicarem a um objeto pai em um serviço de dados SQL, os objetos filhos herdam a permissão. O Data Integration Service verifica as permissões negadas no nível de coluna.

## Segurança em Nível de Coluna

Um administrador pode negar acesso a colunas em uma tabela virtual de um objeto de dados SQL. O administrador pode configurar o comportamento do Data Integration Service para consultas em uma coluna restrita.

Podem ocorrer os seguintes resultados quando o usuário consultar uma coluna para a qual ele não tem permissão.

- A consulta retorna a um valor substituto em lugar dos dados. A consulta retorna um valor substituto em cada linha retornada. O valor substituto substitui o valor da coluna por meio de uma consulta. Se a consulta contiver filtros ou junções, o substituto dos resultados é exibido nos resultados.
- A consulta falha com o erro de permissão insuficiente.

Para obter mais informações sobre a configuração de segurança para serviços de dados SQL, consulte o artigo "Como configurar a segurança para serviços de dados SQL" na Biblioteca de Recursos da Informatica: [https://kb.informatica.com/h2l/HowTo%20Library/1/0266\\_ConfiguringSecurityForSQLDataServices.pdf](https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf).

### Colunas restritas

Quando você configura a segurança em nível de coluna, defina uma opção de coluna que determina o que ocorre quando um usuário seleciona a coluna restrita em uma consulta. Você pode substituir os dados restritos por um valor padrão. Ou pode cancelar a consulta se um usuário selecionar a coluna restrita.

Por exemplo, um Administrador nega o acesso de um usuário à coluna salário na tabela Funcionário. O Administrador configura um valor substituto de 100.000 para a coluna salário. Quando o usuário selecionar a coluna salário em uma consulta SQL, o Data Integration Service retorna 100.000 para o salário em cada linha.

Execute o comando `infacmd sql UpdateColumnOptions` para configurar as opções de colunas. Você não pode definir opções de coluna na ferramenta Administrador.

Quando você executar `infacmd sql UpdateColumnOptions`, digite as seguintes opções:

#### **ColumnOptions.DenyWith=option**

Determina se você vai substituir o valor de coluna restrita ou cancelar a consulta. Se você substituir o valor da coluna, pode optar por substituí-lo por NULL ou por um valor constante. Digite uma das seguintes opções:

- **ERROR.** Cancela a consulta e retorna um erro quando uma consulta SQL selecionar uma coluna restrita.
- **NULL.** Retorna valores nulos para uma coluna restrita em cada linha.
- **VALUE.** Retorna um valor constante em lugar da coluna restrita em cada linha. Configure o valor constante na opção `ColumnOptions.InsufficientPermissionValue`.

#### **ColumnOptions.InsufficientPermissionValue=value**

Substitui o valor de coluna restrita por uma constante. O padrão é uma sequência de caracteres vazia. Se o Data Integration Service substituir a coluna por uma sequência de caracteres vazia, mas a coluna

for um número ou uma data, a consulta retorna erros. Se você não configurar um valor para a opção DenyWith, o Data Integration Service ignora a opção InsufficientPermissionValue.

Para configurar um valor substituto para uma coluna, digite o comando com a seguinte sintaxe:

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd  
Adminpass -sqlds employee_APP.employees_SQL -t Employee -c Salary -o  
ColumnOptions.DenyWith=VALUE ColumnOptions.InsufficientPermissionValue=100000
```

Se você não configurar nenhuma opção para uma coluna restrita, o padrão é não cancelar a consulta. A consulta é executada e o Data Integration Service substitui o valor da coluna por NULL.

## Adicionando segurança em nível de coluna

Configurar segurança de nível de coluna com o comando `infacmd sql SetColumnPermissions`. Você não pode definir segurança de nível de coluna a partir da ferramenta Administrador.

Uma tabela Funcionário contém colunas Nome, Sobrenome, Departamento e Salário. Você possibilita que um usuário acesse a tabela Funcionário mas restringe o usuário de acessar a coluna Salário.

Para restringir o usuário de acessar a coluna Salário, desative o Data Integration Service e digite um `infacmd` semelhante ao seguinte comando:

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd  
Adminpass -sqlds employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

As seguintes instruções SQL retornam NULL na coluna Salário:

