



Informatica®

10.1.1

Guia de Segurança

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.

Este produto inclui software desenvolvido pela Apache Software Foundation (<http://www.apache.org/>) e/ou outros softwares licenciados nas várias versões da Licença Apache (a "Licença"). Você pode obter uma cópia dessas Licenças em <http://www.apache.org/licenses/>. A menos que exigido pela legislação aplicável ou concordado por escrito, o software distribuído em conformidade com estas Licenças é fornecido "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA OU CONDIÇÃO DE QUALQUER TIPO, seja expressa ou implícita. Consulte as Licenças para conhecer as limitações e as permissões que regulam o idioma específico de acordo com as Licenças.

Este produto inclui software desenvolvido pela Mozilla (<http://www.mozilla.org/>), direitos autorais de software de The JBoss Group, LLC; todos os direitos reservados; software copyright © 1999-2006 de Bruno Lowagie e Paulo Soares e outros produtos de software licenciados sob a Licença Pública GNU Lesser General Public License Agreement, que pode ser encontrada em <http://www.gnu.org/licenses/gpl.html>. Os materiais são fornecidos gratuitamente pela Informatica, no estado em que se encontram, sem garantia de qualquer tipo, explícita nem implícita, incluindo, mas não limitando-se, as garantias implicadas de comerciabilidade e adequação a um determinado propósito.

O produto inclui software ACE(TM) e TAO(TM) com copyright de Douglas C. Schmidt e seu grupo de pesquisa na Washington University, University of California, Irvine e Vanderbilt University. Copyright (©) 1993-2006, todos os direitos reservados.

Este produto inclui o software desenvolvido pelo OpenSSL Project para ser usado no kit de ferramentas OpenSSL (copyright The OpenSSL Project. Todos os direitos reservados) e a redistribuição deste software está sujeita aos termos disponíveis em <http://www.openssl.org> e <http://www.openssl.org/source/license.html>.

Este produto inclui o software Curl com o Copyright 1996-2013, Daniel Stenberg, <daniel@haxx.se>. Todos os direitos reservados. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em <http://curl.haxx.se/docs/copyright.html>. É permitido usar, copiar, modificar e distribuir este software com qualquer objetivo, com ou sem taxa, desde que a nota de direitos autorais acima e esta nota de permissão apareçam em todas as cópias.

O produto inclui software copyright 2001-2005 (©) MetaStuff, Ltd. Todos os direitos reservados. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em <http://www.dom4j.org/license.html>.

O produto inclui o copyright de software © 2004-2007, The Dojo Foundation. Todos os direitos reservados. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em <http://dojotoolkit.org/license>.

Este produto inclui o software ICU com o copyright International Business Machines Corporation e outros. Todos os direitos reservados. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em <http://source.icu-project.org/repos/icu/icu/trunk/license.html>.

Este produto inclui o copyright de software © 1996-2006 Per Bothner. Todos os direitos reservados. O direito de usar tais materiais é estabelecido na licença que pode ser encontrada em <http://www.gnu.org/software/kawa/Software-License.html>.

Este produto inclui o software OSSP UUID com Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 e OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em <http://www.opensource.org/licenses/mit-license.php>.

Este produto inclui software desenvolvido pela Boost (<http://www.boost.org/>) ou sob a licença de software Boost. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em http://www.boost.org/LICENSE_1_0.txt.

Este produto inclui software copyright © 1997-2007 University of Cambridge. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em <http://www.pcre.org/license.txt>.

Este produto inclui o copyright de software © 2007 The Eclipse Foundation. Todos os direitos reservados. As permissões e as limitações relativas a este software estão sujeitas aos termos disponíveis em <http://www.eclipse.org/org/documents/epl-v10.php> e em <http://www.eclipse.org/org/documents/edl-v10.php>.

Este produto inclui softwares licenciados de acordo com os termos disponíveis em <http://www.tcl.tk/software/tcltk/license.html>, <http://www.bosrup.com/web/overlib?License>, <http://www.stlport.org/doc/license.html>, <http://asm.ow2.org/license.html>, <http://www.cryptix.org/LICENSE.TXT>, <http://hsqldb.org/web/hsqldblicense.html>, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, http://www.gzip.org/zlib/zlib_license.html, <http://www.openldap.org/software/release/license.html>, <http://www.libssh2.org>, <http://slf4j.org/license.html>, <http://www.sente.ch/software/OpenSourceLicense.html>,

fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3- license-agreement; <http://antlr.org/license.html>; <http://aopalliance.sourceforge.net/>; <http://www.bouncycastle.org/license.html>; <http://www.jgraph.com/jgraphdownload.html>; <http://www.jcraft.com/jsch/LICENSE.txt>; http://jotm.objectweb.org/bsd_license.html; <http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>; <http://www.slf4j.org/license.html>; <http://nanoxml.sourceforge.net/orig/copyright.html>; <http://www.json.org/license.html>; <http://forge.ow2.org/projects/javaservice/>; <http://www.postgresql.org/about/license.html>; <http://www.sqlite.org/copyright.html>; <http://www.tcl.tk/software/tcltk/license.html>; <http://www.jaxen.org/faq.html>; <http://www.jdom.org/docs/faq.html>; <http://www.slf4j.org/license.html>; <http://www.iodbc.org/dataspace/iodbc/wiki/iODBC/License>; <http://www.keplerproject.org/md5/license.html>; <http://www.toedter.com/en/jcalendar/license.html>; <http://www.edankert.com/bounce/index.html>; <http://www.net-snmp.org/about/license.html>; <http://www.openmdx.org/#FAQ>; http://www.php.net/license/3_01.txt; <http://srp.stanford.edu/license.txt>; <http://www.schneier.com/blowfish.html>; <http://www.jmock.org/license.html>; <http://xsom.java.net>; <http://benalman.com/about/license/>; <https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js>; <http://www.h2database.com/html/license.html#summary>; <http://jsoncpp.sourceforge.net/LICENSE>; <http://jdbc.postgresql.org/license.html>; <http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto>; <https://github.com/rantav/hector/blob/master/LICENSE>; <http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html>; <http://jibx.sourceforge.net/jibx-license.html>; <https://github.com/lyokato/libgeohash/blob/master/LICENSE>; <https://github.com/hjiang/jsonxx/blob/master/LICENSE>; <https://code.google.com/p/lz4/>; <https://github.com/jedisct1/libsodium/blob/master/LICENSE>; <http://one-jar.sourceforge.net/index.php?page=documents&file=license>; <https://github.com/EsotericSoftware/kryo/blob/master/license.txt>; <http://www.scala-lang.org/license.html>; <https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt>; <http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html>; <https://aws.amazon.com/asl/>; <https://github.com/twbs/bootstrap/blob/master/LICENSE>; <https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt>.

Este produto inclui software licenciado de acordo com a Academic Free License (<http://www.opensource.org/licenses/afl-3.0.php>), a Common Development and Distribution License (<http://www.opensource.org/licenses/cddl1.php>), a Common Public License (<http://www.opensource.org/licenses/cpl1.0.php>), a Sun Binary Code License Agreement Supplemental License Terms, a BSD License (<http://www.opensource.org/licenses/bsd-license.php>), a nova BSD License (<http://opensource.org/licenses/BSD-3-Clause>), a MIT License (<http://www.opensource.org/licenses/mit-license.php>), a Artistic License (<http://www.opensource.org/licenses/artistic-license-1.0>) e a Initial Developer's Public License Version 1.0 (<http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/>).

Este produto inclui copyright do software © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. Todos os direitos reservados. Permissões e limitações relativas a este software estão sujeitas aos termos disponíveis em <http://xstream.codehaus.org/license.html>. Este produto inclui software desenvolvido pelo Indiana University Extreme! Lab. Para obter mais informações, visite <http://www.extreme.indiana.edu/>.

Este produto inclui software Copyright © 2013 Frank Balluffi e Markus Moeller. Todos os direitos reservados. As permissões e limitações relativas a este software estão sujeitas aos termos da licença MIT.

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

ISENÇÃO DE RESPONSABILIDADE: a Informatica LLC fornece esta documentação no estado em que se encontra, sem garantia de qualquer tipo, expressa ou implícita, incluindo, mas não limitando-se, as garantias implícitas de não infração, comercialização ou uso para um determinado propósito. A Informatica LLC não garante que este software ou documentação não contenha erros. As informações fornecidas neste software ou documentação podem incluir imprecisões técnicas ou erros tipográficos. As informações deste software e documentação estão sujeitas a alterações a qualquer momento sem aviso prévio.

AVISOS

Este produto da Informatica (o "Software") traz determinados drivers (os "drivers da DataDirect") da DataDirect Technologies, uma empresa em funcionamento da Progress Software Corporation ("DataDirect"), que estão sujeitos aos seguintes termos e condições:

1. OS DRIVERS DA DATADIRECT SÃO FORNECIDOS NO ESTADO EM QUE SE ENCONTRAM, SEM GARANTIA DE QUALQUER TIPO, EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO LIMITANDO-SE, AS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E NÃO INFRAÇÃO.
2. EM NENHUM CASO, A DATADIRECT OU SEUS FORNECEDORES TERCEIRIZADOS SERÃO RESPONSÁVEIS, EM RELAÇÃO AO CLIENTE FINAL, POR QUAISQUER DANOS DIRETOS, INDIRETOS, INCIDENTAIS, ESPECIAIS, CONSEQUENCIAIS OU DEMAIS QUE POSSAM ADVIR DO USO DE DRIVERS ODBC, SENDO OU NÃO ANTERIORMENTE INFORMADOS DAS POSSIBILIDADES DE TAIS DANOS. ESTAS LIMITAÇÕES SE APLICAM A TODAS AS CAUSAS DE AÇÃO, INCLUINDO, SEM LIMITAÇÕES, QUEBRA DE CONTRATO, QUEBRA DE GARANTIA, NEGLIGÊNCIA, RESPONSABILIDADE RIGOROSA, DETURPAÇÃO E OUTROS ATOS ILÍCITOS.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. Se você encontrar problemas nesta documentação, informe-nos por escrito e envie para Informatica LLC 2100 Seaport Blvd. Redwood City, CA 94063.

A INFORMATICA LLC 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: 2018-07-02

Conteúdo

Prefácio.....	11
Recursos da Informatica.	11
Rede da Informatica.	11
Base de Dados de Conhecimento da Informatica.	11
Documentação da Informatica.	12
Matrizes de Disponibilidade de Produto Informatica.	12
Informatica Velocity.	12
Informatica Marketplace.	12
Suporte global a clientes Informatica.	12
 Capítulo 1: Introdução à Segurança do Informatica.....	 13
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
 Capítulo 2: Autenticação de Usuário.....	 18
Visão Geral da Autenticação de Usuário.	18
Autenticação de Usuário Nativa.	19
Autenticação de Usuário LDAP.	19
Autenticação Kerberos.	20
Logon único com base em SAML para aplicativos da Web Informatica.	20
 Capítulo 3: Domínios de Segurança LDAP.....	 22
Visão Geral de Domínios de Segurança LDAP.	22
Configurando um Domínio de Segurança LDAP.	23
Etapa 1. Configure a conexão com o servidor LDAP.	23
Etapa 2. Configurar um Domínio de Segurança.	25
Etapa 3. Agende os tempos de sincronização.	27
Usando grupos aninhados no diretório de serviço LDAP.	28
Usando um certificado SSL autoassinado.	28
Excluindo um domínio de segurança LDAP.	29
 Capítulo 4: Autenticação Kerberos Configuração.....	 30
Visão geral da configuração da autenticação Kerberos.	30
Etapa 1. Criar um Domínio de Usuário LDAP com os Usuários do Microsoft Active Directory.	31

Etapa 2. Privilégios de Migração de Usuários Nativos e Permissões para um Domínio de Segurança LDAP.	31
Verificar as Contas de Usuário da Autenticação Kerberos.	32
Criar o Arquivo de Migração do Usuário.	32
Executar o Comando infacmd isp migrateUsers.	33
Solução de problemas do Comando migrateUsers.	34
Verifique os Privilégios e as Permissões das Contas de Usuário	34
Etapa 3. Configurar o Arquivo de Configuração Kerberos.	35
Etapa 4. Gerar o Nome Principal e o Formato Keytab.	37
Requisitos do Principal de Serviço em Nível de Nó.	37
Requisitos do Principal de Serviço em Nível de Processo.	38
Executando o Informatica Kerberos SPN Format Generator no Windows.	38
Executando o Informatica Kerberos SPN Format Generator no UNIX.	40
Etapa 5. Analisar o Arquivo de Texto do Formato de SPN e de Keytab.	41
Etapa 6. Criar os Nomes Principais de Serviço e os Arquivos Keytab.	43
Solução de Problemas dos Nomes Principais de Serviço e dos Arquivos Keytab.	44
Etapa 7. Configurar a Autenticação Kerberos para o Domínio.	46
Etapa 8. Atualizar os Nós no Domínio.	48
Etapa 9. Atualizar as Máquinas Cliente.	49
Etapa 10. Iniciar o Domínio Informatica.	49
Após Configurar a Autenticação Kerberos.	50
Bibliotecas personalizadas Kerberos.	50
Usando bibliotecas Kerberos personalizadas.	51
Revertendo para as bibliotecas Kerberos padrão.	52
Capítulo 5: Segurança de domínio.	53
Visão Geral da Segurança do Domínio.	53
Comunicação Segura Dentro do Domínio.	54
Comunicação Segura para Serviços e o Gerenciador de Serviços.	54
Banco de Dados do Repositório de Configuração de Domínio Seguro.	60
Banco de Dados do Repositório do PowerCenter Seguro.	63
Banco de Dados do Repositório do Modelo Seguro.	64
Comunicação Segura para Fluxos de Trabalho e Sessões.	65
Conexões Seguras com um Serviço de Aplicativo da Web.	65
Requisitos para Conexões Seguras para Serviços de Aplicativo da Web.	66
Ativando Conexões Seguras para a Ferramenta Administrator.	66
Serviços de Aplicativo da Web Informatica.	67
Pacotes de criptografia para o domínio Informatica.	69
Configurar o Domínio Informatica para Usar Codificações Avançadas.	69
Criar as listas de pacote de criptografia.	70
Configure o domínio Informatica com uma nova lista efetiva de pacotes de criptografia.	70
Origens e Destinos Seguros.	71
Origens e Destinos do Serviço de Integração de Dados.	72

Origens e Destinos do PowerCenter.	73
Armazenamento de Dados Seguro.	73
Diretório Seguro no UNIX.	73
Alterando a Chave de Criptografia da Linha de Comando.	74
Serviços de Aplicativo e Portas.	77
 Capítulo 6: Logon único para aplicativos da Web Informatica.....	80
Visão geral do logon único com base em SAML.	80
Processo de autenticação do logon único com base em SAML.	80
Experiência de usuário de aplicativos da Web.	81
Configuração do logon único com base em SAML.	81
Antes de habilitar o logon único.	82
Etapa 1. Criar um domínio de segurança para contas de usuário de aplicativos da Web.	82
Etapa 2. Exportar o certificado do AD FS.	86
Etapa 3. Importar o certificado para o truststore do Truststore.	88
Etapa 4. Configurar o Active Directory Federation Services.	89
Etapa 5. Adicionar URLs de aplicativos da Web Informatica ao AD FS.	96
Etapa 6. Ativar logon único com base em SAML.	98
 Capítulo 7: Gerenciamento de Segurança no Informatica Administrator....	101
Usando a visão geral do Informatica Administrator.	101
Segurança do Usuário.	102
Criptografia.	103
Autenticação.	103
Autorização.	104
Guia Segurança.	105
Usando a seção Pesquisa.	105
Usando o Navegador de Segurança.	105
Grupos.	106
Usuários.	106
Funções.	107
Gerenciamento de Senha.	108
Alterando a senha.	108
Gerenciamento de segurança do domínio.	108
Gerenciamento de segurança do usuário.	109
 Capítulo 8: Usuários e grupos.....	110
Visão Geral de Usuários e GruposUsuários e Grupos.	110
Grupos Padrão.	111
Grupo Administrador.	111
Grupo Todos.	112
Grupo Operador.	112
Entendendo as contas de usuário.	112

Administrador Padrão.	112
Administrador de domínio.	113
Administrador de Cliente de Aplicativo.	113
Usuário.	114
Gerenciando usuários.	114
Criando Usuários NativosCriando UsuáriosCriando Usuários.	115
Editando Propriedades Gerais de Usuários Nativos.	116
Atribuindo Usuários Nativos a Grupos Nativos.	116
Atribuindo Usuários LDAP a Grupos Nativos.	116
Ativando e desativando contas de usuário.	117
Excluindo usuários nativos.	117
Usuários LDAP.	118
Desbloqueando uma conta de usuário.	118
Aumentando a Memória do Sistema para Muitos Usuários.	118
Exibindo a Atividade do Usuário.	119
Gerenciando grupos.	122
Adicionando um Grupo Nativo.	122
Editando Propriedades de um Grupo Nativo.	123
Movendo um grupo nativo para outro grupo nativo.	124
Excluindo um grupo nativo.	124
Grupos LDAP.	124
Gerenciando perfis do sistema operacional.	124
Propriedades do perfil do sistema operacional para o Serviço de Integração do PowerCenter	125
Propriedades do Perfil do Sistema Operacional para o Serviço de Integração de Dados.	126
Criando um perfil do sistema operacional.	128
Editando um perfil do sistema operacional.	130
Atribuindo um perfil do sistema operacional padrão a um usuário ou grupo.	130
Excluindo um perfil do sistema operacional	131
Trabalhando com Perfis do Sistema Operacional em um Domínio Seguro.	131
Trabalhando com Perfis do Sistema Operacional em um Domínio com Autenticação Kerberos	131
Bloqueio de conta.	132
Configurando o bloqueio de conta.	133
Regras e diretrizes para o bloqueio de conta.	133
Capítulo 9: Privilégios e funções.....	134
Visão geral de privilégios e funções.	134
Privilégios.	134
Funções.	136
Privilégios do domínio.	136
Grupo de privilégio Administração de segurança.	137
Grupo de privilégio Administração de Domínio.	138
Grupo de privilégio Monitoramento.	143
Grupo de privilégio Ferramentas.	144

Grupo de Privilégio da Administração de Nuvem.	145
Privilégios do Serviço Analyst.	145
Privilégios do Serviço do Gerenciamento de Conteúdo.	146
Privilégios do Data Integration Service.	147
Privilégios do Serviço do Metadata Manager.	147
Grupo de Privilégio Catálogo.	148
Carregar grupo de privilégio.	149
Grupo de privilégio Modelo.	150
Grupo de privilégio Segurança.	150
Privilégios do Serviço de Repositório do Modelo.	151
Privilégios do Serviço de Repositório do PowerCenter.	152
Grupo de privilégio Ferramentas.	153
Grupo de Privilégio Pastas.	154
Grupo de privilégio Objetos de design.	155
Grupo de privilégio Origens e destinos.	158
Grupo de privilégio de Objetos em Tempo de Execução.	160
Grupo de privilégio de objetos globais.	164
Privilégios do Serviço do Ouvinte do PowerExchange.	167
Privilégios do Serviço do Agente de Log do PowerExchange.	167
Privilégios do Serviço de Agendador.	168
Privilégios do Serviço do Test Data Manager.	169
Grupo de Privilégios Administração.	170
Grupo de Privilégio Conexões.	171
Grupo de Privilégio Domínios de Dados.	171
Grupo de Privilégio Mascaramento de Dados.	172
Grupo de Privilégio Subconjunto de Dados.	173
Grupo de Privilégio Diretivas.	173
Grupo de Privilégios Projetos.	174
Grupo de Privilégio Regras.	176
Grupo de Privilégio Geração de Dados.	177
Gerenciando Funções.	177
Funções definidas pelo sistema.	178
Funções personalizadas.	180
Atribuindo privilégios e funções aos usuários e grupos.	181
Privilégios herdados.	182
Atribuindo Privilégios e Funções a um Usuário ou Grupo por Navegação.	182
Exibindo usuários com privilégios para um serviço.	183
Solucionando problemas de privilégios e funções.	183
Capítulo 10: Permissões.	186
Visão geral de permissões.	186
Tipos de Permissões.	187
Filtros de pesquisa de permissão.	188

Permissões do Objeto de Domínio.	189
Permissões do objeto de domínio.	190
Permissões por usuário ou grupo.	191
Permissões do perfil do sistema operacional.	192
Permissões de Conexão.	194
Tipos de permissões de conexão.	194
Permissões de Conexão Padrão.	195
Atribuindo Permissões sobre uma Conexão.	195
Exibindo detalhes de permissão em uma conexão.	195
Editando permissões em uma conexão.	196
Permissões de aplicativos e objetos de aplicativo.	196
Tipos de permissões de aplicativos e objetos de aplicativo.	196
Atribuindo permissões em um aplicativo ou objeto de aplicativo.	197
Exibindo detalhes de permissões em um aplicativo ou objeto de aplicativo.	197
Editando permissões em um aplicativo ou objeto de aplicativo.	198
Negando permissões em um aplicativo ou objeto de aplicativo.	198
Permissões de Serviço de Dados SQL.	198
Tipos de Permissões de Serviço de Dados SQL.	199
Atribuindo Permissões em um serviço de dados SQL.	199
Exibindo Detalhes de Permissão em um Serviço de Dados SQL.	200
Editando permissões em um Serviço de Dados SQL.	200
Negando Permissões em um Serviço de Dados SQL.	201
Segurança em Nível de Coluna.	201
Permissões do serviço da Web.	202
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.	204
Editando permissões em um serviço Web.	205
Capítulo 11: Relatórios de Auditoria.	206
Visão Geral dos Relatórios de Auditoria.	206
Informações Pessoais do Usuário.	207
Associação de Grupo de Usuários.	207
Privilégios.	208
Associação de Funções.	209
Permissões em Objetos de Domínio.	209
Selecionando Usuários para um Relatório de Auditoria.	210
Selecionando Grupos para um Relatório de Auditoria.	211
Selecionando Funções para um Relatório de Auditoria.	211
Apêndice A: Permissões e Privilégios da Linha de Comando.	213
Comandos infacmd as.	213
Comandos infacmd dis.	214

Comandos infacmd es.	216
Comandos infacmd ipc.	216
Comandos infacmd isp.	216
Comandos infacmd mrs.	228
Comandos infacmd ms.	230
Comandos infacmd oie.	231
Comandos infacmd ps.	231
Comandos infacmd pwx.	232
Comandos infacmd rms.	233
Comandos infacmd rtm.	234
Comandos infacmd sch.	234
Comandos infacmd sql.	235
Comandos infacmd wfs.	236
Comandos pmcmd.	236
Comandos pmrep.	239
Apêndice B: Funções personalizadas.	244
Função Personalizada do Serviço Analyst.	244
Funções Personalizadas do Serviço do Metadata Manager.	245
Função Personalizada do Operador.	247
Funções Personalizadas do Serviço do Repositório do PowerCenter.	248
Regras personalizadas do Test Data Manager.	249
Apêndice C: Lista padrão de pacotes de criptografia.	254
Índice.	256

Prefácio

O Guia de Segurança da Informatica apresenta informações sobre a segurança do domínio Informatica. Ele inclui as informações necessárias para gerenciar a segurança do domínio Informatica e dos clientes Informatica que se conectam ao domínio. Esse guia presume que você conheça o domínio Informatica e o Informatica Administrator. Ele também presume que você esteja familiarizado com os servidores e os processos de autenticação de rede.