```
Select * from Employee  
Select LastName, Salary from Employee
```

O comportamento padrão é retornar valores nulos.

# Permissões do serviço da Web

Os usuários finais podem enviar solicitações de serviço da Web e receber respostas de serviço da Web por meio de um cliente de serviços da Web. As permissões controlam o nível de acesso de um usuário a um serviço da Web.

É possível atribuir permissões a usuários e grupos nos seguintes objetos de serviço da Web:

- Serviço da Web
- Recurso de serviço da Web REST
- Operação de serviço da Web SOAP

Quando você atribui permissões em um objeto de serviço da Web, o usuário ou grupo herda as mesmas permissões em todos os objetos que pertencem ao objeto de serviço da Web. Por exemplo, você atribui a um usuário a permissão de execução para um serviço da Web. O usuário herda a permissão de execução de operações de serviço da Web no serviço da Web.

Você pode negar permissões a usuários e grupos em uma operação de serviço da Web. Quando você nega permissões, configura exceções para as permissões que usuários e grupos possam já ter. Por exemplo, um usuário tem permissões de execução em um serviço da Web que tem três operações. Você pode impedir que um usuário execute uma operação de serviço da Web que pertence ao serviço da Web.

## Tipos de Permissões de Serviços da Web

Um administrador atribui permissões de serviços da Web aos seguintes tipos de usuários e grupos:

- Consumidor de serviços da Web. Um usuário de domínio nativo que envia uma solicitação ao serviço da Web e recebe uma resposta do serviço da Web. O usuário deve ter permissão de execução no serviço da Web.
- Administrador de serviço da Web. Um usuário pode fazer login no Administrator, editar as propriedades do serviço da Web e conceder permissões a outros usuários.
- Operador de serviço da Web. Um usuário pode fazer login no Administrator, monitorar um serviço da Web e iniciar ou parar um serviço da Web.

Um administrador pode atribuir as seguintes permissões a usuários e grupos:

- Permissão de concessão. Os usuários podem gerenciar permissões nos objetos de serviços da Web usando a ferramenta Administrador ou usando o programa de linha de comando *infacmd*.
- Permissão de execução. Os usuários podem enviar solicitações de serviços da Web e receber respostas de serviços da Web.

A seguinte tabela descreve as permissões para cada objeto de serviços da Web SOAP:

Objeto	Permissão de Concessão	Permissão para Execução
Serviço da Web SOAP	Conceder e revogar permissões no serviço da Web e todas as operações de serviço da Web dentro do serviço da Web.	Enviar solicitações de serviço da Web e receber respostas de serviço da Web de todas as operações de serviço da Web dentro do serviço da Web.
Operação de serviço da Web SOAP	Conceder, revogar e negar permissão na operação de serviço da Web.	Enviar solicitações de serviço da Web e receber respostas de serviço da Web da operação de serviço da Web.

A tabela a seguir descreve as permissões para cada objeto de serviços da Web REST:

Objeto	Permissão de Concessão	Permissão para Execução
Serviço da Web REST	Conceda e revogue permissões no serviço da Web REST e todos os recursos de serviços da Web dentro do serviço da Web.	Envie solicitações de serviços da Web e receba respostas de serviços da Web de todos os recursos de serviços da Web no serviço da Web REST.
Recurso REST	Conceda, revogue e negue permissões no recurso de serviço da Web REST.	Enviar solicitações de serviço da Web e receber respostas de serviços da Web do recurso do serviço Web REST.

## Atribuindo permissões em um serviço da Web

Ao atribuir permissões em um objeto de serviços da Web, você define o nível de acesso de um usuário ou grupo para o objeto.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o objeto de serviços da Web.
5. No painel de detalhes, selecione a exibição **Permissões de Grupo** ou **Permissões de Usuário**.
6. Clique no botão **Atribuir Permissão**.

A caixa de diálogo **Atribuir Permissões** exibe todos os usuários ou grupos que não têm permissão no objeto de serviço de dados SQL.

7. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
8. Selecione um usuário ou grupo e clique em **Próximo**.
9. Selecione **Permitir** para cada tipo de permissão que você deseja atribuir.
10. Clique em **Concluir**.

## Exibindo Detalhes de Permissão em um Serviço da Web

Ao exibir detalhes de permissão, você pode exibir a origem de permissões efetivas.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o objeto de serviços da Web.
5. No painel de detalhes, selecione a exibição **Permissões de Grupo** ou **Permissões de Usuário**.
6. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
7. Selecione um usuário ou grupo e clique em **Exibir Detalhes de Permissão**.

A caixa de diálogo **Detalhes da Permissão** é exibida. A caixa de diálogo exibe permissões diretas atribuídas ao usuário ou grupo, permissões diretas atribuídas a grupos pai e permissões herdadas de objetos pai. Além disso, detalhes da permissão exibem se o usuário ou grupo tem a função de administrador que ignora a verificação de permissão.

8. Clique em **Fechar**.
9. Ou clique em **Editar Permissões** para editar permissões diretas.

## Editando permissões em um serviço Web

Você pode editar permissões diretas em um serviço Web para um usuário ou grupo. Ao editar permissões em um objeto de serviço Web, você pode negar permissões no objeto. Não é possível revogar permissões herdadas nem suas próprias permissões.

**Nota:** Se você revogar permissões diretas em um objeto, o usuário ou grupo ainda assim poderá herdar permissões de um grupo ou objeto pai.

1. Na guia Gerenciar, selecione a exibição **Serviços e Nós**.
2. No Navegador, selecione um Serviço de Integração de Dados.
3. No painel de conteúdo, selecione a exibição **Aplicativos**.
4. Selecione o objeto de serviços da Web.
5. No painel de detalhes, selecione a exibição **Permissões de Grupo** ou **Permissões de Usuário**.
6. Insira as condições de filtro para procurar usuários e grupos e clique no botão **Filtro**.
7. Selecione um usuário ou grupo e clique no botão **Editar Permissões Diretas**.

A caixa de diálogo **Editar Permissões** é exibida.

8. Escolha se quer conceder ou revogar permissões.
  - Selecione **Permitir** para atribuir uma permissão.
  - Selecione **Negar** para negar uma permissão em um objeto de serviços Web.

- Desmarque **Permitir** para revogar uma única permissão.
- Selecione **Revogar** para revogar todas as permissões.

Você pode clicar em **Exibir Detalhes da Permissão** para ver se a permissão foi diretamente atribuída ou herdada.

9. Clique em **OK**.

# CAPÍTULO 11

## Relatórios de Auditoria

Este capítulo inclui os seguintes tópicos:

- [Visão Geral dos Relatórios de Auditoria, 207](#)
- [Informações Pessoais do Usuário, 208](#)
- [Associação de Grupo de Usuários, 208](#)
- [Privilégios, 209](#)
- [Associação de Funções, 210](#)
- [Permissões em Objetos de Domínio, 210](#)
- [Selecionando Usuários para um Relatório de Auditoria, 211](#)
- [Selecionando Grupos para um Relatório de Auditoria, 212](#)
- [Selecionando Funções para um Relatório de Auditoria, 212](#)

## Visão Geral dos Relatórios de Auditoria

Use os relatórios de auditoria para exibir as informações sobre usuários e grupos no domínio Informatica e os privilégios e permissões atribuídos a eles.

Você pode gerar os seguintes relatórios de auditoria:

### **Informações Pessoais do Usuário**

Exibe as informações sobre as contas de usuário no domínio, incluindo o status do usuário. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

### **Associação de Grupo de Usuários**

Exibe informações sobre usuários e os grupos aos quais eles pertencem. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

### **Privilégios**

Exibe as informações sobre os privilégios atribuídos a usuários e grupos no domínio. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

### **Funções**

Exibe as informações sobre as funções atribuídas a usuários e grupos no domínio. Você pode selecionar as funções para as quais deseja gerar o relatório.

### **Permissões em Objetos de Domínio**

Exibe as informações sobre os objetos de domínio nos quais os usuários e grupos têm permissão. Você pode selecionar os usuários ou grupos para os quais deseja gerar o relatório.

Você pode gerar os relatórios de auditoria em diferentes formatos, incluindo arquivos CSV, PDF ou de texto. Você também pode exibir o relatório na tela.

Você pode gerar os relatórios de auditoria usando a ferramenta Administrator ou a linha de comando. Para gerar os relatórios de auditoria da linha de comando, execute o programa de linha de comando `infacmd aud`.

## Informações Pessoais do Usuário

O relatório Informações Pessoais do Usuário exibe as informações de contato e o status de contas de usuário no domínio.

Se você executar o relatório para grupos, ele organizará a lista de usuários por grupo e exibirá o nome do grupo e o domínio de segurança de cada grupo. O relatório exibe os grupos aninhados separadamente.

O relatório Informações Pessoais do Usuário exibe as seguintes informações:

**Nome de Logon**

Nome de logon da conta de usuário.

**Nome Completo**

Nome completo da conta de usuário.

**Domínio de segurança**

Domínio de segurança ao qual o usuário pertence.

**Descrição**

Descrição da conta de usuário.

**ID de E-mail**

Endereço de e-mail da conta de usuário.

**Telefone**

Número de telefone da conta de usuário.

**Conta Bloqueada**

Indica se a conta está ou não bloqueada. O relatório exibirá Sim se a conta estiver bloqueada, e Não se a conta não estiver bloqueada.

**Conta Desativada**

Indica se a conta está ou não desativada. O relatório exibirá Sim se a conta estiver desativada, e Não se a conta estiver ativada.

## Associação de Grupo de Usuários

O relatório Associação de Grupo de Usuários exibe informações sobre os usuários e seus grupos associados.

Se você executar o relatório para usuários, ele mostrará a lista de usuários e os grupos aos quais eles pertencem.

O relatório Associação de Grupo de Usuários exibe as seguintes informações:



**Nome de Logon**

Nome de logon da conta de usuário.

**Nome Completo**

Nome completo da conta de usuário.

**Domínio de Segurança**

Domínio de segurança ao qual a conta de usuário pertence.

**Nome do Grupo**

Nome do grupo ao qual o usuário pertence.

**Caminho do Grupo**

Se for um grupo único, o caminho do grupo mostrará o nome do grupo. Se for um grupo aninhado, o caminho do grupo mostrará sua posição na hierarquia de grupos aninhados.

**Domínio de Segurança do Grupo**

Domínio de segurança do grupo ao qual o usuário pertence.

Se você executar o relatório para grupos, ele organizará a lista de usuários por grupo e exibirá o nome do grupo e o domínio de segurança de cada grupo. O relatório exibe os grupos aninhados separadamente. Para cada grupo, o relatório mostra a lista de usuários e os grupos filho que pertencem ao grupo.

O relatório Associação de Grupo de Usuários exibe as seguintes informações dos usuários que pertencem ao grupo:

**Nome de Logon**

Nome de logon da conta de usuário.

**Nome Completo**

Nome completo da conta de usuário.

**Domínio de segurança**

Domínio de segurança ao qual a conta de usuário pertence.

O relatório Associação de Grupo de Usuários exibe as seguintes informações dos grupos filho que pertencem ao grupo:

**Nome do grupo**

Nome do grupo.

**Domínio de segurança**

Domínio de segurança ao qual o grupo pertence.

**Caminho do Grupo**

Se for um grupo único, o caminho do grupo mostrará o nome do grupo. Se for um grupo aninhado, o caminho do grupo mostrará sua posição na hierarquia de grupos aninhados.

## Privilégios

O relatório Privilégios exibe os usuários e grupos e os privilégios atribuídos a eles.

Se você executar o relatório para usuários, ele mostrará a lista de usuários e os privilégios atribuídos a cada um deles. Se você executar o relatório para grupos, ele mostrará a lista de grupos e os privilégios atribuídos a cada um deles.

O relatório Privilégios exibe as seguintes informações:

**Nome do Privilégio**

O nome do privilégio.

**Caminho do Privilégio**

A hierarquia do grupo de privilégio que contém o privilégio.

**Nome do Objeto**

O nome do objeto no qual o privilégio é permitido.

**Tipo de Objeto**

O tipo de objeto no qual o privilégio é permitido.

## Associação de Funções

O relatório Associação de Funções exibe uma lista de funções e os usuários e grupos aos quais elas estão atribuídas.

O relatório Associação de Funções exibe as seguintes informações:

**Nome de Logon**

Nome de logon da conta de usuário à qual a função foi atribuída. Exibe a lista de usuários.