Recursos da Informatica

Rede da Informatica

A Rede da Informatica hospeda o Suporte Global a Clientes da Informatica, a Base de Dados de Conhecimento da Informatica e outros recursos de produtos. Para acessar a Rede da Informatica, visite <https://network.informatica.com>.

Como membro, você pode:

- Acessar todos os seus recursos Informatica em um só lugar.
- Pesquisar a Base de Dados de Conhecimento em busca de recursos de produtos, incluindo documentações, perguntas frequentes e práticas recomendadas.
- Visualizar informações sobre disponibilidade de produtos.
- 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 pesquisar a Rede da Informatica em busca de recursos de produtos, como documentações, artigos de instruções, práticas recomendadas e PAMs.

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

Documentação da Informatica

Para obter a documentação mais recente do seu produto, navegue pela Base de Dados de Conhecimento da Informatica

em https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx

Em caso de dúvidas, comentários ou ideias sobre esta documentação, entre em contato com a equipe de Documentação da Informatica pelo e-mail infa_documentation@informatica.com.

Matrizes de Disponibilidade de Produto Informatica

As Matrizes de Disponibilidade de Produto (PAMs) indicam as versões dos sistemas operacionais, os bancos de dados e outros tipos de fontes e destinos de dados com os quais uma versão de produto é compatível. Se você for membro da Rede da Informatica, poderá acessar PAMs 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. Desenvolvido com base na experiência no mundo real de centenas de projetos de gerenciamento de dados, o Informatica Velocity representa o conhecimento coletivo de nossos consultores, que trabalharam com organizações de todo o mundo para planejar, desenvolver, implantar e manter soluções de gerenciamento de dados bem-sucedidas.

Se você for membro da Rede da Informatica, poderá acessar os recursos do Informatica Velocity em

<http://velocity.informatica.com>.

Se você tiver dúvidas, comentários ou ideias sobre o Informatica Velocity, entre em contato com os Serviços Profissionais da Informatica em ips@informatica.com.

Informatica Marketplace

O Informatica Marketplace é um fórum onde você pode encontrar soluções que aumentam, ampliam ou aprimoram suas implementações da Informatica. Aproveitando qualquer uma das centenas de soluções fornecidas por desenvolvedores e parceiros da Informatica, você pode melhorar sua produtividade e agilizar o tempo de implementação nos seus projetos. Você pode acessar o Informatica Marketplace através do link <https://marketplace.informatica.com>.

Suporte global a clientes Informatica

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

Para descobrir o número de telefone local do Suporte Global a Clientes da Informatica, visite o site da Informatica no seguinte link:

<http://www.informatica.com/us/services-and-training/support-services/global-support-centers>.

Se você for membro da Rede da Informatica, poderá usar o Suporte Online em

<http://network.informatica.com>.

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

Use o keytool para criar um certificado SSL ou um Certificate Signing Request (CSR), bem como armazenamento de chaves e truststores no formato JKS.

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

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>

OpenSSL

Você pode usar o OpenSSL para criar um certificado SSL ou CSR, bem como converter um armazenamento de chaves no formato JKS no 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](#)
- [Logon único com base em SAML para aplicativos da Web Informatica, 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 login na rede. Os aplicativos cliente Informatica usam as credenciais do login 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 login único com base em SAML para aplicativos da Web Informatica. No entanto, você deve concluir todas as tarefas de configuração necessárias antes de ativar o login único com base em SAML. Você não pode ativar o login único com base em SAML em um domínio Informatica configurado para usar a autenticação Kerberos.

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 login, 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 o domínio Informatica para permitir que os usuários em um serviço de diretório LDAP façam login nos aplicativos cliente Informatica. O domínio Informatica 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.

A Informatica não é compatível com a autenticação Kerberos cruzada ou com vários realms. O host do servidor, as máquinas cliente e o servidor de autenticação kerberos devem estar no mesmo realm.

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.

Logon único com base em SAML para aplicativos da Web Informatica

Você pode configurar um domínio Informatica para permitir que os usuários usem o logon único (SSO) com base em SAML para fazer logon em aplicativos da Web da ferramenta Administrator, da ferramenta Analyst e da ferramenta Monitoring.

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. Em um domínio Informatica, o aplicativo da Web Informatica é o provedor de serviços. O Microsoft Active Directory Federation Services (AD FS) 2.0 é o provedor de identidade que autentica os usuários de aplicativos da Web com o repositório de identidade 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 de administrador 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 AD FS. O AD FS 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.

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

CAPÍTULO 3

Domínios de Segurança LDAP

Este capítulo inclui os seguintes tópicos:

- [Visão Geral de Domínios de Segurança LDAP, 22](#)
- [Configurando um Domínio de Segurança LDAP, 23](#)
- [Excluindo um domínio de segurança LDAP, 29](#)

Visão Geral de Domínios de Segurança LDAP

Um domínio de segurança LDAP inclui um conjunto de usuários e grupos que são importados de um serviço de diretório LDAP. Você deverá criar um domínio de segurança LDAP se usar a autenticação de usuário LDAP ou a autenticação de rede Kerberos.

Configure os domínios de segurança LDAP para armazenar a lista de usuários de um serviço de diretório LDAP cujo acesso ao domínio Informatica e aos aplicativos cliente você deseja permitir. O domínio de segurança LDAP não armazena as credenciais de conta de usuário. Quando um usuário faz logon em um cliente Informatica, o Gerenciador de Serviços verifica se a conta de usuário está em um domínio de segurança. Se a conta de usuário pertencer a um domínio de segurança LDAP, o Gerenciador de Serviços autenticará o usuário com o serviço de diretório LDAP.

Quando você instala serviços Informatica sem ativar a autenticação Kerberos, o instalador do Informatica cria o domínio de segurança nativo por padrão. Após a instalação, você poderá adicionar usuários e grupos ao domínio de segurança nativo. Se você tiver usuários em um serviço de diretório LDAP para conceder acesso aos aplicativos cliente Informatica, poderá configurar domínios de segurança LDAP além do domínio de segurança nativo. Configure uma conexão com o servidor LDAP e importe os usuários e os grupos nos domínios de segurança LDAP.

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. Após a instalação, você pode configurar uma conexão com o servidor LDAP e importar usuários e grupos do serviço de diretório LDAP para o domínio de segurança LDAP. Se você usa a autenticação Kerberos, não pode usar o domínio de segurança Nativo.

Configurando um Domínio de Segurança LDAP

Você pode criar um domínio de segurança LDAP para contas de usuário importadas de um serviço de diretório LDAP. Para organizar diferentes grupos de usuários, você pode criar vários domínios de segurança LDAP.

Crie e gerencie usuários e grupos LDAP no serviço de diretório LDAP. Configure uma conexão com o servidor LDAP e usar 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 os domínios de segurança LDAP. Se o servidor LDAP usa o protocolo SSL, também é necessário especificar a localização do certificado SSL.

Você pode importar usuários dos seguintes serviços de diretório LDAP:

- IBM Tivoli Directory Server
- Microsoft Active Directory

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

- Novell eDirectory
- OpenLDAP
- Servidor de Diretório Sun Java System

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, em seguida, sincronizar o domínio de segurança LDAP com o serviço de diretório LDAP.

Use a caixa de diálogo Configuração LDAP para configurar a conexão com o serviço de diretório LDAP e criar o domínio de segurança LDAP. Você também pode usar a caixa de diálogo Configuração LDAP para configurar um agendamento de sincronização.

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

1. Configure a conexão com o serviço de diretório LDAP.
2. Configure um domínio de segurança.
3. Agende os tempos de sincronização.

Etapa 1. Configure a conexão com o servidor LDAP

Configure a conexão com o servidor LDAP que contém o serviço de diretório do qual você deseja importar as contas de usuário para o domínio Informatica.

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 para o arquivo de truststore `cacerts` em cada nó do gateway dentro no domínio Informatica. Consulte ["Usando um certificado SSL autoassinado" na página 28](#) para obter detalhes.

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

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 **Conectividade do LDAP**.
4. Configure as propriedades de conexão do servidor LDAP.

Talvez seja necessário entrar em contato com o administrador do LDAP para obter as informações sobre 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 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. Selecione dos seguintes serviços de diretório: Nota: Se você usar a autenticação Kerberos, deverá selecionar o Microsoft Active Directory.
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. Deixe em branco para login anônimo. Para obter mais informações, consulte a documentação do serviço de diretório LDAP.
Senha	Senha do usuário principal. Deixe em branco para login anônimo. Não disponível para uso com a autenticação Kerberos.
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. Para ativar o Gerenciador de Serviços para reconhecer um certificado autoassinado como válido, especifique o arquivo truststore e a senha a ser usada.
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. Ative essa opção.

Propriedade	Descrição
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.

5. Clique em Testar Conexão para verificar se a conexão com o servidor LDAP é válida.

Etapa 2. Configurar um Domínio de Segurança

Crie um domínio de segurança para cada conjunto de contas de usuário e grupos que você deseja importar do serviço de diretório LDAP. Configurar bases e filtros de pesquisa para definir o conjunto de contas de usuários e grupos a ser incluídos em um domínio de segurança. 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 importa grupos e a lista de usuários que pertence aos grupos. Ele importa os grupos incluídos no filtro de grupos e as contas de usuário incluídas no filtro de usuários.

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.

Nota: Ao contrário dos nomes de usuários nativos, os nomes de usuários LDAP podem fazer distinção de maiúsculas e minúsculas.

Quando você definir o serviço de diretório LDAP, pode usar atributos diferentes para o ID exclusivo (UID). O Gerenciador de Serviços exige um UID particular para identificar usuários em cada serviço de diretório LDAP. Antes de configurar o domínio de segurança, verifique se o serviço de diretório LDAP usa o UID exigido.

A tabela a seguir mostra o UID necessário para cada serviço de diretório LDAP:

Serviço de Diretório LDAP	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Novell eDirectory	uid
OpenLDAP	uid
Servidor de Diretório Sun Java System	uid

O Gerenciador de Serviços não importa o atributo LDAP que indica se uma conta de usuário está ativada ou desativada. Você deve ativar ou desativar uma conta de usuário na ferramenta Administrator. O status da conta de usuário no serviço de diretório LDAP afeta a autenticação de usuário nos aplicativos cliente. Por

exemplo, uma conta de usuário está ativada no domínio Informatica mas desativada no serviço de diretório LDAP. Se o serviço de diretório LDAP permitir que as contas de usuário desativadas façam login, o usuário poderá fazer login nos aplicativos cliente. Se o serviço de diretório LDAP não permitir que as contas de usuário desativadas façam login, o usuário não poderá fazer login nos aplicativos cliente.

Nota: 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 LDAP**.
3. Na caixa de diálogo **Configuração LDAP**, clique na guia **Domínios de Segurança**.
4. Clique em **Adicionar**.
5. Use a sintaxe de consulta LDAP para criar filtros e especificar os usuários e grupos a serem incluídos no domínio de segurança que você está criando.

Talvez seja necessário entrar em contato com o administrador do LDAP para obter as informações sobre os usuários e grupos disponíveis no serviço de diretório LDAP.

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. Ele 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.

Propriedade	Descrição
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.

- 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.
- Para adicionar outro domínio de segurança LDAP, repita as etapas [4](#) a [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.
- Clique em **OK** para salvar os domínios de segurança.

Etapa 3. Agende os tempos de sincronização

Você pode configurar um agendamento para que o Gerenciador de Serviços sincronize periodicamente a lista de usuários e grupos no domínio de segurança LDAP com a lista de usuários e grupos no serviço de diretório LDAP.