**Nome Completo**

Nome completo da conta de usuário à qual a função foi atribuída. Exibe a lista de usuários.

**Nome do grupo**

Nome do grupo ao qual a função foi atribuída. Exibe a lista de grupos.

**Domínio de segurança**

Domínio de segurança ao qual o usuário ou grupo pertence.

**Nome do Objeto**

Nome do objeto em que o conjunto de privilégios é permitido na função.

**Tipo de Objeto**

Tipo de objeto em que o conjunto de privilégios é permitido na função.

## Permissões em Objetos de Domínio

O relatório Permissões em Objetos de Domínio exibe os usuários e grupos e os objetos nos quais eles têm permissão.

Se você executar o relatório para usuários, ele mostrará a lista de usuários e os objetos nos quais eles têm permissões. Se você executar o relatório para grupos, ele mostrará a lista de grupos e os objetos nos quais eles têm permissões.

O relatório Permissões em Objetos de Domínio exibe as seguintes informações:

**Nome do Objeto**

O nome do objeto no qual o usuário ou grupo tem permissão.

#### Tipo de Objeto

O tipo de objeto no qual o usuário ou grupo tem permissão.

#### Caminho do Objeto

A localização do objeto no repositório.

## Selecionando Usuários para um Relatório de Auditoria

Você pode gerar um relatório de auditoria para vários usuários.

1. Na ferramenta Administrator, clique em **Segurança > Relatórios de Auditoria**.
2. Na lista **Selecionar Tipo de Relatório**, selecione o tipo de relatório de auditoria que você deseja executar.
3. Na lista **Gerar Relatório para**, selecione **Usuários** e clique em **Ir**.  
A caixa de diálogo **Selecionar Usuários** é exibida. Por padrão, o ícone **Usuários** está selecionado, e a lista de todos os usuários disponíveis é exibida. A lista mostra o nome completo do usuário e o domínio de segurança ao qual o usuário pertence.
4. Na lista **Usuários Disponíveis**, selecione os usuários para os quais você deseja executar o relatório.  
Use as teclas Shift ou Ctrl para selecionar vários usuários.
5. Para selecionar usuários por grupo, clique no ícone **Grupos**.  
A lista **Grupos Disponíveis** exibe todos os grupos no domínio, e a lista **Membros** exibe os usuários que são membros dos grupos. Na lista **Membros**, selecione os usuários para os quais você deseja executar o relatório. Você pode selecionar usuários de vários grupos.
6. Clique em **Adicionar**.  
Para executar o relatório para todos os usuários, clique no ícone **Usuários** e clique em **Adicionar Tudo** sem selecionar nenhum usuário.  
Para executar o relatório para todos os usuários em um grupo, clique no ícone **Grupos**. Selecione um grupo e clique em **Adicionar Tudo** sem selecionar nenhum usuário na lista **Membros**.  
Os usuários selecionados são movidos para a lista **Usuários Selecionados**.
7. Na lista **Formato de Saída do Relatório**, selecione o formato para exibição do relatório.  
Por padrão, o relatório é exibido na tela.  
Você também pode exibir um relatório de auditoria em um dos seguintes formatos:
  - Texto. Gera o relatório de auditoria como um arquivo de texto com valores listados em colunas.
  - CSV. Gera o relatório de auditoria como um arquivo de texto com valores separados por vírgulas.
  - PDF. Gera o relatório de auditoria no formato .pdf. Você deve instalar o Acrobat Reader para exibir o relatório.
8. Clique em **Gerar Relatório**.

# Selecionando Grupos para um Relatório de Auditoria

Você pode executar relatórios de auditoria para vários grupos.

1. Na ferramenta Administrator, clique em **Segurança > Relatórios de Auditoria**.
2. Na lista **Selecionar Tipo de Relatório**, selecione o tipo de relatório de auditoria que você deseja executar.
3. Na lista **Gerar Relatório para**, selecione **Grupos** e clique em **Ir**.  
A caixa de diálogo **Selecionar Grupos** é exibida. A lista de grupos é organizada por domínio de segurança.
4. Na lista **Grupos Disponíveis**, selecione os grupos para os quais você deseja executar o relatório.  
Use as teclas Shift ou Ctrl para selecionar vários grupos.
5. Clique em **Adicionar**.  
Para executar o relatório para todos os grupos, não selecione nenhum grupo e clique em **Adicionar Tudo**.  
Os grupos selecionados são movidos para a lista **Grupos Selecionados**.
6. Na lista **Formato de Saída do Relatório**, selecione o formato para exibição do relatório.  
Por padrão, os relatórios são exibidos na tela.  
Você também pode executar um relatório de auditoria em um dos seguintes formatos:
  - Texto. Gera o relatório de auditoria como um arquivo de texto com valores listados em colunas.
  - CSV. Gera o relatório de auditoria como um arquivo de texto com valores separados por vírgulas.
  - PDF. Gera o relatório de auditoria no formato .pdf. Você deve instalar o Acrobat Reader para exibir o relatório.
7. Clique em **Gerar Relatório**.

# Selecionando Funções para um Relatório de Auditoria

Ao executar o relatório Associação de Funções, você deve selecionar as funções para as quais deseja executar o relatório.

1. Na ferramenta Administrator, clique em **Segurança > Relatórios de Auditoria**.
2. Na lista **Selecionar Tipo de Relatório**, selecione o relatório **Associação de Funções**.
3. Na lista **Gerar Relatório para**, selecione **Funções** e clique em **Ir**.  
A caixa de diálogo **Selecionar Funções** é exibida. A lista de funções definidas pelo sistema aparece separadamente da lista de funções personalizadas.
4. Na lista **Funções Disponíveis**, selecione as funções para as quais você deseja executar o relatório.  
Use as teclas Shift ou Ctrl para selecionar várias funções.
5. Clique em **Adicionar**.  
Para executar o relatório para todas as funções, não selecione nenhuma função e clique em **Adicionar Tudo**.

As funções selecionadas são movidas para a lista **Funções Selecionadas**.

6. Na lista **Formato de Saída do Relatório**, selecione o formato para exibição do relatório.

Por padrão, os relatórios são exibidos na tela.

Você também pode executar um relatório de auditoria em um dos seguintes formatos:

- Texto. Gera o relatório de auditoria como um arquivo de texto com valores listados em colunas.
- CSV. Gera o relatório de auditoria como um arquivo de texto com valores separados por vírgulas.
- PDF. Gera o relatório de auditoria no formato .pdf. Você deve instalar o Acrobat Reader para exibir o relatório.

7. Clique em **Gerar Relatório**.

## APÊNDICE A

# Permissões e Privilégios da Linha de Comando

Este apêndice inclui os seguintes tópicos:

- [Comandos \*infacmd as\*, 214](#)
- [Comandos \*infacmd cluster\*, 215](#)
- [Comandos \*infacmd dis\*, 216](#)
- [Comandos \*infacmd dp\*, 218](#)
- [Comandos \*infacmd es\*, 218](#)
- [Comandos \*infacmd ipc\*, 218](#)
- [Comandos \*infacmd isp\*, 218](#)
- [Comandos \*infacmd mas\*, 228](#)
- [Comandos \*infacmd mi\*, 229](#)
- [Comandos \*infacmd mrs\*, 229](#)
- [Comandos \*infacmd ms\*, 232](#)
- [Comandos \*infacmd tools\*, 232](#)
- [Comandos \*infacmd ps\*, 232](#)
- [Comandos \*infacmd pwx\*, 233](#)
- [Comandos \*infacmd rms\*, 234](#)
- [Comandos \*infacmd rtm\*, 235](#)
- [Comandos \*infacmd sch\*, 235](#)
- [Comandos \*infacmd sql\*, 236](#)
- [Comandos \*infacmd wfs\*, 237](#)
- [Comandos \*pmcmd\*, 237](#)
- [Comandos \*pmrep\*, 240](#)

## Comandos *infacmd as*

Para executar comandos *infacmd as*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio, privilégios de Serviço Analyst e permissões de objeto de domínio.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd as*:

Comando <i>infacmd as</i>	Grupo de Privilégio	Nome do Privilégio	Permissão para...
CreateAuditTables	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde o Serviço Analyst é executado
CreateService	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde o Serviço Analyst é executado
DeleteAuditTables	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde o Serviço Analyst é executado
ListServiceOptions	-	-	Serviço Analyst
ListServiceProcessOptions	-	-	Serviço Analyst
UpdateServiceOptions	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde o Serviço Analyst é executado
UpdateServiceProcessOptions	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde o Serviço Analyst é executado

## Comandos *infacmd cluster*

Para executar os comandos *infacmd cluster*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio e permissões de configuração de cluster.

A seguinte tabela relaciona os privilégios e as permissões necessários para os comandos *infacmd cluster*:

Comando <i>infacmd cluster</i>	Grupo de Privilégios	Nome do Privilégio	Permissão para...
clearConfigurationProperties	Administração de Domínio	Gerenciar conexões	Gravar na configuração de cluster
createConfiguration	Administração de Domínio	Gerenciar conexões	Gravar nas configurações de cluster
deleteConfiguration	Administração de Domínio	Gerenciar conexões	Gravar nas configurações de cluster
exportConfiguration com propriedades confidenciais	-	-	Gravar na configuração de cluster
exportConfiguration sem propriedades confidenciais	-	-	Ler nas configurações do cluster

Comando infacmd cluster	Grupo de Privilégios	Nome do Privilégio	Permissão para...
listAssociatedConnections	-	-	-
listConfigurations	-	-	-
listConfigurationGroupPermissions	-	-	-
listConfigurationProperties	-	-	Ler nas configurações do cluster
listConfigurationSets	-	-	Ler nas configurações do cluster
listConfigurationUserPermissions	-	-	-
refreshConfiguration	Administração de Domínio	Gerenciar conexões	Gravar nas configurações de cluster
setConfigurationPermissions	-	-	Conceder na configuração de cluster
setConfigurationProperties	Administração de Domínio	Gerenciar conexões	Gravar nas configurações de cluster

## Comandos infacmd dis

Para executar comandos *infacmd dis*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio, privilégios de Serviço de Integração de Dados e permissões de objeto de domínio.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd dis*:

Comando infacmd dis	Grupo de Privilégios	Nome do Privilégio	Permissão para...
BackupApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
CancelDataObjectCacheRefresh	-	-	-
CreateService	Administração de Domínio	Gerenciar Serviços	Domínio ou nó onde o Serviço de Integração de Dados é executado
DeployApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
ListApplicationObjects	-	-	-



Comando infacmd dis	Grupo de Privilégios	Nome do Privilégio	Permissão para...
ListApplications	-	-	-
ListComputeOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Integração de Dados
ListDataObjectOptions	-	-	-
ListServiceOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Integração de Dados
ListServiceProcessOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Integração de Dados
PurgeDataObjectCache	-	-	-
RefreshDataObjectCache	-	-	-
RenameApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
RestoreApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
StartApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
StopApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
stopBlazeService	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
UndeployApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
UpdateApplication	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
UpdateApplicationOptions	Administração de Aplicativo	Gerenciar Aplicativos	Aplicativo
UpdateDataObjectOptions	Administração de Aplicativo	Gerenciar Aplicativos	-
UpdateComputeOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Integração de Dados
UpdateServiceOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Integração de Dados
UpdateServiceProcessOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Integração de Dados

## Comandos infacmd dp

Os usuários devem ser usuários nativos ou receber a função Administrador para executar os seguintes comandos infacmd dp:

- startSparkJobServer
- stopSparkJobServer

## Comandos infacmd es

Os usuários devem ser atribuídos com a função Administrador do domínio para executar os seguintes comandos infacmd es:

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

## Comandos infacmd ipc

Para executar comandos *infacmd ipc*, os usuários devem ter uma das permissões relacionadas de objeto de repositório do modelo.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd ipc*:

Comando infacmd ipc	Grupo de Privilégios	Nome do Privilégio	Permissão para...
ExportToPC	-	-	Leitura na pasta que cria tabelas de referência a serem exportadas
genReuseReportFromPC	Ferramentas	Acessar o Gerenciador de Repositório	-

## Comandos infacmd isp

Para executar os seguintes comandos *infacmd isp*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio, privilégios de serviço, permissões de objeto de domínio e permissões de conexão.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd isp*:

Comando <i>infacmd isp</i>	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
AddAlertUser (para outros usuários)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
AddAlertUser (para sua conta de usuário)	-	-	-
AddConnectionPermissions	-	-	Conceder na conexão
AddDomainLink*	-	-	-
AddDomainNode	Administração de Domínio	Gerenciar Nós e Grades	Domínio e nó
AddGroupPrivilege	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
AddLicense	Administração de Domínio	Gerenciar Serviços	Pasta pai ou do domínio
AddNodeResource	Administração de Domínio	Gerenciar Nós e Grades	Nó
AddRolePrivilege	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
AddServiceLevel*	-	-	-
AddUserToGroup	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
AssignGroupPermission (em serviços de aplicativo ou objetos de licença)	Administração de Domínio	Gerenciar Serviços	Serviço de aplicativo ou objeto de licença
AssignGroupPermission (no domínio)*	-	-	-
AssignGroupPermission (nas pastas)	Administração de Domínio	Gerenciar Pastas do Domínio	Pasta
AssignGroupPermission (nos nós e grades)	Administração de Domínio	Gerenciar Nós e Grades	Nó ou grade
AssignGroupPermission (nos perfis do sistema operacional)*	-	-	-
AssignISTOMMService	Administração de Domínio	Gerenciar Serviços	Serviço do Metadata Manager

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
AssignLicense	Administração de Domínio	Gerenciar Serviços	Objeto de licença e serviço de aplicativo
AssignRSToWSHubService	Administração de Domínio	Gerenciar Serviços	Serviço do Repositório do PowerCenter e Hub de Serviços da Web
AssignRoleToGroup	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
AssignRoleToUser	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
AssignUserPermission (nos serviços de aplicativo ou objetos de licença)	Administração de Domínio	Gerenciar Serviços	Serviço de aplicativo ou objeto de licença
AssignUserPermission (no domínio)*	-	-	-
AssignUserPermission (nas pastas)	Administração de Domínio	Gerenciar Pastas do Domínio	Pasta
AssignUserPermission (nos nós ou grades)	Administração de Domínio	Gerenciar Nós e Grades	Nó ou grade
AssignUserPermission (nos perfis do sistema operacional)*	-	-	-
AssignUserPrivilege	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
AssignedToLicense	Administração de Domínio	Gerenciar Serviços	Objeto de licença e serviço de aplicativo
ConvertLogFile	-	-	Domínio ou serviço de aplicativo
CreateConnection*	-	-	-
CreateFolder	Administração de Domínio	Gerenciar Pastas do Domínio	Pasta pai ou do domínio
CreateGrid	Administração de Domínio	Gerenciar Nós e Grades	Pasta pai ou de domínio e nós atribuídos à grade

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
CreateGroup	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
CreateIntegrationService	Administração de Domínio	Gerenciar Serviços	Pasta pai ou de domínio, nó ou grade onde é executado o Serviço de Integração do PowerCenter, objeto de licença e Serviço do Repositório do PowerCenter associado
CreateMMService	Administração de Domínio	Gerenciar Serviços	Pasta pai ou de domínio, nó onde é executado o Serviço do Metadata Manager, objeto de licença e Serviço de Integração do PowerCenter associado e Serviço do Repositório do PowerCenter
CreateOSProfile*	-	-	-
CreateRepositoryService	Administração de Domínio	Gerenciar Serviços	Pasta pai ou de domínio, nó onde é executado o Serviço do Repositório do PowerCenter e objeto de licença
CreateRole	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
CreateSAPBWService	Administração de Domínio	Gerenciar Serviços	Pasta pai ou de domínio, nó ou grade onde é executado o Serviço SAP BW, o objeto de licença e o Serviço de Integração do PowerCenter associado
CreateUser	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
CreateWSHubService	Administração de Domínio	Gerenciar Serviços	Pasta pai ou de domínio, nó ou grade onde é executado o Hub de Serviços da Web, o objeto de licença e o Serviço do Repositório do PowerCenter associado
DisableNodeResource	Administração de Domínio	Gerenciar Nós e Grades	Nó

<b>Comando infacmd isp</b>	<b>Grupo de Privilégios</b>	<b>Nome do Privilégio</b>	<b>Permissão Ativada</b>
DisableService (para Serviço do Metadata Manager)	Administração de Domínio	Gerenciar Execução do Serviço	Serviço do Metadata Manager, Serviço de Integração do PowerCenter associado e Serviço do Repositório do PowerCenter.
DisableService (para outros serviços de aplicativo)	Administração de Domínio	Gerenciar Execução do Serviço	Serviço de aplicativo
DisableServiceProcess	Administração de Domínio	Gerenciar Execução do Serviço	Serviço de aplicativo
DisableUser	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
EditUser	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
EnableNodeResource	Administração de Domínio	Gerenciar Nós e Grades	Nó
EnableService (para Serviço do Metadata Manager)	Administração de Domínio	Gerenciar Execução do Serviço	Serviço do Metadata Manager, Serviço de Integração do PowerCenter associado e Serviço do Repositório do PowerCenter.
EnableService (para todos os outros serviços de aplicativo)	Administração de Domínio	Gerenciar Execução do Serviço	Serviço de aplicativo
EnableServiceProcess	Administração de Domínio	Gerenciar Execução do Serviço	Serviço de aplicativo
EnableUser	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ExportDomainObjects (para conexões)	Administração de Domínio	Gerenciar conexões	Leitura em conexões
ExportDomainObjects (para usuários, grupos e funções)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ExportUsersAndGroups	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
GetFolderInfo	-	-	Pasta
GetLastError	-	-	Serviço de aplicativo
GetLog	-	-	Domínio ou serviço de aplicativo
GetNodeName	-	-	Nó
GetServiceOption	-	-	Serviço de aplicativo
GetServiceProcessOption	-	-	Serviço de aplicativo
GetServiceProcessStatus	-	-	Serviço de aplicativo
GetServiceStatus	-	-	Serviço de aplicativo
GetSessionLog	Objetos de Tempo de Execução	Monitorar	Leitura na pasta de repositório
GetWorkflowLog	Objetos de Tempo de Execução	Monitorar	Leitura na pasta de repositório
Ajuda	-	-	-
ImportDomainObjects (para conexões)	Administração de Domínio	Gerenciar conexões	Gravar em conexões
ImportDomainObjects (para usuários, grupos e funções)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ImportUsersAndGroups	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ListAlertUsers	-	-	Domínio
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	Leitura na conexão
ListConnectionPermissions	-	-	-
ListConnectionPermissions por grupo	-	-	-
ListConnectionPermissions por usuário	-	-	-
ListConnections	-	-	-

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
ListDomainLinks	-	-	Domínio
ListDomainOptions	-	-	Domínio
ListFolders	-	-	Pastas
ListGridNodes	-	-	-
ListGroupPermissions	-	-	-
ListGroupPrivilege	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
ListGroupsForUser	-	-	Domínio
ListLDAPConnectivity	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ListLicenses	-	-	Objetos de licença
ListNodeOptions	-	-	Nó
ListNodeResources	-	-	Nó
ListNodes	-	-	-
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domínio
ListRolePrivileges	-	-	-
ListSMTPOptions	-	-	Domínio
ListSecurityDomains	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ListServiceLevels	-	-	Domínio
ListServiceNodes	-	-	Serviço de aplicativo
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListUserPermissions	-	-	-



Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
ListUserPrivilege	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
MoveFolder	Administração de Domínio	Gerenciar Pastas do Domínio	Pastas de origem e destino
MoveObject (para serviços de aplicativo ou objetos de licença)	Administração de Domínio	Gerenciar Serviços	Pastas de origem e destino
MoveObject (para nós ou grades)	Administração de Domínio	Gerenciar Nós e Grades	Pastas de origem e destino
Ping	-	-	-
PurgeLog*	-	-	-
RemoveAlertUser (para outros usuários)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
RemoveAlertUser (para conta de usuário)	-	-	-
RemoveConnection	-	-	Gravar na conexão
RemoveConnectionPermissions	-	-	Conceder na conexão
RemoveDomainLink*	-	-	-
RemoveFolder	Administração de Domínio	Gerenciar Pastas do Domínio	Pasta pai ou de domínio e pasta sendo removida
RemoveGrid	Administração de Domínio	Gerenciar Nós e Grades	Pasta pai ou de domínio e grade
RemoveGroup	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
RemoveGroupPrivilege	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
RemoveLicense	Administração de Domínio	Gerenciar Serviços	Pasta pai ou de domínio ou objeto de licença
RemoveNode	Administração de Domínio	Gerenciar Nós e Grades	Pasta pai ou de domínio e nó

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
RemoveNodeResource	Administração de Domínio	Gerenciar Nós e Grades	Nó
RemoveOSProfile*	-	-	-
RemoveRole	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
RemoveRolePrivilege	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
RemoveService	Administração de Domínio	Gerenciar Serviços	Pasta pai ou de domínio e serviço de aplicativo
RemoveServiceLevel*	-	-	-
RemoveUser	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
RemoveUserFromGroup	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
RemoveUserPrivilege	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
RenameConnection	-	-	Gravar na conexão
ResetPassword (para outros usuários)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ResetPassword (para sua conta de usuário)	-	-	-
RunCPUProfile	Administração de Domínio	Gerenciar Nós e Grades	Nó
SetConnectionPermission	-	-	Conceder na conexão
SetLDAPConnectivity	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
SetRepositoryLDAPConfiguration	-	-	Domínio
ShowLicense	-	-	Objeto de licença

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
ShutdownNode	Administração de Domínio	Gerenciar Nós e Grades	Nó
SwitchToGatewayNode*	-	-	-
SwitchToWorkerNode*	-	-	-
UnAssignISMMService	Administração de Domínio	Gerenciar Serviços	Serviço de Integração do PowerCenter e Serviço do Metadata Manager
UnAssignRoleFromGroup	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
UnAssignRoleFromUser	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
UnassignLicense	Administração de Domínio	Gerenciar Serviços	Objeto de licença e serviço de aplicativo
UnassignRSWSHubService	Administração de Domínio	Gerenciar Serviços	Serviço do Repositório do PowerCenter e Hub de Serviços da Web
UnassociateDomainNode	Administração de Domínio	Gerenciar Nós e Grades	Nó
UpdateConnection	-	-	Gravar na conexão
UpdateDomainOptions*	-	-	-
UpdateFolder	Administração de Domínio	Gerenciar Pastas do Domínio	Pasta
UpdateGatewayInfo*	-	-	-
UpdateGrid	Administração de Domínio	Gerenciar Nós e Grades	Grades e nós
UpdateIntegrationService	Administração de Domínio	Gerenciar Serviços	Serviço de Integração do PowerCenter
UpdateLicense	Administração de Domínio	Gerenciar Serviços	Objeto de licença
UpdateMMService	Administração de Domínio	Gerenciar Serviços	Serviço do Metadata Manager

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
UpdateNodeOptions	Administração de Domínio	Gerenciar Nós e Grades	Nó
UpdateNodeRole	Administração de Domínio	Gerenciar Nós e Grades	Nó
UpdateOSProfile	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	Perfil do sistema operacional
UpdateRepositoryService	Administração de Domínio	Gerenciar Serviços	Serviço do Repositório do PowerCenter
UpdateSAPBWService	Administração de Domínio	Gerenciar Serviços	Serviço SAP BW
UpdateSMTPOptions*	-	-	-
UpdateServiceLevel*	-	-	-
UpdateServiceProcess	Administração de Domínio	Gerenciar Serviços	Serviço de Integração do PowerCenter Cada nó adicionado ao Serviço de Integração do PowerCenter
UpdateWSHubService	Administração de Domínio	Gerenciar Serviços	Hub de Serviços da Web
generateHadoopConnectionFromHiveConnection	-	-	-
listMonitoringOptions	Monitoramento	Configuração de Monitoramento	Domínio
purgeMonitoringData	Monitoramento	Configuração de Monitoramento	Domínio
updateMonitoringOptions	Monitoramento	Configuração de Monitoramento	Domínio
<i>*Para executar esses comandos, os usuários devem receber a função Administrador do domínio.</i>			

## Comandos infacmd mas

Para executar comandos *infacmd mas*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio, privilégios de Serviço de Acesso a Metadados e permissões de objeto de domínio.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd mas*:

Comando <i>infacmd</i> dis	Grupo de Privilégios	Nome do Privilégio	Permissão para...
CreateService	Administração de Domínio	Gerenciar Serviços	Domínio ou nó onde o Serviço de Acesso a Metadados é executado
ListServiceOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Acesso a Metadados
ListServiceProcessOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Acesso a Metadados
UpdateServiceOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Acesso a Metadados
UpdateServiceProcessOptions	Administração de Domínio	Gerenciar Serviços	Serviço de Acesso a Metadados

## Comandos *infacmd mi*

Os usuários devem receber a função Administrador no Serviço de Ingestão em Massa para executar os seguintes comandos *infacmd mi*:

- clearSamlConfig
- updateSamlConfig

## Comandos *infacmd mrs*

Para executar comandos *infacmd mrs*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio, privilégios de Serviço de Repositório do Modelo e permissões de objeto de repositório do modelo.

Os usuários podem executar os seguintes comandos, que estão relacionados a operações de bloqueio e controle de versão, em objetos que eles possuem. Executar os comandos em objetos que outros usuários possuem requer o privilégio Gerenciar Desenvolvimento Baseado em Equipe:

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout
- UnlockObject

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd mrs*:

Comando <i>infacmd mrs</i>	Grupo de Privilégios	Nome do Privilégio	Permissão para...
BackupContents	Administração de Domínio	Gerenciar Serviço	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
CheckInObject	Administração de Domínio	Gerenciar Desenvolvimento Baseado em Equipe	O Serviço de Repositório do Modelo
CreateContents	Administração de Domínio	Gerenciar Serviço	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
CreateFolder	Administração de Domínio	Para a Developer tool: - Acesso ao Developer Para a ferramenta Analyst: - Acesso ao Analyst - Acesso ao espaço de trabalho Descoberta	O Serviço de Repositório do Modelo
CreateProject	Administração de Domínio	Criar, Editar e Excluir Projetos	O Serviço de Repositório do Modelo
CreateService	Administração de Domínio	Gerenciar Serviço	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
DeleteContents	Administração de Domínio	Gerenciar Serviço	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
DeleteFolder	Administração de Domínio	Para a Developer tool: - Acesso ao Developer Para a ferramenta Analyst: - Acesso ao Analyst - Acesso ao espaço de trabalho Descoberta	O Serviço de Repositório do Modelo
DeleteProject	Administração de Domínio	Criar, Editar e Excluir Projetos	O Serviço de Repositório do Modelo
ListBackupFiles	Administração de Domínio	Gerenciar Serviço	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
ListCheckedOutObjects	Administração de Domínio	Gerenciar Desenvolvimento Baseado em Equipe	O Serviço de Repositório do Modelo
ListFolders	Administração de Domínio	Gerenciar Serviço	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
ListLockedObjects	Administração de Domínio	Gerenciar Desenvolvimento Baseado em Equipe	O Serviço de Repositório do Modelo

Comando infacmd mrs	Grupo de Privilégios	Nome do Privilégio	Permissão para...
ListProjects	Administração de Domínio	Para a Developer tool: - Acesso ao Developer Para a ferramenta Analyst: - Acesso ao Analyst - Acesso ao espaço de trabalho Descoberta	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
ListServiceOptions	-	-	O Serviço de Repositório do Modelo
ListServiceProcessOptions	-	-	O Serviço de Repositório do Modelo
PopulateVCS	Administração de Domínio	Gerenciar Desenvolvimento Baseado em Equipe	O Serviço de Repositório do Modelo
ReassignCheckedOutObject	Administração de Domínio	Gerenciar Desenvolvimento Baseado em Equipe	O Serviço de Repositório do Modelo
RebuildDependencyGraph	-	-	O Serviço de Repositório do Modelo
RenameFolder	Administração de Domínio	Para a Developer tool: - Acesso ao Developer Para a ferramenta Analyst: - Acesso ao Analyst - Acesso ao espaço de trabalho Descoberta	O Serviço de Repositório do Modelo
RestoreContents	Administração de Domínio	Gerenciar Serviço	O domínio ou o nó onde o Serviço de Repositório do Modelo é executado
UndoCheckout	Administração de Domínio	Gerenciar Desenvolvimento Baseado em Equipe	O Serviço de Repositório do Modelo
UnlockObject	Administração de Domínio	Gerenciar Desenvolvimento Baseado em Equipe	O Serviço de Repositório do Modelo
UpdateServiceOptions	Administração de Domínio	Gerenciar Serviço	O Serviço de Repositório do Modelo
UpdateServiceProcessOptions	Administração de Domínio	Gerenciar Serviço	O Serviço de Repositório do Modelo
UpgradeContents	Administração do Serviço de Repositório do Modelo	Gerenciar Serviço	O Serviço de Repositório do Modelo

## Comandos infacmd ms

Para executar comandos *infacmd ms*, os usuários devem ter um dos conjuntos relacionados de permissões de objeto de domínio.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd ms*:

Comando infacmd ms	Grupo de Privilégios	Nome do Privilégio	Permissão para...
deleteMappingPersistedOutputs	-	-	Executar no aplicativo
getRequestLog	-	-	-
listMappingParams	-	-	-
listMappingPersistedOutputs	-	-	Exibir no aplicativo
listMappings	-	-	-
runMapping	-	-	Executar objetos de conexão usados pelo mapeamento.

## Comandos infacmd tools

Para executar comandos *infacmd tools*, os usuários devem ter uma das permissões relacionadas de objeto de repositório do modelo.

A tabela a seguir lista as permissões necessárias para comandos *infacmd tools*:

Comando infacmd tools	Grupo de Privilégios	Nome do Privilégio	Permissão para...
ExportObjects	-	-	Leitura do projeto
ImportObjects	-	-	Gravar no projeto

## Comandos infacmd ps

Para executar comandos *infacmd ps*, os usuários devem ter um dos conjuntos relacionados de privilégios de criação de perfil e permissões de objeto de domínio.



A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd ps*:

Comando <i>infacmd ps</i>	Grupo de Privilégio	Nome do Privilégio	Permissão para...
CreateWH	-	-	-
DropWH	-	-	-
Executar	-	-	Leitura do projeto Executar no objeto de conexão de origem
List	-	-	Leitura do projeto
Purge	-	-	Ler e gravar no projeto

## Comandos *infacmd pwx*

Para executar comandos *infacmd pwx*, os usuários devem ter um dos conjuntos relacionados de permissões e privilégios do serviço de aplicativo PowerExchange.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd pwx*:

Comando <i>infacmd pwx</i>	Grupo de Privilégio	Nome do Privilégio	Permissão para...
CloseForceListener	Comandos de Gerenciamento	closeforce	-
CloseListener	Comandos de Gerenciamento	fechar	-
CondenseLogger	Comandos de Gerenciamento	condense	-
CreateListenerService	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde é executado o serviço de aplicativo PowerExchange
CreateLoggerService	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde é executado o serviço de aplicativo PowerExchange
DisplayAllLogger	Comandos de Informações	displayall	-
DisplayCPULogger	Comandos de Informações	displaycpu	-
DisplayEventsLogger	Comandos de Informações	displayevents	-

Comando infacmd pwx	Grupo de Privilégio	Nome do Privilégio	Permissão para...
DisplayMemoryLogger	Comandos de Informações	displaymemory	-
DisplayRecordsLogger	Comandos de Informações	displayrecords	-
DisplayStatusLogger	Comandos de Informações	displaystatus	-
FileSwitchLogger	Comandos de Gerenciamento	fileswitch	-
ListTaskListener	Comandos de Informações	listtask	-
ShutDownLogger	Comandos de Gerenciamento	shutdown	-
StopTaskListener	Comandos de Gerenciamento	stoptask	-
UpdateListenerService	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde é executado o serviço de aplicativo PowerExchange
UpdateLoggerService	Administração de Domínio	Gerenciar Serviço	Domínio ou nó onde é executado o serviço de aplicativo PowerExchange

## Comandos infacmd rms

Para executar comandos *infacmd rms*, os usuários devem ter um dos conjuntos listados de privilégios e permissões de domínio

A seguinte tabela lista os privilégios e as permissões necessários para os comandos *infacmd rms*:

Comando infacmd rms	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
ListComputeNodeAttributes	Administração de Domínio	-	Serviço do Gerenciador de Recursos
ListServiceOptions	Administração de Domínio	-	Serviço do Gerenciador de Recursos
SetComputeNodeAttributes	Administração de Domínio	Gerenciar Serviços	Serviço do Gerenciador de Recursos
UpdateServiceOptions	Administração de Domínio	Gerenciar Serviços	Serviço do Gerenciador de Recursos

## Comandos infacmd rtm

Para executar comandos *infacmd rtm*, os usuários devem ter um dos conjuntos relacionados de privilégios do Serviço de Repositório do Modelo e permissões de objeto de domínio.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd rtm*:

Comando infacmd rtm	Grupo de Privilégio	Nome do Privilégio	Permissão para...
Deployimport	-	-	-
Exportar	-	-	Leitura no projeto que contém tabelas de referência a ser exportadas
Importar	-	-	Leitura e Gravação no projeto onde as tabelas de referência são importadas

## Comandos infacmd sch

Para executar comandos *infacmd sch*, os usuários devem ter um dos conjuntos listados de permissões e privilégios.

A tabela a seguir lista os privilégios e as permissões necessários para os comandos *infacmd sch*:

Comando infacmd sch	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
CreateSchedule	Privilégios do Agendador	Criar Agendamento	Serviço de Agendador
DeleteSchedule	Privilégios do Agendador	Excluir Agendamento	Serviço de Agendador
ListSchedule	Privilégios do Agendador	Exibir Agendamentos	Serviço de Agendador
ListServiceOptions	Privilégios do Domínio	Gerenciar serviços	Serviço de Agendador
ListServiceProcessOptions	Privilégios do Domínio	Gerenciar serviços	Serviço de Agendador
PauseAll	Privilégios do Agendador	Editar Agendamento	Serviço de Agendador
PauseSchedule	Privilégios do Agendador	Editar Agendamento	Serviço de Agendador
ResumeAll	Privilégios do Agendador	Editar Agendamento	Serviço de Agendador
ResumeSchedule	Privilégios do Agendador	Editar Agendamento	Serviço de Agendador
UpdateSchedule	Privilégios do Agendador	Editar Agendamento	Serviço de Agendador
UpdateService	Privilégios do Domínio	Gerenciar serviços	Serviço de Agendador

Comando infacmd sch	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
UpdateServiceProcess	Privilégios do Domínio	Gerenciar serviços	Serviço de Agendador
Atualizar	Privilégios do Domínio	Gerenciar serviços	Serviço de Agendador

## Comandos infacmd sql

Para executar comandos *infacmd sql*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio, privilégios de Serviço de Integração de Dados e permissões de objeto de domínio.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd sql*:

Comando infacmd sql	Grupo de Privilégio	Nome do Privilégio	Permissão para...
ExecuteSQL	-	-	Com base em objetos que você deseja acessar em sua instrução SQL
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	Administração de Aplicativo	Gerenciar Aplicativos	-
SetColumnPermissions	-	-	Conceder para o objeto
SetSQLDataServicePermissions	-	-	Conceder para o objeto
SetStoredProcedurePermissions	-	-	Conceder para o objeto
SetTablePermissions	-	-	Conceder para o objeto
StartSQLDataService	Administração de Aplicativo	Gerenciar Aplicativos	-

Comando infacmd sql	Grupo de Privilégio	Nome do Privilégio	Permissão para...
StopSQLDataService	Administração de Aplicativo	Gerenciar Aplicativos	-
UpdateColumnOptions	Administração de Aplicativo	Gerenciar Aplicativos	-
UpdateSQLDataServiceOptions	Administração de Aplicativo	Gerenciar Aplicativos	-
UpdateTableOptions	Administração de Aplicativo	Gerenciar Aplicativos	-

## Comandos infacmd wfs

Para executar comandos `infacmd wfs`, os usuários não exigem quaisquer privilégios ou permissões.

## Comandos pmcmd

Para executar os seguintes comandos `pmcmd`, os usuários devem ter os conjuntos relacionados de privilégios do Serviço do Repositório do PowerCenter e permissões de objeto de repositório do PowerCenter.

Quando o Serviço de Integração do PowerCenter é executado no modo de segurança, os usuários devem ter a função Administrador para o Serviço do Repositório do PowerCenter associado para executar os comandos a seguir:

- `aborttask`
- `abortworkflow`
- `getrunningsessionsdetails`
- `getservicedetails`
- `getsessionstatistics`
- `gettaskdetails`
- `getworkflowdetails`
- `recoverworkflow`
- `scheduleworkflow`
- `starttask`
- `startworkflow`
- `stoptask`
- `stopworkflow`
- `unscheduleworkflow`

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *pmcmd*:

Comando <i>pmcmd</i>	Grupo de Privilégio	Nome do Privilégio	Permissão
aborttask (iniciado pela própria conta de usuário)	-	-	Ler e Executar na pasta
aborttask (iniciado por outros usuários)	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta
abortworkflow (iniciado pela própria conta de usuário)	-	-	Ler e Executar na pasta