Importante: Antes de iniciar o processo de sincronização, verifique se o arquivo `/etc/hosts` contém uma entrada para o nome do host do servidor LDAP. Se o Gerenciador de Serviços não puder resolver o nome do host do servidor LDAP, a sincronização de usuário poderá falhar.

Durante a sincronização, o Gerenciador de Serviços importa usuários e grupos do serviço de diretório LDAP. O Gerenciador de Serviços exclui todos os usuários ou grupos do domínio de segurança LDAP que não estão mais incluídos nos filtros de pesquisa usados para a importação.

Por padrão, o Gerenciador de Serviços não possui um horário agendado para sincronização com o serviço de diretório LDAP. Para garantir uma lista precisa de usuários e grupos nos domínios de segurança LDAP, você pode agendar os horários durante o dia para o Gerenciador de Serviços sincronizar os domínios de segurança LDAP. O Gerenciador de Serviços sincroniza os domínios de segurança LDAP com o serviço de diretório LDAP todos os dias nos horários definidos.

Nota: Durante a sincronização, o Gerenciador de Serviços bloqueia a conta do usuário que ele sincroniza. Quando a conta de usuário for bloqueada, o Gerenciador de Serviços não poderá autenticar a conta de usuário. É possível que os usuários não consigam efetuar login nos aplicativos clientes. Se os usuários estiverem conectados aos aplicativos cliente quando a sincronização for iniciada, talvez eles não consigam executar nenhuma tarefa. A duração do processo de sincronização depende do número de usuários e grupos a serem sincronizados. Para evitar a interrupção do uso, sincronize os domínios de segurança durante os horários em que a maioria dos usuários não está conectada. Para sincronizar mais de 100 usuários ou grupos, ative a paginação no serviço de diretório LDAP antes de executar a sincronização. Se você não ativar a paginação no serviço de diretório LDAP, a sincronização poderá falhar.

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

- 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.
É possível adicionar quantos tempos de sincronização no dia você quiser. Se a lista de usuários e grupos no serviço de diretório LDAP for alterada com frequência, você pode agendar o Gerenciador de Serviços para sincronizar várias vezes ao dia.
5. 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**.
6. Clique em **OK** para salvar o agendamento da sincronização.

Nota: Se você reiniciar o domínio Informatica antes da sincronização do Gerenciador de Serviços com o serviço de diretório LDAP, os horários de sincronização adicionados serão perdidos.

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 o utilitário de gerenciamento de chaves e certificados Java keytool para importar o certificado no arquivo de truststore `cacerts` em cada nó de gateway do 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\jre\bin
```

Reinicie o nó depois de importar o certificado.

Excluindo um domínio de segurança LDAP

Para proibir permanentemente os usuários em um domínio de segurança LDAP de acessar clientes de aplicativo, exclua o domínio de segurança LDAP. Quando você exclui um domínio de segurança LDAP, o Service Manager exclui todas as contas de usuário e grupos nesse domínio do banco de dados de configuração de domínio.

1. Na caixa de diálogo Configuração LDAP, clique na guia **Domínios de Segurança**.
A caixa de diálogo Configuração LDAP exibe a lista de domínios de segurança.
2. Para assegurar que você esteja excluindo o domínio de segurança correto, clique no nome do domínio de segurança para exibir o filtro usado para importar os usuários e os grupos e verifique se esse é o domínio de segurança que você deseja excluir.
3. Clique no botão **Excluir** ao lado de um domínio de segurança para excluir esse domínio de segurança.
4. Clique em **OK** para confirmar que você deseja excluir o domínio de segurança.

CAPÍTULO 4

Autenticação Kerberos Configuração

Este capítulo inclui os seguintes tópicos:

- [Visão geral da configuração da autenticação Kerberos, 30](#)
- [Etapa 1. Criar um Domínio de Usuário LDAP com os Usuários do Microsoft Active Directory, 31](#)
- [Etapa 2. Privilégios de Migração de Usuários Nativos e Permissões para um Domínio de Segurança LDAP, 31](#)
- [Etapa 3. Configurar o Arquivo de Configuração Kerberos, 35](#)
- [Etapa 4. Gerar o Nome Principal e o Formato Keytab, 37](#)
- [Etapa 5. Analisar o Arquivo de Texto do Formato de SPN e de Keytab, 41](#)
- [Etapa 6. Criar os Nomes Principais de Serviço e os Arquivos Keytab, 43](#)
- [Etapa 7. Configurar a Autenticação Kerberos para o Domínio, 46](#)
- [Etapa 8. Atualizar os Nós no Domínio, 48](#)
- [Etapa 9. Atualizar as Máquinas Cliente, 49](#)
- [Etapa 10. Iniciar o Domínio Informatica, 49](#)
- [Após Configurar a Autenticação Kerberos, 50](#)
- [Bibliotecas personalizadas Kerberos, 50](#)

Visão geral da configuração da autenticação Kerberos

Ao criar o domínio Informatica durante a instalação, você pode selecionar a opção para ativar a autenticação Kerberos. 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.

Para configurar a autenticação Kerberos para o domínio Informatica na linha de comando, execute as seguintes etapas:

1. Crie um Domínio de Usuário LDAP com os Usuários do Microsoft Active Directory.
2. Migre usuários nativos para um domínio de segurança LDAP.
3. Defina a configuração Kerberos e copie o arquivo de configuração no diretório Informatica.

4. Gere o SPN e o nome de arquivo keytab no formato exigido pelo domínio Informatica.
5. Analise o arquivo de texto do formato de SPN e de arquivo keytab.
6. Crie os SPNs e os arquivos keytab.
7. Configure a autenticação Kerberos para o domínio Informatica.
8. Atualize os nós no domínio Informatica.
9. Atualize as máquinas cliente.
10. Inicie o domínio Informatica e execute a ferramenta Administrator.

Depois de configurar a autenticação Kerberos e os domínios de segurança LDAP, verifique se as contas de usuário têm os privilégios e as permissões apropriados. Verifique se os serviços no domínio apresentam o desempenho esperado e se os usuários podem fazer login com conexão única.

Nota: As etapas fornecidas assumem que você tenha instalado os serviços Informatica sem ativar a autenticação Kerberos. Se você tiver ativado a autenticação Kerberos durante a instalação, siga as etapas dos guias de instalação do Informatica.

Etapa 1. Criar um Domínio de Usuário LDAP com os Usuários do Microsoft Active Directory

Antes de configurar o domínio Informatica para usar a autenticação Kerberos, verifique se todas as contas de usuário estão em domínios de segurança LDAP dentro do domínio Informatica. Contas de usuário devem ser importadas para um domínio de segurança LDAP do Microsoft Active Directory.

Se o domínio Informatica tiver contas de usuário em um domínio de segurança LDAP que não usa o Microsoft Active Directory, migre-os para o Microsoft Active Directory. Para obter mais informações sobre a migração de contas de usuário para o Microsoft Active Directory, consulte a documentação da implementação de LDAP.

Se o domínio tiver contas de usuário no domínio de segurança nativo, migre os usuários para o Microsoft Active Directory. Configure um domínio de segurança LDAP e a conexão com o serviço do Microsoft Active Directory. Em seguida, configure filtros para os usuários e grupos e sincronize as contas de usuário no Microsoft Active Directory com as contas de usuário no domínio de segurança LDAP.

Para obter mais informações sobre como configurar um domínio LDAP e sincronizar as contas de usuário, consulte [“Configurando um Domínio de Segurança LDAP” na página 23](#)

Etapa 2. Privilégios de Migração de Usuários Nativos e Permissões para um Domínio de Segurança LDAP

Se o domínio Informatica tiver contas de usuários no domínio de segurança nativo, migre todos os grupos de usuários, funções, privilégios e permissões de contas para as contas de usuário correspondentes em um domínio de segurança LDAP. Depois de configurar o domínio Informatica para usar a autenticação Kerberos, você não poderá acessar as contas de usuário no domínio de segurança nativo.

Se o domínio tiver contas de usuário no domínio de segurança nativo, as contas de usuário do Active Directory correspondentes no domínio de segurança LDAP deverão ter os mesmos grupos, funções,

privilégios e permissões. Migre os grupos, as funções, os privilégios e as permissões dos usuários nativos para os usuários no domínio de segurança LDAP. Em seguida, verifique se os grupos, as funções, os privilégios e as permissões foram migrados corretamente.

Se o domínio não tiver contas de usuário em um domínio de segurança nativo, você poderá continuar em [“Etapa 3. Configurar o Arquivo de Configuração Kerberos” na página 35.](#)

Para migrar os grupos, as funções, os privilégios e as permissões dos usuários nativos para os usuários no domínio de segurança LDAP, execute as seguintes etapas:

1. Verificar as contas de usuário da Autenticação Kerberos.
2. Criar o arquivo de migração do usuário.
3. Executar o comando `infacmd isp migrateusers`.
4. Verificar os grupos, as funções, os privilégios e as permissões das contas de usuário.

Nota: Para evitar problemas ao migrar as funções de grupos de usuários, os privilégios e as permissões, não execute fluxos de trabalho nem modifique grupos de usuários, funções, privilégios ou permissões durante o processo de migração.

Verificar as Contas de Usuário da Autenticação Kerberos

Exiba a lista de contas de usuário nativo e determine as contas que você deseja migrar para um domínio de segurança LDAP da 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 LDAP deve ter uma conta correspondente no serviço Microsoft Active Directory que você usa para a autenticação Kerberos.

Se as contas não estiverem no serviço do Microsoft Active Directory, adicione as contas de usuário ao serviço de diretório. Para obter mais informações sobre como adicionar contas de usuário ao serviço do Microsoft Active Directory, consulte a documentação do Microsoft Active Directory.

Nota: O nome de usuário das contas de usuário no domínio de segurança LDAP tem um comprimento máximo de 20 caracteres. Quando você adicionar as contas de usuário ao serviço do Microsoft Active Directory, certifique-se de que o nome de usuário não tenha mais de 20 caracteres.

Criar o Arquivo de Migração do Usuário

O comando `infacmd isp migrateUsers` usa um arquivo de migração do usuário para determinar quais grupos, funções, privilégios e permissões serão atribuídas aos usuários LDAP. O arquivo de migração do usuário é um arquivo de texto simples que contém a lista de usuários nativos e os usuários LDAP correspondentes que exigem os mesmos grupos, funções, privilégios e permissões.

Quando você cria o arquivo de migração do usuário, deve especificar o domínio de segurança da conta de usuário. Uma barra (/) separa o domínio de segurança do nome de usuário. Uma vírgula (,) separa o usuário nativo do usuário LDAP correspondente. Os domínios de segurança fazem distinção entre maiúsculas e minúsculas. Os nomes de usuário não fazem distinção entre maiúsculas e minúsculas.

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

```
Native/<SourceUserName>,LDAP/<TargetUserName>
```


Você pode migrar os grupos, as funções, os privilégios e as permissões de usuários nativos para usuários em diferentes domínios de segurança LDAP. Por exemplo, o arquivo de migração do usuário contém a seguinte lista de usuários:

```
Native/User1,LDAPSecurityDomain/User1
Native/User2,LDAPSecurityDomain/User2
Native/User3,newLDAPSecDomain/User3
```

O comando `migrateUser` atribui ao User1 e ao User2 no LDAPSecurityDomain os mesmos grupos, funções, privilégios e permissões do User1 e do User2 no domínio de segurança nativo. O comando atribui ao User3 em newLDAPSecDomain os mesmos grupos, funções, privilégios e permissões do User3 no domínio de segurança nativo.

O comando `migrateUsers` ignora qualquer entrada com um nome de usuário da fonte ou um nome de usuário de destino duplicado.

Executar o Comando `infacmd isp migrateUsers`

Para migrar grupos, funções, privilégios e permissões dos usuários do domínio de segurança nativo para usuários do domínio de segurança LDAP, execute o comando `infacmd migrateUsers` e especifique o arquivo de migração do usuário a ser usado.

Antes de executar o comando `infacmd isp migrateUsers`, verifique se todas as instâncias dos seguintes serviços no domínio estão em execução:

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

Certifique-se de que o Serviço do Repositório do PowerCenter esteja em execução no modo normal.

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

```
infacmd isp migrateUsers -dn <DomainName> -un <AdministratorUserName> -pd
<AdministratorPassword> -umf <UserMigrationFile>
```

Por exemplo, o seguinte comando migra os grupos, as funções, os privilégios e as permissões para usuários com base no arquivo de migração do usuário `um_s.txt`:

```
infacmd isp migrateUsers -dn UMT_Domain -un Administrator -pd Administrator -umf C:\UMT
\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 onde você executa o comando.

Para obter mais informações sobre o comando, consulte a *Referência de Comandos da Informatica*.

Solução de problemas do Comando migrateUsers

Como melhorar o desempenho de migração?

Para melhorar o desempenho da migração, execute as seguintes etapas:

1. Crie vários arquivos de migração de usuário exclusivo com um número limitado de usuários em cada arquivo.
2. Execute várias instâncias do comando migrateUsers simultaneamente.

Por exemplo, para migrar os grupos, as funções, os privilégios e as permissões para 150 usuários, crie três arquivos de migração, sendo que cada um conterá 50 usuários. Em seguida, execute três instâncias do comando migrateUsers simultaneamente. Especifique um arquivo de migração de usuário exclusivo para cada instância do comando.

O comando migrateUsers falha.

Se o comando migrateUsers falhar, os seguintes caminhos de recuperação estarão disponíveis:

- Execute o comando migrateUsers novamente.
- Modifique o arquivo de migração do usuário. Em seguida, execute o comando migrateUsers.

Quando você executar o comando novamente, especifique o mesmo arquivo de migração do usuário. 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.

Para modificar o arquivo de migração do usuário, realize as seguintes etapas:

1. Exiba os detalhes do arquivo de log que foi criado quando você executou o comando migrateUsers.
2. Exclua os usuários que o comando migrou com êxito do arquivo de migração do usuário.
3. Execute o comando migrateUsers.

Verifique os Privilégios e as Permissões das Contas de Usuário

Antes de ativar a autenticação Kerberos, verifique se os usuários no domínio de segurança LDAP têm os grupos, as funções, os privilégios e as permissões. Você pode usar infacmd para verificar os grupos, as funções, os privilégios e as permissões das contas de usuário no domínio de segurança LDAP.

Verifique se os seguintes objetos foram migrados com sucesso:

Usuários e grupos

Para determinar os grupos aos quais as contas de usuário pertencem, obtenha uma lista de usuários e grupos associados. Execute o seguinte comando:

```
infacmd aud getUserGroupAssociation
```

Funções

Para obter a lista de funções associadas aos usuários e aos grupos de domínio, execute o seguinte comando:

```
infacmd aud getUserGroupAssociationForRoles
```

Privilégios

Para obter uma lista de privilégios atribuídos aos usuários e aos grupos no domínio, execute o seguinte comando:

```
infacmd aud getPrivilegeAssociation
```

Permissões

Para obter uma lista de permissões atribuídas aos usuários e aos grupos no domínio, execute o seguinte comando:

```
infacmd aud getDomainObjectPermissions
```

Permissões em pastas e objetos globais

Se o domínio tiver um Serviço do Repositório do PowerCenter, verifique as permissões às pastas do PowerCenter e aos objetos de repositório global atribuídos às contas de usuário. O repositório do PowerCenter pode ter os seguintes objetos:

- Pastas
- Grupos de implantação
- Rótulos
- Consultas
- Conexões

Depois de configurar o domínio para usar a autenticação Kerberos, você não poderá modificar as contas de usuários nativos.

Depois de confirmar que os grupos, as funções, os privilégios e as permissões das contas de usuário nativo foram movidos com sucesso para as contas de usuário LDAP, exclua as contas de usuário nativo. Use a ferramenta Administrator para excluir as contas de usuário. Para obter mais informações, consulte [“Excluindo usuários nativos” na página 117](#).

Etapa 3. Configurar o Arquivo de Configuração Kerberos

O Kerberos armazena as informações de configuração em um arquivo denominado *krb5.conf*. O Informatica exige a definição de propriedades específicas no arquivo de configuração Kerberos para que o domínio Informatica possa usar a autenticação Kerberos corretamente. Você deve definir as propriedades no arquivo de configuração *krb5.conf* e, em seguida, copiar o arquivo para o diretório do Informatica.

O arquivo de configuração contém as informações sobre o servidor Kerberos, incluindo o realm Kerberos e o endereço do KDC. Você pode solicitar que o administrador do Kerberos defina as propriedades no arquivo de configuração e envie uma cópia dele para você.

1. Faça backup do arquivo *krb5.conf* antes de realizar qualquer alteração.
2. Edite o arquivo *krb5.conf*.
3. Na seção *libdefaults*, defina ou adicione as propriedades exigidas pela Informatica.

A seguinte tabela lista os valores para os quais você deve definir propriedades na seção `libdefaults`:

Parâmetro	Valor
<code>default_realm</code>	Nome do realm de serviço para o domínio Informatica.
<code>encaminável</code>	Permite que um serviço delegue credenciais de usuário do cliente para outro serviço. Defina esse parâmetro como <code>True</code> . O domínio Informatica exige que os serviços de aplicativo autenticuem as credenciais de usuário do cliente com outros serviços.
<code>default_tkt_enctypes</code>	Tipo de criptografia para a chave da sessão no tíquete de concessão de tíquete (TGT). Defina esse parâmetro como <code>rc4-hmac</code> . O Informatica é compatível somente com o tipo de criptografia <code>rc4-hmac</code> .
<code>udp_preference_limit</code>	Determina o protocolo que o Kerberos usa quando envia uma mensagem ao KDC. Defina <code>udp_preference_limit = 1</code> para usar sempre o TCP. O domínio Informatica é compatível somente com o protocolo TCP. Se o <code>udp_preference_limit</code> for definido como qualquer outro valor, o domínio Informatica poderá encerrar inesperadamente.

- Na seção `realms`, inclua o número de porta no endereço do KDC separado por dois-pontos.

Por exemplo, se o endereço KDC for `kerberos.example.com` e o número de porta for 88, defina o parâmetro `kdc` da seguinte maneira:

```
kdc = kerberos.example.com:88
```

- Salve o arquivo `krb5.conf`.
- Copie o arquivo de configuração para o diretório da Informatica.

Você deve copiar o `krb5.conf` no seguinte diretório: `<INFA_HOME>/services/shared/security`

Se o domínio tiver vários nós, copie o `krb5.conf` no mesmo diretório em todos os nós no domínio.

O seguinte exemplo mostra o conteúdo de um `krb5.conf` com as propriedades necessárias:

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
    admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
    kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
}

[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

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

Etapa 4. Gerar o Nome Principal e o Formato Keytab

Se você executar o domínio Informatica com a autenticação Kerberos, deverá associar os arquivos keytab e os nomes principais de serviço (SPN) Kerberos aos nós e aos processos no domínio Informatica. A Informatica necessita que os arquivos keytab autentiquem os serviços na rede sem solicitar senhas.

Com base nos requisitos de segurança do domínio, você pode definir o nível principal de serviço para um dos seguintes níveis:

Nível de Nó

Se o domínio for usado para teste ou desenvolvimento e não necessitar de um alto nível de segurança, você poderá definir o principal de serviço em nível de nó. Você pode usar um arquivo keytab e um SPN para o nó e todos os processos de serviço no nó. Você também deverá configurar um arquivo keytab e um SPN separado para os processos HTTP no nó.

Nível de Processo

Se o domínio for usado para produção e necessitar de um alto nível de segurança, você poderá definir o principal de serviço em nível de processo. Crie um SPN e um arquivo keytab exclusivos para cada nó e cada processo no nó. Você também deverá configurar um arquivo keytab e um SPN separado para os processos HTTP no nó.

O domínio Informatica requer que os nomes dos arquivos keytab e os nomes principais de serviços sigam um formato específico. Para garantir que você siga o formato correto para os nomes de arquivos keytab e para os nomes principais de serviço, use o Informatica Kerberos SPN Format Generator para gerar uma lista dos nomes de arquivos keytab e dos nomes principais de serviço no formato exigido pelo domínio Informatica.

Requisitos do Principal de Serviço em Nível de Nó

Se o domínio Informatica não necessitar de um alto nível de segurança, o nó e os processos do serviço poderão compartilhar os mesmos SPNs e arquivos keytab. O domínio não necessita de um SPN separado para cada processo do serviço em um nó.

O domínio Informatica necessita de SPNs e arquivos keytab para os seguintes componentes em nível de nó:

Nome distinto (DN) da entidade de segurança para o serviço de diretório LDAP

Nome principal para o DN de usuário de vinculação usado para pesquisar o serviço de diretório LDAP. O nome do arquivo keytab deve ser `infa_ldapuser.keytab`.

Processo do nó

Nome principal do nó da Informatica que inicia ou aceita chamadas de autenticação. O mesmo nome principal é usado para autenticar os serviços no nó. Cada nó de gateway no domínio precisa de um nome principal separado.

Processos HTTP no domínio

Nome da entidade de segurança para todos os serviços de aplicativo da Web no domínio Informatica, incluindo o Informatica Administrator. O navegador usa esse nome de entidade de segurança para se autenticar em todos os processos HTTP no domínio. O nome do arquivo de keytab deve ser `webapp_http.keytab`.

Requisitos do Principal de Serviço em Nível de Processo

Se o domínio Informatica necessitar de um alto nível de segurança, crie um SPN e um arquivo keytab separados para cada nó e cada serviço no nó.

O domínio Informatica necessita de SPNs e arquivos keytab para os seguintes componentes em nível de processo:

Nome distinto (DN) da entidade de segurança para o serviço de diretório LDAP

Nome principal para o DN de usuário de vinculação usado para pesquisar o serviço de diretório LDAP. O nome do arquivo keytab deve ser `infa_ldapuser.keytab`.

Processo do nó

Nome principal do nó da Informatica que inicia ou aceita chamadas de autenticação.

Serviço Informatica Administrator

Nome principal do serviço Informatica Administrator que autentica o serviço com outros serviços no domínio Informatica. O nome do arquivo de keytab deve ser `_AdminConsole.keytab`.

Processos HTTP no domínio

Nome da entidade de segurança para todos os serviços de aplicativo da Web no domínio Informatica, incluindo o Informatica Administrator. O navegador usa esse nome de entidade de segurança para se autenticar em todos os processos HTTP no domínio. O nome do arquivo de keytab deve ser `webapp_http.keytab`.

Processo do serviço

Nome principal do serviço de aplicativo executado em um nó no domínio Informatica. Cada serviço de aplicativo exige um nome de principal de serviço e de arquivo keytab exclusivo.

Executando o Informatica Kerberos SPN Format Generator no Windows

Você pode executar o Informatica Kerberos SPN Format Generator para gerar um arquivo que mostra o formato correto dos nomes de SPNs e de arquivo keytab exigidos no domínio Informatica.

1. Em uma máquina que hospeda o nó da Informatica, vá para o seguinte diretório da Informatica:
`<InformaticaDirectory>/Tools/Kerberos`
2. Execute o arquivo `SPNFormatGenerator.bat`.
A página de **boas-vindas** do Informatica Kerberos SPN Format Generator é exibida.
3. Clique em **Avançar**.
A página **Nível Principal de Serviço** é exibida.
4. Selecione o nível usado para definir os principais de serviço Kerberos para o domínio.