abortworkflow (iniciado por outros usuários)	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta
conectar	-	-	-
desconectar	-	-	-
sair	-	-	-
getrunningsessionsdetails	Objetos de Tempo de Execução	Monitorar	-
getservicedetails	Objetos de Tempo de Execução	Monitorar	Ler na pasta
getserviceproperties	-	-	-
getsessionstatistics	Objetos de Tempo de Execução	Monitorar	Ler na pasta
gettaskdetails	Objetos de Tempo de Execução	Monitorar	Ler na pasta
getworkflowdetails	Objetos de Tempo de Execução	Monitorar	Ler na pasta
ajuda	-	-	-
pingservice	-	-	-
recoverworkflow (iniciado pela própria conta de usuário)	Objetos de Tempo de Execução	Executar	Ler e Executar na pasta Ler e Executar no objeto de conexão Permissão no perfil do sistema operacional (se aplicável)
recoverworkflow (iniciado por outros usuários)	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta Ler e Executar no objeto de conexão Permissão no perfil do sistema operacional (se aplicável)

Comando pmcmd	Grupo de Privilégio	Nome do Privilégio	Permissão
scheduleworkflow	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta Ler e Executar no objeto de conexão Permissão no perfil do sistema operacional (se aplicável)
setfolder	-	-	Ler na pasta
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	Objetos de Tempo de Execução	Executar	Ler e Executar na pasta Ler e Executar no objeto de conexão Permissão no perfil do sistema operacional (se aplicável)
startworkflow	Objetos de Tempo de Execução	Executar	Ler e Executar na pasta Ler e Executar no objeto de conexão Permissão no perfil do sistema operacional (se aplicável)
stoptask (iniciado pela própria conta de usuário)	-	-	Ler e Executar na pasta
stoptask (iniciado por outros usuários)	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta
stopworkflow (iniciado pela própria conta de usuário)	-	-	Ler e Executar na pasta
stopworkflow (iniciado por outros usuários)	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta
unscheduleworkflow	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta
unsetfolder	-	-	Ler na pasta
versão	-	-	-
waittask	Objetos de Tempo de Execução	Monitorar	Ler na pasta
waitworkflow	Objetos de Tempo de Execução	Monitorar	Ler na pasta

# Comandos pmrep

Os usuários devem ter privilégio de acesso de Repository Manager para executar todos os comandos *pmrep* com exceção dos seguintes:

- Executar
- Criar
- Restaurar
- Atualizar
- Versão
- Ajuda

Para executar os seguintes comandos *pmrep*, os usuários devem ter um dos conjuntos relacionados de privilégios de domínio, privilégios de Serviço do Repositório do PowerCenter, permissões de objeto de domínio e permissões de objeto de repositório do PowerCenter.

Os usuários devem ser o proprietário do objeto ou ter a função Administrador para o Serviço do Repositório do PowerCenter para executar os comandos a seguir:

- AssignPermission
- ChangeOwner
- CreateQuery
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- DeleteQuery
- ModifyFolder (para alterar proprietário, configurar permissões, designar a pasta como compartilhada ou editar o nome ou a descrição da pasta)

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *pmrep*:

Comando pmrep	Grupo de Privilégios	Nome do Privilégio	Permissão
AddToDeploymentGroup	Objetos Globais	Gerenciar Grupos de Implantação	Ler na pasta original Ler e Gravar no grupo de implantação
ApplyLabel	-	-	Ler na pasta Ler e Executar no rótulo
AssignPermission	-	-	-
BackUp	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
ChangeOwner	-	-	-
CheckIn (para seus próprios check-outs)	Objetos de Design	Criar, Editar e Excluir	Ler e Gravar na pasta



Comando pmrep	Grupo de Privilégios	Nome do Privilégio	Permissão
CheckIn (para seus próprios check-outs)	Origens e Destinos	Criar, Editar e Excluir	Ler e Gravar na pasta
CheckIn (para seus próprios check-outs)	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta
CheckIn (para os check-outs de outros)	Objetos de Design	Gerenciar Versões	Ler e Gravar na pasta
CheckIn (para os check-outs de outros)	Origens e Destinos	Gerenciar Versões	Ler e Gravar na pasta
CheckIn (para os check-outs de outros)	Objetos de Tempo de Execução	Gerenciar Versões	Ler e Gravar na pasta
CleanUp	-	-	-
ClearDeploymentGroup	Objetos Globais	Gerenciar Grupos de Implantação	Ler e Gravar no grupo de implantação
Conectar	-	-	-
Criar	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
CreateConnection	Objetos Globais	Criar Conexões	-
CreateDeploymentGroup	Objetos Globais	Gerenciar Grupos de Implantação	-
CreateFolder	Pastas	Criar	-
CreateLabel	Objetos Globais	Criar Rótulos	-
CreateQuery	Objetos Globais	Criar Consultas	-
Excluir	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	Objetos de Design	Criar, Editar e Excluir	Ler e Gravar na pasta
DeleteObject	Origens e Destinos	Criar, Editar e Excluir	Ler e Gravar na pasta
DeleteObject	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta
DeleteQuery	-	-	-

Comando pmrep	Grupo de Privilégios	Nome do Privilégio	Permissão
DeployDeploymentGroup	Objetos Globais	Gerenciar Grupos de Implantação	Ler na pasta original Ler e Gravar na pasta de destino Ler e Executar no grupo de implantação
DeployFolder	Pastas	Copiar no repositório original Criar no repositório de destino	Ler na pasta
ExecuteQuery	-	-	Ler e Executar na consulta
Saída	-	-	-
FindCheckout	-	-	Ler na pasta
GetConnectionDetails	-	-	Ler no objeto de conexão
Ajuda	-	-	-
KillUserConnection	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
ListConnections	-	-	Ler no objeto de conexão
ListObjectDependencies	-	-	Ler na pasta
ListObjects	-	-	Ler na pasta
ListTablesBySess	-	-	Ler na pasta
ListUserConnections	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
ModifyFolder (para alterar proprietário, configurar permissões, designar a pasta como compartilhada ou editar o nome ou a descrição da pasta)	-	-	-
ModifyFolder (para alterar status)	Pastas	Gerenciar Versões	Ler e Gravar na pasta
Notificar	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
ObjectExport	-	-	Ler na pasta
ObjectImport	Objetos de Design	Criar, Editar e Excluir	Ler e Gravar na pasta
ObjectImport	Origens e Destinos	Criar, Editar e Excluir	Ler e Gravar na pasta

Comando pmrep	Grupo de Privilégios	Nome do Privilégio	Permissão
ObjectImport	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta
PurgeVersion	Objetos de Design	Gerenciar Versões	Ler e Gravar na pasta Ler, Gravar e Executar em consultas se você especificar um nome de consulta
PurgeVersion	Origens e Destinos	Gerenciar Versões	Ler e Gravar na pasta Ler, Gravar e Executar em consultas se você especificar um nome de consulta
PurgeVersion	Objetos de Tempo de Execução	Gerenciar Versões	Ler e Gravar na pasta Ler, Gravar e Executar em consultas se você especificar um nome de consulta
PurgeVersion (para limpar objetos no nível de pasta)	Pastas	Gerenciar Versões	Ler e Gravar na pasta
PurgeVersion (para limpar objetos no nível de repositório)	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
Registrar	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
RegisterPlugin	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
Restaurar	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
RollbackDeployment	Objetos Globais	Gerenciar Grupos de Implantação	Ler e Gravar na pasta de destino
Executar	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta Ler no objeto de conexão
TruncateLog	Objetos de Tempo de Execução	Gerenciar Execução	Ler e Executar na pasta
UndoCheckout (para seus próprios check-outs)	Objetos de Design	Criar, Editar e Excluir	Ler e Gravar na pasta
UndoCheckout (para seus próprios check-outs)	Origens e Destinos	Criar, Editar e Excluir	Ler e Gravar na pasta
UndoCheckout (para seus próprios check-outs)	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta

Comando pmrep	Grupo de Privilégios	Nome do Privilégio	Permissão
UndoCheckout (para check-outs de outros)	Objetos de Design	Gerenciar Versões	Ler e Gravar na pasta
UndoCheckout (para check-outs de outros)	Origens e Destinos	Gerenciar Versões	Ler e Gravar na pasta
UndoCheckout (para check-outs de outros)	Objetos de Tempo de Execução	Gerenciar Versões	Ler e Gravar na pasta
Cancelar registro	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
UnregisterPlugin	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
UpdateConnection	-	-	Ler e Gravar no objeto de conexão
UpdateEmailAddr	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta
UpdateSeqGenVals	Objetos de Design	Criar, Editar e Excluir	Ler e Gravar na pasta
UpdateSrcPrefix	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta
UpdateStatistics	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
UpdateTargPrefix	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta
Atualizar	Administração de Domínio	Gerenciar Serviços	Permissão no Serviço do Repositório do PowerCenter
Validar	Objetos de Design	Criar, Editar e Excluir	Ler e Gravar na pasta
Validar	Objetos de Tempo de Execução	Criar, Editar e Excluir	Ler e Gravar na pasta
Versão	-	-	-

## APÊNDICE B

# Funções personalizadas

Este apêndice inclui os seguintes tópicos:

- [Função Personalizada do Serviço Analyst, 245](#)
- [Funções Personalizadas do Serviço do Metadata Manager, 246](#)
- [Função Personalizada do Operador, 248](#)
- [Funções Personalizadas do Serviço do Repositório do PowerCenter, 249](#)
- [Regras personalizadas do Test Data Manager, 250](#)

## Função Personalizada do Serviço Analyst

O Consumidor do Business Glossary do Serviço Analyst é uma função personalizada do Serviço Analyst.

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada Consumidor do Business Glossary do Serviço Analyst:

Grupo de Privilégios	Nome do Privilégio
Acesso a Espaços de Trabalho	Espaço de trabalho do glossário

# Funções Personalizadas do Serviço do Metadata Manager

Funções personalizadas do Serviço do Metadata Manager incluem as funções de Usuário Avançado do Metadata Manager, Usuário Básico do Metadata Manager e Usuário Intermediário do Metadata Manager.

## Usuário Avançado do Metadata Manager

A tabela a seguir lista os privilégios padrão atribuídos à função personalizada de usuário avançado do Metadata Manager:

Grupo de Privilégio	Nome do Privilégio
Catálogo	<ul style="list-style-type: none"><li>- Compartilhar Atalhos</li><li>- Exibir Linhagem</li><li>- Exibir Catálogos Relacionados</li><li>- Exibir Relatórios</li><li>- Exibir Resultados do Perfil</li><li>- Exibir Catálogo</li><li>- Exibir Relacionamentos</li><li>- Gerenciar Relacionamentos</li><li>- Exibir Comentários</li><li>- Publicar Comentários</li><li>- Excluir Comentários</li><li>- Exibir Links</li><li>- Gerenciar Links</li><li>- Exibir Glossário</li><li>- Gerenciar Objetos</li></ul>
Carregar	<ul style="list-style-type: none"><li>- Exibir Recurso</li><li>- Carregar Recurso</li><li>- Gerenciar Agendamento</li><li>- Limpar Metadados</li><li>- Gerenciar Recurso</li></ul>
Modelo	<ul style="list-style-type: none"><li>- Exibir Modelo</li><li>- Gerenciar Modelo</li><li>- Exportar/Importar Modelos</li></ul>
Segurança	Gerenciar Permissões do Catálogo

## Usuário Básico do Metadata Manager

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada Usuário Básico do Metadata Manager:

Grupo de Privilégio	Nome do Privilégio
Catálogo	<ul style="list-style-type: none"><li>- Exibir Linhagem</li><li>- Exibir Catálogos Relacionados</li><li>- Exibir Catálogo</li><li>- Exibir Relacionamentos</li><li>- Exibir Comentários</li><li>- Exibir Links</li></ul>
Modelo	Exibir Modelo

## Usuário Intermediário do Metadata Manager

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada Usuário Intermediário do Metadata Manager:

Grupo de Privilégio	Nome do Privilégio
Catálogo	<ul style="list-style-type: none"><li>- Exibir Linhagem</li><li>- Exibir Catálogos Relacionados</li><li>- Exibir Relatórios</li><li>- Exibir Resultados do Perfil</li><li>- Exibir Catálogo</li><li>- Exibir Relacionamentos</li><li>- Exibir Comentários</li><li>- Publicar Comentários</li><li>- Excluir Comentários</li><li>- Exibir Links</li><li>- Gerenciar Links</li><li>- Exibir Glossário</li></ul>
Carregar	<ul style="list-style-type: none"><li>- Exibir Recurso</li><li>- Carregar Recurso</li></ul>
Modelo	Exibir Modelo

# Função Personalizada do Operador

A função personalizada do Operador inclui privilégios para gerenciar, programar e monitorar serviços de aplicativo.

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada Operador do

Grupo de Privilégios	Nome do Privilégio
Administração de Aplicativo	Gerenciar Aplicativos
Administração de Domínio	Gerenciar Execução do Serviço
Administração do Serviço de Repositório do Modelo	Gerenciar Desenvolvimento Baseado em Equipe