A seguinte tabela descreve os níveis que você pode selecionar:

Nível	Descrição
Nível de Processo	Configura o domínio para usar um nome de entidade de serviço (SPN) exclusivo e um arquivo de keytab para cada nó e cada serviço de aplicativo em um nó. O número de SPNs e de arquivos keytab exigidos para cada nó depende do número de processos de serviço de aplicativo que são executados no nó. Use a opção de nível de processo para domínios que exigem alto nível de segurança, como domínios de produção.
Nível de Nó	Configure o domínio para compartilhar SPNs e arquivos keytab em um nó. Essa opção requer um arquivo keytab e SPN para o nó e todos os serviços de aplicativo executados no nó. Ele também requer um arquivo keytab e um SPN separado para todos os processos HTTP no nó. Use a opção de nível de nó para domínios que não exigem alto nível de segurança, como domínios de teste e desenvolvimento.

- Clique em **Avançar**.

A página **Parâmetros de Autenticação - Autenticação Kerberos** é exibida.

- Insira os parâmetros de domínio e de nó para gerar o formato do SPN.

A seguinte tabela descreve os parâmetros que você precisa especificar:

Aviso	Descrição
Nome do Domínio	O nome do domínio. O nome não deve ter mais de 128 caracteres e deve ser somente ASCII de 7 bits. Ele não pode conter espaços nem qualquer um dos seguintes caracteres: ` % * + ; " ? , < > \ /
Nome do nó	Nome do nó da Informática.
Nome de host do nó	Nome do host totalmente qualificado ou endereço IP da máquina na qual você deseja criar o nó. O nome de host do nó não pode conter o caractere sublinhado (_). Nota: Não use <i>localhost</i> . O nome de host deve identificar explicitamente a máquina.
Nome do Realm do Serviço	Nome do realm Kerberos para os serviços do domínio Informática. O nome do realm deve estar em maiúsculas.

Se você definir o principal de serviço em nível de nó, o utilitário exibirá o botão **+Node**. Se você definir o principal de serviço em nível de processo, o utilitário exibirá os botões **+Node** e **+Service**.

- Para gerar o formato do SPN para um nó adicional, clique em **+Node** e especifique o nome do nó e o nome de host.

Você pode inserir vários nós em um domínio.

- Para gerar o formato do SPN para um serviço, clique em **+Service** e especifique o nome do serviço no campo **Serviço no Nó**.

O campo **Serviço no Nó** será exibido somente se você definir o principal de serviço em nível de processo e clicar em **+Service**. Você pode inserir vários serviços para um nó. Os serviços aparecem imediatamente abaixo do nó em que são executados.

- Para remover um nó da lista, clique em **-Node**.

O Informatica SPN Format Generator exclui o nó. Se você tiver adicionado serviços ao nó, os serviços serão excluídos com o nó.

10. Para remover um serviço de um nó, desmarque o campo do nome do serviço.

11. Clique em **Avançar**.

O SPN Format Generator exibe o caminho e o nome do arquivo que contém a lista de entidades de serviço e os nomes do arquivo keytab.

12. Clique em **Concluído** para sair do SPN Format Generator.

O SPN Format Generator gera um arquivo de texto que contém os nomes de SPNs e arquivos keytab no formato necessário para o domínio Informatica.

Executando o Informatica Kerberos SPN Format Generator no UNIX

Você pode executar o Informatica Kerberos SPN Format Generator para gerar um arquivo que mostra o formato correto dos nomes de SPNs e de arquivo keytab exigidos no domínio Informatica.

1. Em uma máquina que hospeda o nó da Informatica, vá para o seguinte diretório da Informatica:
<InformaticaDirectory>/Tools/Kerberos
2. Em uma linha de comando shell, execute o arquivo SPNFormatGenerator.sh.
3. Pressione **Enter** para continuar.
4. Na seção **Nível Principal de Serviço**, selecione o nível usado para definir os principais de serviço Kerberos do domínio.

A seguinte tabela descreve os níveis que você pode selecionar:

Nível	Descrição
1->Nível de Processo	Configura o domínio para usar um nome de entidade de serviço (SPN) exclusivo e um arquivo de keytab para cada nó e cada serviço de aplicativo em um nó. O número de SPNs e de arquivos keytab exigidos para cada nó depende do número de processos de serviço de aplicativo que são executados no nó. Use a opção de nível de processo para domínios que exigem alto nível de segurança, como domínios de produção.
2->Nível de Nó	Configure o domínio para compartilhar SPNs e arquivos keytab em um nó. Essa opção requer um arquivo keytab e SPN para o nó e todos os serviços de aplicativo executados no nó. Ele também requer um arquivo keytab e um SPN separado para todos os processos HTTP no nó. Use a opção de nível de nó para domínios que não exigem alto nível de segurança, como domínios de teste e desenvolvimento.

5. Insira os parâmetros de domínio e de nó necessários para gerar o formato do SPN.

A seguinte tabela descreve os parâmetros que você precisa especificar:

Aviso	Descrição
Nome do Domínio	O nome do domínio. O nome não deve ter mais de 128 caracteres e deve ser somente ASCII de 7 bits. Ele não pode conter espaços nem qualquer um dos seguintes caracteres: ` % * + ; " ? , < > \ /
Nome do nó	Nome do nó da Informatica.
Nome de host do nó	Nome do host totalmente qualificado ou endereço IP da máquina na qual você deseja criar o nó. O nome de host do nó não pode conter o caractere sublinhado (_). Nota: Não use <i>localhost</i> . O nome de host deve identificar explicitamente a máquina.
Nome do Realm do Serviço	Nome do realm Kerberos para os serviços do domínio Informatica. O nome do realm deve estar em maiúsculas.

Se você definir o principal de serviço em nível de nó, o prompt **Adicionar Nó?** será exibido. Se você definir o principal de serviço em nível de processo, o prompt **Adicionar Serviço?** será exibido.

- No prompt **Adicionar Nó?**, digite 1 para gerar o formato do SPN para um nó adicional. Em seguida, insira o nome do nó e o nome do host do nó.

Para gerar os formatos do SPN para vários nós, digite 1 em cada prompt **Adicionar Nó?** e digite um nome de nó e um nome do host do nó.

- No prompt **Adicionar Serviço?** digite 1 para gerar o formato do SPN para um serviço que será executado no nó precedente. Em seguida, digite o nome do serviço.

Para gerar os formatos do SPN para vários serviços, digite 1 em cada prompt **Adicionar Serviço?** e digite um nome do serviço.

- Digite 2 para finalizar os prompts **Adicionar Serviço?** ou **Adicionar Nó?**.

O SPN Format Generator exibe o caminho e o nome do arquivo que contém a lista de entidades de serviço e os nomes do arquivo keytab.

- Pressione Enter para sair do SPN Format Generator.

O SPN Format Generator gera um arquivo de texto que contém os nomes de SPNs e arquivos keytab no formato necessário para o domínio Informatica.

Etapa 5. Analisar o Arquivo de Texto do Formato de SPN e de Keytab

O Kerberos SPN Format Generator gera um arquivo de texto denominado SPNKeytabFormat.txt que lista o formato dos nomes de principal de serviço e de arquivo keytab exigidos pelo domínio Informatica. A lista inclui os nomes de SPN e de arquivo keytab com base no nível principal de serviço selecionado.

Analise o arquivo de texto e verifique se há mensagens de erro.

O arquivo de texto contém as seguintes informações:

Nome da Entidade

Identifica o nó ou o serviço associado ao processo.

SPN

Formato do SPN no banco de dados principal Kerberos. O SPN faz distinção entre maiúsculas e minúsculas. Cada tipo de SPN tem um formato diferente.

Um SPN pode ter um dos seguintes formatos:

Tipo de Keytab	Formato do SPN
NODE_SPN	isp/<NodeName>/<DomainName>@<REALMNAME>
NODE_AC_SPN	_AdminConsole/<NodeName>/<DomainName>@<REALMNAME>
NODE_HTTP_SPN	HTTP/<NodeHostName>@<REALMNAME> Nota: 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	<ServiceName>/<NodeName>/<DomainName>@<REALMNAME>

Nome do Arquivo Keytab

Formato do nome do arquivo keytab a ser criado para o SPN associado no banco de dados principal Kerberos. O nome de arquivo keytab faz distinção entre maiúsculas e minúsculas.

Os nomes de arquivo keytab usam os seguintes formatos:

Tipo de Keytab	Nome do Arquivo Keytab
NODE_SPN	<NodeName>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<ServiceName>.keytab

Tipo de Keytab

Tipo do keytab. O tipo de keytab pode ser um dos seguintes tipos:

- NODE_SPN. O arquivo keytab de um processo do nó.
- NODE_AC_SPN. O arquivo keytab do processo do serviço Informatica Administrator.
- NODE_HTTP_SPN. O arquivo keytab do processo HTTP em um nó.
- SERVICE_PROCESS_SPN. O arquivo keytab de um processo do serviço.

Entidades de Serviço em Nível de Nó

O seguinte exemplo mostra os conteúdos do arquivo SPNKeytabFormat.txt gerado para os principais de serviço em nível de nó:

ENTITY_NAME	SPN	KEY_TAB_NAME
KEY_TAB_TYPE		
Node01	isp/Node01/Infadomain@MY.SVCREALM.COM	Node01.keytab
NODE_SPN		
Node01	HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab
NODE_HTTP_SPN		
Node02	isp/Node02/Infadomain@MY.SVCREALM.COM	Node02.keytab

NODE_SPN		
Node02	HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab
NODE_HTTP_SPN		
Node03	isp/Node03/Infadomain@MY.SVCREALM.COM	Node03.keytab
NODE_SPN		
Node03	HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab
NODE_HTTP_SPN		

Principal de Serviço em Nível de Processo

O seguinte exemplo mostra os conteúdos do arquivo SPNKeytabFormat.txt gerados para os principais de serviço em nível de processo:

ENTITY_NAME	SPN
KEY_TAB_NAME	KEY_TAB_TYPE
Node01	isp/Node01/Infadomain@MY.SVCREALM.COM
Node01.keytab	NODE_SPN
Node01	_AdminConsole/Node01/Infadomain@MY.SVCREALM.COM
_AdminConsole.keytab	NODE_AC_SPN
Node01	HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab	NODE_HTTP_SPN
Node02	isp/Node02/Infadomain@MY.SVCREALM.COM
Node02.keytab	NODE_SPN
Node02	_AdminConsole/Node02/Infadomain@MY.SVCREALM.COM
_AdminConsole.keytab	NODE_AC_SPN
Node02	HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab	NODE_HTTP_SPN
Service10:Node01	Service10/Node01/Infadomain@MY.SVCREALM.COM
Service10.keytab	SERVICE_PROCESS_SPN
Service100:Node02	Service100/Node02/Infadomain@MY.SVCREALM.COM
Service100.keytab	SERVICE_PROCESS_SPN
Service200:Node02	Service200/Node02/Infadomain@MY.SVCREALM.COM
Service200.keytab	SERVICE_PROCESS_SPN

Etapa 6. Criar os Nomes Principais de Serviço e os Arquivos Keytab

Depois de gerar a lista de SPN e os nomes do arquivo keytab no formato exigido pela Informatica, envie uma solicitação para o administrador do Kerberos para adicionar os SPNs ao banco de dados principal do Kerberos e criar arquivos keytab.

Use as seguintes diretrizes ao criar o SPN e os arquivos keytab:

O nome da entidade de segurança do usuário (UPN) deve ser igual ao SPN.

Ao criar uma conta de usuário para a entidade de segurança de serviço, você deve definir o UPN com o mesmo nome que o SPN. Os serviços de aplicativo no domínio Informatica podem atuar como um serviço ou um cliente dependendo da operação. Você deve configurar a entidade de segurança de serviço de forma que ela seja identificável pelos mesmos UPN e SPN.

Uma conta de usuário deve ser associada a apenas um SPN. Não defina vários SPNs para uma conta de usuário.