Monitoramento	<p>O grupo de privilégio Monitoramento inclui os seguintes privilégios:</p> <ul style="list-style-type: none"><li>- Exibição: Exibir Trabalhos e Outros Usuários</li><li>- Exibição: Exibir Estatísticas</li><li>- Exibição: Exibir Relatórios</li><li>- Monitoramento de Acesso: Acesso com a Ferramenta Analyst</li><li>- Monitoramento de Acesso: Acesso com a Developer Tool</li><li>- Monitoramento de Acesso: Acesso com a Ferramenta Administrator</li><li>- Executar Ações nas Tarefas</li></ul> <p><b>Nota:</b> Em um domínio que usa a autenticação Kerberos, os usuários também devem ter a função de Administrador do Serviço de Repositório do Modelo que está configurado para monitoramento.</p>
Agendador	<p>O grupo de privilégio Agendador inclui os seguintes privilégios:</p> <ul style="list-style-type: none"><li>- Gerenciar Trabalhos Agendados: Criar Agendamento</li><li>- Gerenciar Trabalhos Agendados: Excluir Agendamento</li><li>- Gerenciar Trabalhos Agendados: Editar Agendamento</li><li>- Gerenciar Trabalhos Agendados: Exibir Agendamentos</li></ul>
Ferramentas	Acessar o Informatica Administrator



# Funções Personalizadas do Serviço do Repositório do PowerCenter

As funções personalizadas do Serviço do Repositório do PowerCenter incluem o Administrador de Conexão do PowerCenter, o Desenvolvedor do PowerCenter, o Operador do PowerCenter e o Administrador de Pasta do Repositório do PowerCenter.

## Administrador de Conexão do PowerCenter

A tabela a seguir lista os privilégios padrão atribuídos a função personalizada do administrador de conexão do PowerCenter:

Grupo de Privilégio	Nome do Privilégio
Ferramentas	Acessar o Workflow Manager
Objetos Globais	Criar Conexões

## Desenvolvedor do PowerCenter

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada Desenvolvedor do PowerCenter:

Grupo de Privilégio	Nome do Privilégio
Ferramentas	<ul style="list-style-type: none"><li>- Acessar o Designer</li><li>- Acessar o Workflow Manager</li><li>- Acessar o Workflow Monitor</li></ul>
Objetos de Design	<ul style="list-style-type: none"><li>- Criar, Editar e Excluir</li><li>- Gerenciar Versões</li></ul>
Origens e Destinos	<ul style="list-style-type: none"><li>- Criar, Editar e Excluir</li><li>- Gerenciar Versões</li></ul>
Objetos de Tempo de Execução	<ul style="list-style-type: none"><li>- Criar, Editar e Excluir</li><li>- Executar</li><li>- Gerenciar Versões</li><li>- Monitorar</li></ul>

## Operador do PowerCenter

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada Operador do PowerCenter:

Grupo de Privilégio	Nome do Privilégio
Ferramentas	Acessar o Workflow Monitor
Objetos de Tempo de Execução	<ul style="list-style-type: none"><li>- Executar</li><li>- Gerenciar Execução</li><li>- Monitorar</li></ul>

### Administrador da Pasta de Repositório do PowerCenter

A tabela a seguir lista os privilégios padrão atribuídos ao administrador da pasta de repositório do PowerCenter função personalizada:

Grupo de Privilégio	Nome do Privilégio
Ferramentas	Acessar o Repository Manager
Pastas	<ul style="list-style-type: none"><li>- Copiar</li><li>- Criar</li><li>- Gerenciar Versões</li></ul>
Objetos Globais	<ul style="list-style-type: none"><li>- Gerenciar Grupos de Implantação</li><li>- Executar Grupos de Implantação</li><li>- Criar Rótulos</li><li>- Criar Consultas</li></ul>

## Regras personalizadas do Test Data Manager

As funções personalizadas do Test Data Manager incluem Administrador de Dados de Teste, Desenvolvedor de Dados de Teste, DBA do Projeto de Dados de Teste, Desenvolvedor do Projeto de Dados de Teste, Proprietário do Projeto de Dados de Teste, Gerente de Riscos de Dados de Teste, Especialista de Dados de Teste e Engenheiro de Teste.

### Administrador de Dados de Teste

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada do Administrador de Dados de Teste:

Grupo de Privilégios	Nome do Privilégio
Projetos	Auditar projeto
Administração	<ul style="list-style-type: none"><li>- Exibir Conexões</li><li>- Gerenciar Conexões</li><li>- Gerenciar Preferências</li></ul>

## Desenvolvedor de Dados de Teste

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada do Desenvolvedor de Dados de Teste:

Grupo de Privilégios	Nome do Privilégio
Diretivas	<ul style="list-style-type: none"><li>- Exibir Diretivas</li><li>- Gerenciar Diretivas</li></ul>
Domínios de Dados	<ul style="list-style-type: none"><li>- Exibir Domínios de Dados</li><li>- Gerenciar Domínios de Dados</li></ul>
Projetos	Auditar projeto

## DBA do Projeto de Dados de Teste

A tabela a seguir lista os privilégios padrão atribuídos à função personalizada DBA do Projeto de Dados de Teste:

Grupo de Privilégios	Nome do Privilégio
Projetos	<ul style="list-style-type: none"><li>- Exibir Projeto</li><li>- Executar Projeto</li><li>- Monitorar Projeto</li><li>- Auditar projeto</li></ul>
Administração	<ul style="list-style-type: none"><li>- Exibir Conexões</li><li>- Gerenciar Conexões</li></ul>

## Desenvolvedor do Projeto de Dados de Teste

A tabela a seguir lista os privilégios padrão atribuídos à função personalizada Desenvolvedor do Projeto de Dados de Teste:

Grupo de Privilégios	Nome do Privilégio
Diretivas	Exibir Diretivas
Domínios de Dados	Exibir Domínios de Dados
Projetos	<ul style="list-style-type: none"><li>- Exibir Projeto</li><li>- Descobrir Projeto</li><li>- Executar Projeto</li><li>- Monitorar Projeto</li><li>- Auditar projeto</li><li>- Importar Metadados</li></ul>
Mascaramento de dados	<ul style="list-style-type: none"><li>- Exibir Mascaramento de Dados</li><li>- Gerenciar Mascaramento de Dados</li></ul>

Grupo de Privilégios	Nome do Privilégio
Subconjunto de Dados	<ul style="list-style-type: none"> <li>- Exibir Subconjunto de Dados</li> <li>- Gerenciar Subconjunto de Dados</li> </ul>
Administração	<ul style="list-style-type: none"> <li>- Exibir Conexões</li> <li>- Gerenciar Conexões</li> </ul>

### Proprietário do Projeto de Dados de Teste

A tabela a seguir lista os privilégios padrão atribuídos à função personalizada Proprietário do Projeto de Dados de Teste:

Grupo de Privilégios	Nome do Privilégio
Diretivas	Exibir Diretivas
Domínios de Dados	Exibir Domínios de Dados
Projetos	<ul style="list-style-type: none"> <li>- Exibir Projeto</li> <li>- Gerenciar Projeto</li> <li>- Descobrir Projeto</li> <li>- Executar Projeto</li> <li>- Monitorar Projeto</li> <li>- Auditar projeto</li> <li>- Importar Metadados</li> </ul>
Mascaramento de dados	<ul style="list-style-type: none"> <li>- Exibir Mascaramento de Dados</li> <li>- Gerenciar Mascaramento de Dados</li> </ul>
Subconjunto de Dados	<ul style="list-style-type: none"> <li>- Exibir Subconjunto de Dados</li> <li>- Gerenciar Subconjunto de Dados</li> </ul>
Administração	<ul style="list-style-type: none"> <li>- Exibir Conexões</li> <li>- Gerenciar Conexões</li> </ul>

### Gerente de Riscos de Dados de Teste

A tabela a seguir lista os privilégios padrão atribuídos à função personalizada Gerente de Riscos de Dados de Teste:

Grupo de Privilégios	Nome do Privilégio
Diretivas	Exibir Diretivas
Domínios de Dados	Exibir Domínios de Dados
Projetos	Auditar projeto

## Especialista de Dados de Teste

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada do Especialista de Test Data:

Grupo de Privilégios	Nome do Privilégio
Diretivas	Exibir Diretivas
Domínios de Dados	<ul style="list-style-type: none"><li>- Exibir Domínios de Dados</li><li>- Gerenciar Domínios de Dados</li></ul>
Projetos	<ul style="list-style-type: none"><li>- Exibir Projeto</li><li>- Gerenciar Projeto</li><li>- Descobrir Projeto</li><li>- Executar Projeto</li><li>- Monitorar Projeto</li><li>- Auditar projeto</li><li>- Importar Metadados</li></ul>
Mascaramento de dados	<ul style="list-style-type: none"><li>- Exibir Mascaramento de Dados</li><li>- Gerenciar Mascaramento de Dados</li></ul>
Subconjunto de Dados	<ul style="list-style-type: none"><li>- Exibir Subconjunto de Dados</li><li>- Gerenciar Subconjunto de Dados</li></ul>
Administração	<ul style="list-style-type: none"><li>- Exibir Conexões</li><li>- Gerenciar Conexões</li></ul>

## Engenheiro de Teste

A seguinte tabela lista os privilégios padrão atribuídos à função personalizada Engenheiro de Teste:

Grupo de Privilégios	Nome do Privilégio
Projetos	<ul style="list-style-type: none"><li>- Exibir Projeto</li><li>- Monitorar Projeto</li></ul>

# ÍNDICE

## A

- Administrador
  - função [180](#)
- administrador de domínio
  - descrição [121](#)
- administrador padrão
  - descrição [121](#)
  - modificando [121](#)
  - senhas, alterando [121](#)
- administradores
  - cliente de aplicativo [122](#)
  - domínio [121](#)
  - padrão [121](#)
- alterando
  - senha da conta de usuário [117](#)
- aplicativo
  - permissões [197](#)
- arquivo de truststore cacerts [31](#)
- as
  - permissões por comando [214](#)
  - privilegios por comando [214](#)
- atividade de logon
  - exibindo [128](#)
- autenticação
  - Kerberos [20](#)
  - LDAP [20](#), [26](#), [110](#)
  - nativa [19](#), [110](#)
  - Service Manager [110](#)
- autenticação Kerberos
  - descrição [20](#)
- Autenticação Kerberos
  - Arquivo de formato de SPN e keytab [46](#)
  - autenticação de realm cruzado [36](#)
  - contas de entidade de segurança de serviço [41](#)
  - keytab [42](#)
  - nível de nó [37](#)
  - nível de processo [37](#)
  - nome da entidade de segurança de serviço [42](#)
  - Sincronização LDAP [59](#)
  - visão geral [33](#), [34](#)
- autenticação LDAP
  - Azure Active Directory [25](#)
  - certificado SSL autoassinado [31](#)
  - configurando [26](#)
  - descrição [20](#), [110](#)
  - grupos aninhados [31](#)
  - serviços de diretório [26](#)
  - serviços de diretório com suporte [24](#)
- autenticação nativa
  - descrição [19](#), [110](#)
- autorização
  - Gerenciador de Serviços [111](#)
  - Serviço de Integração de Dados [111](#)
  - Serviço de Repositório do Modelo [111](#)
  - Serviço do Metadata Manager [111](#)

- autorização ()
  - Serviço do Repositório do PowerCenter [111](#)
  - serviços de aplicativo [111](#)

## C

- Carregar grupo de privilégio
  - descrição [158](#)
- certificado SSL
  - autenticação LDAP [31](#)
- Cliente do PowerCenter
  - administrador [122](#)
- cluster
  - permissões por comando [215](#)
  - privilegios por comando [215](#)
- conexões
  - permissões [194](#)
  - permissões padrão [195](#)
  - tipos de permissão [195](#)
- configuração de cliente
  - domínio seguro [87](#)
- configurações do LDAP
  - excluindo [31](#)
- consultas de objeto
  - privilegios para o PowerCenter [172](#)
- contas
  - alterando a senha [117](#)
- contas de usuário
  - alterando a senha [117](#)
  - ativando [125](#)
  - criadas durante a instalação [121](#)
  - padrão [121](#)
  - visão geral [121](#)
- convertUserActivityLog
  - logs de atividade do usuário [128](#)
- Criar Tabelas de Referência
  - privilegio [155](#)

## D

- Data Integration Service
  - privilegios [155](#)
- descrição do grupo
  - caracteres inválidos [131](#)
- descrição do usuário
  - caracteres inválidos [123](#)
- destinos
  - privilegios [166](#)
- dis
  - permissões por comando [216](#)
  - privilegios por comando [216](#)
- domínio
  - administrador [121](#)
  - Função Administrador [181](#)

- domínio ()
  - privilegios [146](#)
  - privilegios de administração [147](#)
  - privilegios de administração de segurança [146](#)
  - segurança do usuário [117](#)
  - sincronização de usuário [111](#)
  - usuários com privilegios [185](#)
- domínio de segurança LDAP
  - descrição [20](#)
- domínio de segurança nativo
  - descrição [19](#)
- domínio Informatica
  - permissões [117](#)
  - privilegios [117](#)
  - segurança do usuário [117](#)
  - usuários, gerenciando [123](#)
- domínio seguro
  - configuração de cliente [87](#)
- domínios de segurança
  - exclusão de LDAP [31](#)
  - LDAP [20](#)
  - nativa [19](#)

## E

- Editar Metadados de Tabela de Referência
  - privilegio [155](#)
- es
  - permissões por comando [218](#)
  - privilegios por comando [218](#)
- esquema virtual
  - permissões [199](#)
  - permissões herdadas [199](#)

## F

- filtros
  - getUserActivityLog [129](#)
- filtros de pesquisa
  - permissões [190](#)
- fluxo de trabalho
  - permissões [197](#)
  - permissões herdadas [197](#)
- funções
  - Administrador [180](#)
  - atribuindo [183](#)
  - descrição [145](#)
  - gerenciando [180](#)
  - personalizadas [182](#)
  - solução de problemas [185](#)
  - visão geral [114](#)
- funções definidas pelo sistema
  - Administrador [180](#)
  - atribuindo aos usuários e grupos [183](#)
  - descrição [180](#)
- funções personalizadas
  - atribuindo aos usuários e grupos [183](#)
  - criando [182](#)
  - descrição [180](#), [182](#)
  - editando [182](#)
  - excluindo [183](#)
  - Operador [248](#)
  - privilegios, atribuindo [183](#)
  - Serviço Analyst [245](#)
  - Serviço do Metadata Manager [246](#)
  - Serviço do Repositório do PowerCenter [249](#)

## G

- Gerenciador de Serviços
  - autorização [111](#)
  - sign-on único [111](#)
- gerenciamento de conta
  - visão geral [115](#)
- getUserActivityLog
  - filtros [129](#)
  - logs de atividade do usuário [128](#)
- grades
  - permissões [190](#)
- Grupo de privilegio Administração de segurança
  - descrição [146](#)
- Grupo de privilegio da Administração de Nuvem
  - domínio [153](#)
- Grupo de privilegio de Objetos em tempo de Execução
  - descrição [168](#)
- Grupo de privilegio de Objetos Globais
  - descrição [172](#)
- Grupo de privilegio Ferramentas
  - domínio [153](#)
  - Serviço do Repositório do PowerCenter [161](#)
- Grupo de privilegio Modelo
  - descrição [159](#)
- Grupo de privilegio Monitoramento
  - domínio [151](#)
- Grupo de privilegio Objetos de Design
  - descrição [163](#)
- Grupo de privilegio Origens e Destinos
  - descrição [166](#)
- Grupo de privilegio Pastas
  - descrição [162](#)
- Grupo de privilegio Procurar
  - descrição [157](#)
- Grupo de privilegio Segurança
  - descrição [159](#)
- Grupo de privilegios Administração de Domínio
  - descrição [147](#)
- Grupo Todos
  - descrição [120](#)
- grupos
  - caracteres inválidos [131](#)
  - definir Todos como padrão [120](#)
  - funções, atribuindo [183](#)
  - gerenciando [131](#)
  - grupo pai [131](#)
  - nome inválido [131](#)
  - privilegios, atribuindo [183](#)
  - sincronização [111](#)
  - visão geral [113](#)
- grupos aninhados
  - autenticação LDAP [31](#)
  - serviço de diretório LDAP [31](#)
- grupos de implantação
  - privilegios para o PowerCenter [172](#)
- grupos de privilegio
  - Administração do Informatica Cloud [153](#)
- Grupos de privilegio
  - descrição [145](#)
- grupos de privilegios
  - Administração de domínio [147](#)
  - Administração de segurança [146](#)
  - Carregar [158](#)
  - Ferramentas [153](#), [161](#)
  - Modelo [159](#)
  - Monitoramento [151](#)
  - Objetos de Design [163](#)

- grupos de privilégios (
  - Objetos de Tempo de Execução [168](#)
  - Objetos Globais [172](#)
  - Origens e Destinos [166](#)
  - Pastas [162](#)
  - Procurar [157](#)
  - Segurança [159](#)
- Grupos LDAP
  - gerenciando [131](#)
  - importando [26](#)
- grupos nativos
  - adicionando [131](#)
  - editando [132](#)
  - excluindo [133](#)
  - gerenciando [131](#)
  - movendo para outro grupo [132](#)
  - usuários, atribuindo [124](#)
- grupos pai
  - descrição [131](#)

## I

- Informatica Administrator
  - guias, exibindo [109](#)
  - Navegador [113](#)
  - Página de segurança [112](#)
  - pesquisando [112](#)
  - visão geral [109](#)
- Informatica Analyst
  - administrador [122](#)
- Informatica Developer
  - administrador [122](#)
- ipc
  - permissões por comando [218](#)
  - privilégios por comando [218](#)
- isp
  - permissões por comando [218](#)
  - privilégios por comando [218](#)

## L

- licenças
  - permissões [190](#)
- logon único
  - configurando [70](#)
  - visão geral [67](#)
- logs de atividade do usuário
  - códigos de atividade [128](#)
  - convertUserActivityLog [128](#)
  - formatos de saída [128](#)
  - getUserActivityLog [128](#)

## M

- mapeamento
  - permissões [197](#)
  - permissões herdadas [197](#)
- mas
  - permissões por comando [228](#)
  - privilégios por comando [228](#)
- memória do sistema
  - aumentando [127](#)
- Metadata Manager
  - administrador [122](#)

- mrs
  - permissões por comando [229](#)
  - privilégios por comando [229](#)
- ms
  - permissões por comando [232](#)
  - privilégios por comando [232](#)

## N

- Navegador
  - Página de segurança [113](#)
- nome inválido
  - conta de usuário [123](#)
  - grupos [131](#)
- nós
  - permissões [190](#)

## O

- objetos de conexão
  - privilégios para o PowerCenter [172](#)
- objetos de design
  - descrição [163](#)
  - privilégios [163](#)
- objetos de domínio
  - permissões [190](#)
- objetos em tempo de execução
  - descrição [168](#)
  - privilégios [168](#)
- objetos globais
  - privilégios para o PowerCenter [172](#)
- operação do serviço da Web
  - permissões [203](#)
- Operador}
  - funções personalizadas [248](#)
- operating system profile
  - managing [133](#)
- origens
  - privilégios [166](#)

## P

- pacotes de criptografia
  - configurando [97](#)
- Página de segurança
  - Informatica Administrator [112](#)
  - Navegador [113](#)
- pastas
  - permissões [190](#)
  - privilégios [162](#)
- perfil do sistema operacional
  - criando [137](#)
  - editando [133](#)
  - excluindo [140](#)
  - padrão [139](#)
  - propriedades, Serviço de Acesso a Metadados [137](#)
  - propriedades, Serviço de Integração de Dados [133](#), [135](#)
  - propriedades, Serviço de Integração do PowerCenter [133](#)
- perfis do sistema operacional
  - permissões [190](#), [193](#)
  - visão geral [115](#)
- permissão direta
  - descrição [189](#)
- permissão efetiva
  - descrição [189](#)



- permissão herdada
  - descrição [189](#)
- permissões
  - aplicativo [197](#)
  - comandos de cluster [215](#)
  - comandos de sql [236](#)
  - comandos dis [216](#)
  - comandos do ipc [218](#)
  - comandos do isp [218](#)
  - comandos mas [228](#)
  - comandos mrs [229](#)
  - comandos MS [232](#)
  - comandos pmcmd [237](#)
  - comandos pmrep [240](#)
  - comandos ps [232](#)
  - comandos pwx [233](#)
  - Comandos rms [234](#)
  - comandos rtm [235](#)
  - comandos tools [232](#)
  - comandos wfs [237](#)
  - como comandos [214](#)
  - conexões [194](#)
  - descrição [188](#)
  - diretas [189](#)
  - efetivas [189](#)
  - esquema virtual [199](#)
  - filtros de pesquisa [190](#)
  - fluxo de trabalho [197](#)
  - grades [190](#)
  - herdado [189](#)
  - licenças [190](#)
  - mapeamento [197](#)
  - nós [190](#)
  - objetos de domínio [190](#)
  - operação do serviço da Web [203](#)
  - pastas [190](#)
  - perfis do sistema operacional [190](#), [193](#)
  - procedimento armazenado virtual [199](#)
  - serviço da Web [203](#)
  - serviço de dados SQL [199](#)
  - serviços de aplicativo [190](#)
  - tabela virtual [199](#)
  - tipos [189](#)
  - trabalhando com privilégios [188](#)
- Permissões
  - Comandos es [218](#)
  - Comandos sch [235](#)
- permissões de domínio
  - diretas [189](#)
  - efetivas [189](#)
  - herdado [189](#)
- pmcmd
  - permissões por comando [237](#)
  - privilégios por comando [237](#)
- pmrep
  - permissões por comando [240](#)
  - privilégios por comando [240](#)
- privilégios
  - administração de domínio [147](#)
  - administração de segurança [146](#)
  - Administração do Informatica Cloud [153](#)
  - atribuindo [183](#)
  - comandos de cluster [215](#)
  - comandos de sql [236](#)
  - comandos dis [216](#)
  - comandos do ipc [218](#)
  - comandos do isp [218](#)
  - Comandos es [218](#)
- privilégios ()
  - comandos mas [228](#)
  - comandos mrs [229](#)
  - comandos MS [232](#)
  - comandos pmcmd [237](#)
  - comandos pmrep [240](#)
  - comandos ps [232](#)
  - comandos pwx [233](#)
  - Comandos rms [234](#)
  - comandos rtm [235](#)
  - Comandos sch [235](#)
  - comandos tools [232](#)
  - comandos wfs [237](#)
  - como comandos [214](#)
  - Data Integration Service [155](#)
  - descrição [144](#)
  - destinos [166](#)
  - domínio [146](#)
  - ferramentas de domínio [153](#)
  - Ferramentas do serviço de repositório do PowerCenter [161](#)
  - herdado [184](#)
  - monitoramento [151](#)
  - objetos de design [163](#)
  - objetos em tempo de execução [168](#)
  - Objetos globais do PowerCenter [172](#)
  - origens [166](#)
  - pastas [162](#)
  - programas de linha de comando [214](#)
  - Serviço Analyst [153](#)
  - Serviço de Agendador [176](#)
  - Serviço de Repositório do Modelo [159](#)
  - Serviço de Repositório do PowerCenter [160](#)
  - Serviço do Agente de Log do PowerExchange [175](#)
  - Serviço do Gerenciamento de Conteúdo [155](#)
  - Serviço do Metadata Manager [156](#)
  - Serviço do Ouvinte do PowerExchange [175](#)
  - solução de problemas [185](#)
  - trabalhando com permissões [188](#)
- Privilégios do Serviço do Metadata Manager
  - Carregar grupo de privilégio [158](#)
  - Grupo de privilégio Modelo [159](#)
  - Grupo de privilégio Procurar [157](#)
  - Grupo de privilégio Segurança [159](#)
- privilégios herdados
  - descrição [184](#)
- procedimento armazenado virtual
  - permissões [199](#)
  - permissões herdadas [199](#)
- programas de linha de comando
  - privilégios [214](#)
- provedor de identidade
  - configurando para logon único [71](#)
- ps
  - permissões por comando [232](#)
  - privilégios por comando [232](#)
- pwx
  - permissões por comando [233](#)
  - privilégios por comando [233](#)

## R

- recurso de serviço da Web
  - permissões [203](#)
- relatórios de auditoria
  - descrição [207](#)
  - para grupos [212](#)
  - para usuários [211](#), [212](#)

- relatórios de auditoria ()
  - visão geral [116](#)
- rms
  - permissões por comando [234](#)
  - privilegios por comando [234](#)
- rótulos
  - privilegios para o PowerCenter [172](#)
- rtm
  - permissões por comando [235](#)
  - privilegios por comando [235](#)

## S

- sch
  - permissões por comando [235](#)
  - privilegios por comando [235](#)
- Seção Pesquisa
  - Informatica Administrator [112](#)
- Security Assertion Markup Language (SAML)
  - asserção criptografada [75](#)
  - asserção, assinada ou criptografada [72](#)
  - assinatura de solicitação [72](#), [73](#)
  - habilitando em nós de gateway [72](#)
  - habilitando no domínio [71](#)
  - resposta assinada [72](#), [74](#)
  - suporte para [67](#)
- segurança
  - funções [145](#)
  - permissões [117](#)
  - privilegios [117](#), [144](#), [146](#)
  - senhas [123](#)
- segurança de nível de coluna
  - restringindo colunas [202](#)
- Segurança do PowerCenter
  - gerenciando [112](#)
- segurança do usuário
  - descrição [110](#)
- senha
  - alterando para uma conta de usuário [117](#)
- senhas
  - alterando para administrador padrão [121](#)
  - requisitos [123](#)
  - usuários nativos [123](#)
- Service Manager
  - autenticação [110](#)
- Serviço Analyst
  - funções personalizadas [245](#)
  - privilegios [153](#)
- serviço da Web
  - permissões [203](#)
  - tipos de permissão [203](#)
- Serviço de Agendador
  - privilegios [176](#)
- serviço de dados SQL
  - permissões [199](#)
  - permissões herdadas [199](#)
  - tipos de permissão [199](#)
- serviço de diretório LDAP
  - grupos aninhados [31](#)
- Serviço de Integração de Dados
  - autorização [111](#)
- Serviço de Repositório do Modelo
  - autorização [111](#)
  - privilegios [159](#)
  - sincronização de usuário [111](#)
  - usuários com privilegios [185](#)

- Serviço de Repositório do PowerCenter
  - privilegios [160](#)
  - usuários com privilegios [185](#)
- Serviço do Agente de Log do PowerExchange
  - privilegios [175](#)
- Serviço do Gerenciamento de Conteúdo
  - privilegios [155](#)
- Serviço do Metadata Manager
  - autorização [111](#)
  - funções personalizadas [246](#)
  - privilegios [156](#)
  - sincronização de usuário [111](#)
  - usuários com privilegios [185](#)
- Serviço do Ouvinte do PowerExchange
  - privilegios [175](#)
- Serviço do Repositório do PowerCenter
  - autorização [111](#)
  - Função Administrador [181](#)
  - funções personalizadas [249](#)
  - sincronização de usuário [111](#)
- serviços de aplicativo
  - autorização [111](#)
  - permissões [190](#)
  - sincronização de usuário [111](#)
- sign-on único
  - descrição [111](#)
- sincronização
  - usuários [111](#)
  - Usuários LDAP [26](#)
- sql
  - permissões por comando [236](#)
  - privilegios por comando [236](#)

## T

- tabela virtual
  - permissões [199](#)
  - permissões herdadas [199](#)
- Test Data Manager
  - administrador [122](#)
- tools
  - permissões por comando [232](#)
  - privilegios por comando [232](#)

## U

- UpdateColumnOptions
  - substituindo valores de colunas [202](#)
- usuários
  - atribuindo a grupos [124](#)
  - caracteres inválidos [123](#)
  - funções, atribuindo [183](#)
  - gerenciando [123](#)
  - grande número de [127](#)
  - memória do sistema [127](#)
  - nome inválido [123](#)
  - privilegios, atribuindo [183](#)
  - sincronização [111](#)
  - visão geral [114](#)
- Usuários LDAP
  - ativando [125](#)
  - atribuindo a grupos [125](#)
  - gerenciando [123](#)
  - importando [26](#)
- usuários nativos
  - adicionando [123](#)

usuários nativos ()  
ativando [125](#)  
atribuindo a grupos [124](#)  
editando [124](#)  
excluindo [125](#)  
gerenciando [123](#)  
senhas [123](#)  
utilitário keytool [31](#)

## V

variáveis de ambiente  
INFA\_TRUSTSTORE [87](#)  
INFA\_TRUSTSTORE\_PASSWORD [87](#)

## W

wfs  
permissões por comando [237](#)  
privilégios por comando [237](#)