Ative de delegação no Microsoft Active Directory.

Você deve ativar a delegação para todas as contas de usuário com entidades de segurança de serviço usadas no domínio Informatica. No Serviço Microsoft Active Directory, defina a opção **Confiar neste usuário para delegação a qualquer serviço (apenas Kerberos)** para cada conta de usuário na qual você definir um SPN.

A autenticação delegada acontece quando um usuário é autenticado com um serviço e esse serviço usa as credenciais do usuário autenticado para se conectar a outro serviço. Como os serviços no domínio Informatica precisam se conectar a outros serviços para concluir uma operação, o domínio Informatica requer que a opção de delegação esteja ativada no Microsoft Active Directory.

Por exemplo, quando um cliente do PowerCenter se conecta ao Serviço do Repositório do PowerCenter, a conta de usuário do cliente é autenticada com a entidade de segurança do Serviço do Repositório do PowerCenter. Quando o Serviço do Repositório do PowerCenter se conecta ao Serviço de Integração do PowerCenter, a entidade de segurança do Serviço do Repositório do PowerCenter pode usar a credencial de usuário do cliente para se autenticar no Serviço de Integração do PowerCenter. Não é necessário que a conta de usuário do usuário também se autentique no Serviço de Integração do PowerCenter.

Use o utilitário ktpass para criar os arquivos keytab de entidades de segurança de serviço.

O Microsoft Active Directory fornece o utilitário ktpass para criar arquivos keytab. A Informatica oferece suporte à autenticação Kerberos somente no Microsoft Active Directory e certificou somente arquivos keytab criados com ktpass.

Os arquivos keytab de um nó devem estar disponíveis na máquina que o hospeda. Por padrão, os arquivos keytab são armazenados no seguinte diretório: <INFA_HOME>/isp/config/keys.

Quando você receber os arquivos keytab do administrador do Kerberos, copie-os para o diretório especificado para os arquivos keytab usados no domínio Informatica.

Solução de Problemas dos Nomes Principais de Serviço e dos Arquivos Keytab

Você pode usar os utilitários Kerberos para verificar se o principal de serviço e os nomes do arquivo keytab criados pelo administrador do Kerberos correspondem à entidade de serviço e aos nomes do arquivo keytab solicitados por você. Você também pode usar os utilitários para determinar o status do KDC (Centro de Distribuição de Chaves).

Você pode usar os utilitários Kerberos *setspn*, *kinit* e *klist* para exibir e verificar os SPNs e os arquivos 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.

Nota: Os seguintes exemplos mostram maneiras de usar os utilitários Kerberos para verificar se os SPNs e os arquivos keytab são válidos. Os exemplos podem ser diferentes da maneira como o administrador do Kerberos usa os utilitários para criar os SPNs e os arquivos keytab necessários para o domínio Informatica. 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:

klist

Você pode usar *klist* para listar os principais do 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 <keytab_file>
```

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

```
Keytab name: FILE:int_srvc01.keytab
KVNO Timestamp Principal
-----
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
```

kinit

Você pode usar o *kinit* para solicitar uma concessão de tíquete para uma conta de usuário para verificar se o KDC está em execução e se ele pode conceder tíquetes. Para solicitar uma concessão de tíquete para uma conta de usuário, execute o seguinte comando:

```
kinit <user_account>
```

Você também pode usar o *kinit* para solicitar uma concessão de tíquete e verificar se o arquivo keytab pode ser usado para estabelecer uma conexão Kerberos. Para solicitar uma concessão de tíquete para um SPN, execute o seguinte comando:

```
kinit -V -k -t <keytab_file> <SPN>
```

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

```
Using default cache: /tmp/krb5cc_10000073
Using principal: int_srvc01/node01_vMPE/Domn96_vMPE@REALM
Using keytab: int_srvc01.keytab
Authenticated to Kerberos v5
```

setspn

Você pode usar o *setspn* para exibir, modificar ou excluir o SPN de uma conta do serviço do Active Directory. Na máquina que hospeda o serviço do Active Directory, abra uma janela de linha de comando e execute o comando.

Para exibir os SPNs associados a uma conta de usuário, execute o seguinte comando:

```
setspn -L <user_account>
```

O seguinte exemplo de saída mostra o SPN associado à conta de usuário *is96svc*:

```
Registered ServicePrincipalNames for CN=is96svc,OU=AllSvcAccts,OU=People,
DC=ds,DC=intrac0rp,DC=zec0rp:
    int_srvc01/node02_vMPE/Domn96_vMPE
```

Para exibir as contas de usuário associadas a um SPN, execute o seguinte comando:

```
setspn -Q <SPN>
```

O seguinte exemplo de saída mostra a conta de usuário associada ao SPN *int_srvc01/node02_vMPE/Domn96_vMPE*:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
CN=is96svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
    int_srvc01/node02_vMPE/Domn96_vMPE

Existing SPN found!
```

Para procurar SPNs duplicados, execute o seguinte comando:

```
setspn -X
```

O seguinte exemplo de saída mostra várias contas de usuário associadas a um SPN:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
Processing entry 1125
HOST/mtb01.REALM is registered on these accounts:
    CN=Team1svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
    CN=MTB1svc,OU=IIS,OU=WPC960K3,OU=WINServers,DC=ds,DC=intrac0rp,DC=zec0rp
```

Nota: Procurar SPNs duplicados pode levar muito tempo e usar uma grande quantidade de memória.

kdestroy

Você pode usar o *kdestroy* para excluir os tíquetes ativos de autorização Kerberos e os caches de credenciais de usuário contidos neles. Se você executar o *kdestroy* sem parâmetros, excluirá o cache de credenciais padrão.

Etapa 7. Configurar a Autenticação Kerberos para o Domínio

Execute o comando `infasetup` para alterar a autenticação do domínio Informatica para a autenticação de rede Kerberos.

Nota: Verifique se o check-in de todos os objetos de repositório foi feito antes de configurar o domínio para usar a autenticação Kerberos.

Quando você executa o comando `infasetup` para alterar a autenticação do domínio, o comando cria os seguintes domínios de segurança LDAP:

- Domínio de segurança interno. O domínio de segurança interno é um domínio de segurança LDAP com o nome `_infaInternalNamespace`. O domínio de segurança `_infaInternalNamespace` contém a conta de usuário do administrador padrão criada quando você configura a autenticação Kerberos. Depois de configurar a autenticação Kerberos, você não poderá adicionar usuários ao domínio de segurança `_infaInternalNamespace` ou excluí-lo.
- Domínio de segurança do realm do usuário. O domínio de segurança do realm do usuário é um domínio de segurança LDAP vazio com o mesmo nome do realm do usuário Kerberos. Depois de configurar a autenticação Kerberos, você poderá importar os usuários do banco de dados principal Kerberos no domínio de segurança do realm do usuário.

O comando `infasetup` também cria uma conta de usuário do administrador. Especifique o nome de usuário do administrador. Depois de configurar a autenticação Kerberos, o domínio de segurança `_infaInternalNamespace` conterá a conta de usuário do administrador.

Para configurar o domínio para usar a autenticação Kerberos, execute o seguinte comando:

```
infasetup switchToKerberosMode
```

1. Em um nó de gateway, execute o comando `infasetup` para alterar a autenticação do domínio.
No prompt de comando, vá para o diretório onde os programas de linha de comando da Informatica estão localizados. Por padrão, os programas de linha de comando são instalados no seguinte diretório:
`<InformaticaInstallationDir>/isp/bin`
2. Execute o comando `infasetup` com as opções e os argumentos necessários.
Insira os seguintes comandos:
 - Windows: `infasetup switchToKerberosMode`
 - UNIX: `infasetup.sh switchToKerberosMode`

A tabela a seguir descreve as opções para o comando `switchToKerberosMode`:

Opção	Argumento	Descrição
-administratorName -ad	administrator_name	Nome de usuário da conta de administrador de domínio criada quando você configura a autenticação Kerberos. A conta de usuário deve estar no banco de dados principal Kerberos. Depois de configurar a autenticação Kerberos, esse usuário é incluído no domínio de segurança <i>_infalInternalNamespace</i>
-ServiceRealmName -srn	realm _name_of_node_spn	Nome do realm Kerberos ao qual os serviços do domínio Informatica pertencem. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas. O nome do realm de serviço e o nome do realm do usuário devem ser iguais.
-UserRealmName -urn	realm _name_of_user_spn	Nome do realm Kerberos ao qual os usuários do domínio Informatica pertencem. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas. O nome do realm de serviço e o nome do realm do usuário devem ser iguais.
-SPNShareLevel -spnSL	PROCESS NODE	Nível principal de serviço do domínio. Defina a propriedade como um dos seguintes níveis: <ul style="list-style-type: none"> - Processo. O domínio exige um nome principal de serviço (SPN) exclusivo e um arquivo keytab para cada nó e cada serviço em um nó. O número de SPNs e os arquivos keytab necessários para cada nó depende do número de processos do serviço que são executados no nó. Use a opção de nível de processo se o domínio necessitar de um alto nível de segurança, como um domínio de produção. - Nó. O domínio usa um SPN e o arquivo keytab do nó e todos os serviços executados no nó. Ele também requer um arquivo keytab e um SPN separado para todos os processos HTTP no nó. Use a opção de nível de nó se o domínio não necessitar de um alto nível de segurança, como um domínio de teste ou de desenvolvimento. O padrão é processo.

O comando `switchToKerberosMode` altera o modo de autenticação do domínio de autenticação de usuário nativa ou LDAP para autenticação de rede Kerberos.

Etapa 8. Atualizar os Nós no Domínio

Execute o comando `infasetup` para atualizar todos os outros nós no domínio com as informações do servidor de autenticação Kerberos.

Atualize todos os nós de gateway e de funcionário com as informações do servidor de autenticação Kerberos, exceto o nó de gateway no qual você executou o comando `switchToKerberosMode`.

Para atualizar os nós de gateway e do funcionário, use os seguintes comandos:

infasetup UpdateGatewayNode

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

infasetup UpdateWorkerNode

Use o comando `UpdateWorkerNode` para definir os parâmetros da autenticação Kerberos em um nó do funcionário no domínio. Se o domínio tiver vários nós do funcionário, execute o comando `UpdateWorkerNode` em cada um deles.

1. Em uma máquina que hospeda um nó da Informatica, execute o comando `infasetup` para atualizar o nó.
No prompt de comando, vá para o diretório onde os programas de linha de comando da Informatica estão localizados. Por padrão, os programas de linha de comando são instalados no seguinte diretório:
`<InformaticaInstallationDir>/isp/bin`
2. 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`

A seguinte tabela descreve as opções para atualizar as informações de autenticação Kerberos para um nó:

Opção	Argumento	Descrição
<code>-EnableKerberos</code> <code>-krb</code>	<code>enable_kerberos</code>	Configura o domínio Informatica para usar a autenticação Kerberos.
<code>-ServiceRealmName</code> <code>-srn</code>	<code>realm</code> <code>_name_of_node_spn</code>	Nome do realm Kerberos ao qual os serviços do domínio Informatica pertencem. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas. O nome do realm de serviço e o nome do realm do usuário devem ser iguais.
<code>-UserRealmName</code> <code>-urn</code>	<code>realm</code> <code>_name_of_user_spn</code>	Nome do realm Kerberos ao qual os usuários do domínio Informatica pertencem. O nome do realm deve estar em letras maiúsculas e fazer distinção entre maiúsculas e minúsculas. O nome do realm de serviço e o nome do realm do usuário devem ser iguais.

Etapa 9. Atualizar as Máquinas Cliente

Copie o arquivo de configuração Kerberos e defina a variável de ambiente nas máquinas que hospedam os clientes Informatica. Você também deve configurar o navegador para acessar os aplicativos da Web da 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 as máquinas cliente.

Copie o arquivo de configuração para cada máquina que hospeda um cliente Informatica. Você deve copiar o arquivo `krb5.conf` para o seguinte diretório: <Diretório do Cliente Informatica>/shared/security

Defina as variáveis de ambiente KRB5_CONFIG com o arquivo de configuração Kerberos.

Use a variável de ambiente KRB5_CONFIG para armazenar o caminho e o nome do arquivo de configuração Kerberos, `krb5.conf`. Você deve definir a variável de ambiente KRB5_CONFIG em cada máquina que hospeda um cliente Informatica.

Configure o navegador da Web.

Se o domínio Informatica é executado em uma rede com autenticação Kerberos, você deve configurar o navegador para permitir o acesso aos aplicativos da Web Informatica. No Microsoft Internet Explorer e no Google Chrome, adicione a URL do aplicativo da Web Informatica à lista de sites confiáveis. Se você estiver usando o Chrome versão 41 ou posterior, deverá definir também as diretivas

`AuthServerWhitelist` e `AuthNegotiateDelegateWhitelist`.

No UNIX, crie um arquivo de cache de credenciais para conexão única

Para executar os programas de linha de comando da Informatica no UNIX com conexão única, você deve gerar um arquivo de cache de credenciais para autenticar a conta de usuário que executa os comandos na rede Kerberos. Use o utilitário `kinit` no MIT Kerberos para gerar o arquivo de cache de credenciais. O arquivo de cache de credenciais permite que um usuário execute os comandos sem as opções de nome do usuário e senha.

Se você usar um arquivo de cache de credenciais, deverá definir o caminho e o nome de arquivo padrão para o cache de credenciais na variável de ambiente KRB5CCNAME.

Para obter mais informações sobre como executar os programas de linha de comando da Informatica no UNIX com conexão única, consulte a *Referência de Comandos da Informatica*.

Etapa 10. Iniciar o Domínio Informatica

Depois de configurar o domínio Informatica para usar a autenticação Kerberos, inicie o domínio e a ferramenta Administrator.

1. No Windows, você pode iniciar o serviço Informatica pelo Painel de Controle ou pelo menu Iniciar.

Para iniciar o Informatica no Menu Iniciar do Windows, clique em **Programas > Informatica [Versão] > Servidor**. Clique com o botão direito em **Iniciar os Serviços Informatica** e selecione **Executar como Administrador**.

No UNIX, execute o seguinte comando para iniciar o daemon da Informatica:

```
infaservice.sh startup
```

Por padrão, o `infaservice.sh` é instalado no seguinte diretório: <INFA_HOME>/tomcat/bin

2. Inicie o Informatica Administrator.

Use a seguinte URL para iniciar a ferramenta Administrator: `http://<fully qualified hostname>:<http port>`. Se você tiver configurado a ferramenta Administrator para usar uma conexão segura, use o protocolo HTTPS: `https://<fully qualified hostname>:<http port>`

Quando você inicia a ferramenta Administrator, deve adicionar a URL à lista de sites confiáveis do navegador.

3. Selecione o domínio de segurança para sua conta de usuário.

Se você usa a autenticação Kerberos, a rede usará logon único. Você não precisa fazer logon na ferramenta Administrator com nome de usuário e senha.

Após Configurar a Autenticação Kerberos

Se o nível principal de serviço do domínio estiver em nível de processo, o domínio exigirá um SPN e um arquivo keytab para cada serviço criado no domínio. Antes de ativar um serviço, verifique se um SPN e um arquivo keytab estão disponíveis para o serviço. O Kerberos não poderá autenticar o serviço de aplicativo se ele não tiver um arquivo keytab no diretório da Informatica.

Se os SPNs e os arquivos keytab não estiverem disponíveis para os serviços de aplicativo que você planeja criar no domínio, o SPN e o arquivo keytab deverão ser criados antes que você ative o serviço. Você pode usar o Informatica Kerberos SPN Format Generator para gerar o formato do nome do SPN e do arquivo keytab do serviço. Para economizar tempo, escolha os nomes dos serviços que você deseja criar e os nós em que eles serão executados. Em seguida, execute o utilitário para gerar o formato do nome do SPN e do arquivo keytab de todos os serviços de uma vez.

Para obter mais informações sobre a execução do Informatica Kerberos SPN Format Generator, consulte [“Etapa 4. Gerar o Nome Principal e o Formato Keytab” na página 37](#).

Envie uma solicitação ao administrador do Kerberos para adicionar os SPNs ao banco de dados principal e para criar o arquivo keytab correspondente.

Quando você receber os arquivos keytab do administrador do Kerberos, copie-os no diretório especificado para o arquivo keytab. Por padrão, os arquivos keytab são armazenados no seguinte diretório:

`<INFA_HOME>/isp/config/keys`

Se o principal de serviço do domínio estiver em nível de nó, você poderá criar e ativar serviços de aplicativo sem criar SPNs nem arquivos keytab adicionais.

Bibliotecas personalizadas Kerberos

Você pode configurar clientes de banco de dados personalizados ou nativos e processos Informatica dentro de um domínio Informatica para usar bibliotecas Kerberos personalizadas em vez das bibliotecas Kerberos padrão usadas pelo Informatica.

Você pode querer usar bibliotecas Kerberos personalizadas nos seguintes cenários:

Use bibliotecas Kerberos personalizadas em um domínio Informatica não configurado para usar o Kerberos.

Nesse cenário, você tem um cliente de banco de dados que se conecta a bancos de dados de origem e destino usados em mapeamentos. Os bancos de dados são configurados para usarem bibliotecas

Kerberos personalizadas para autenticação. No entanto, o domínio Informatica não está configurado para usar a autenticação Kerberos.

Para permitir que o cliente de banco de dados se conecte a bancos de dados por meio do Informatica, você pode disponibilizar as bibliotecas personalizadas ao cliente de banco de dados. No entanto, os processos do domínio Informatica não usam as bibliotecas Kerberos personalizadas para autenticação.

Use bibliotecas Kerberos personalizadas em um domínio Informatica protegido por Kerberos.

Nesse cenário, o cliente de banco de dados se conecta aos bancos de dados de origem ou destino configurados para usar bibliotecas Kerberos personalizadas. No entanto, o domínio Informatica é configurado para usar as bibliotecas Kerberos Informatica padrão para autenticação.

Para permitir que o cliente de banco de dados se conecte aos bancos de dados pelo Informatica, você pode configurar o domínio Informatica para carregar as bibliotecas Kerberos personalizadas em vez das bibliotecas Informatica Kerberos padrão. Todos os processos e subprocessos do domínio Informatica usam as bibliotecas Kerberos personalizadas.

Se necessário, você pode remover os vínculos para as bibliotecas personalizadas Kerberos e atualizar os nós no domínio para os quais reverter usando as bibliotecas Kerberos Informatica padrão.

Usando bibliotecas Kerberos personalizadas

Use o comando `infasetup updateMitKerberosLinkage` para configurar clientes de banco de dados e serviços de aplicativo em um domínio Informatica para usar bibliotecas Kerberos personalizadas.

Você deve especificar o diretório que contém as bibliotecas Kerberos que deseja usar. É possível copiar as bibliotecas para cada nó ou para um local compartilhado que seja acessível a todos os nós no domínio.

Se o domínio Informatica usar a autenticação Kerberos, certifique-se de que as bibliotecas Kerberos personalizadas que você deseja usar sejam do mesmo número de versão das bibliotecas Kerberos que o Informatica usa por padrão.

1. Coloque as bibliotecas Kerberos personalizadas em um local que seja acessível a todos os nós no domínio Informatica.
2. Desligue o domínio.
3. Execute o comando `infasetup updateMitKerberosLinkage` em cada nó do domínio.

A seguinte tabela descreve as opções e os argumentos do comando `infasetup updateMitKerberosLinkage`:

Opção	Argumento	Descrição
-useKerberos -krb	verdadeiro falso	<p>Obrigatório. Defina esse valor como <code>true</code> se o domínio Informatica usa a autenticação Kerberos. Se <code>true</code>, os processos Informatica fazem chamadas Kerberos com as bibliotecas Kerberos padrão ou com as bibliotecas no diretório especificado com a opção <code>-mkd</code>.</p> <p>Defina esse valor como <code>false</code> se o domínio Informatica não usar a autenticação Kerberos. Se for <code>false</code>, o domínio Informatica não carregará bibliotecas Kerberos. Clientes de banco de dados realizam chamadas Kerberos com as bibliotecas personalizadas especificadas no diretório especificado com a opção <code>-mkd</code>.</p>
-mitKerberosDirectory -mkd	kerberos_library_directory_node_spn	<p>Opcional. O diretório que contém as bibliotecas Kerberos personalizadas. O diretório deve conter os arquivos de biblioteca. Não é possível usar links simbólicos.</p> <p>Se a opção <code>-krb</code> for <code>true</code>, certifique-se de que as bibliotecas Kerberos personalizadas que você deseja usar tenham o mesmo número de versão das bibliotecas Kerberos que o Informatica usa por padrão.</p> <p>Se houver várias versões da mesma biblioteca, todas as versões deverão ser do mesmo tamanho e ter a mesma soma de verificação. Por exemplo, se o diretório contiver duas versões de <code>libkrb5</code>, como <code>libkr5.so.3</code> e <code>libkrb5.so</code>, ambas as bibliotecas deverão ter o mesmo valor de tamanho e soma de verificação de arquivo.</p> <p>Se o diretório especificado estiver vazio, o comando removerá todas as bibliotecas Kerberos personalizadas do domínio Informatica.</p> <p>Se a opção <code>-krb</code> for <code>true</code>, mas você não especificar um diretório de biblioteca, o Informatica usará as bibliotecas Kerberos padrão.</p>

- Reinicie o domínio depois de executar o comando em todos os nós.

Revertendo para as bibliotecas Kerberos padrão

Execute o comando `infasetup restoreMitKerberosLinkage` nos nós de um domínio Informatica para restaurar os vínculos para as bibliotecas Kerberos padrão usadas pelo Informatica. O comando remove os vínculos para qualquer biblioteca Kerberos personalizada existente dentro do domínio Informatica.

- Desligue o domínio.
- Execute o comando `infasetup restoreMitKerberosLinkage` em cada nó do domínio.
O comando não usa opções ou argumentos.
- Reinicie o domínio depois de executar o comando em todos os nós.

CAPÍTULO 5

Segurança de domínio

Este capítulo inclui os seguintes tópicos:

- [Visão Geral da Segurança do Domínio, 53](#)
- [Comunicação Segura Dentro do Domínio, 54](#)
- [Conexões Seguras com um Serviço de Aplicativo da Web, 65](#)
- [Pacotes de criptografia para o domínio Informatica, 69](#)
- [Origens e Destinos Seguros, 71](#)
- [Armazenamento de Dados Seguro, 73](#)
- [Serviços de Aplicativo e Portas, 77](#)

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. Você pode especificar a palavra-chave que o instalador usa para gerar a chave de criptografia. 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 e o navegador

Origens e destinos

Você pode ativar a comunicação segura entre o Serviço de Integração de Dados e o Serviço de Integração do PowerCenter 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 com base em uma palavra-chave que você especifica durante a instalação. O Informatica usa a chave de criptografia para criptografar e descriptografar dados confidenciais que são armazenados no domínio.

Comunicação Segura Dentro do Domínio

Você pode usar a opção de Comunicação Segura para proteger a conexão entre serviços e entre os serviços e os gerenciadores de serviços no domínio. Você também pode ativar a segurança para fluxos de trabalho e usar bancos de dados seguros para os repositórios criados no domínio.

Após proteger o domínio, configure os aplicativos cliente Informatica para operar com um domínio seguro.

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

Requisitos para a Comunicação Segura no Domínio

Antes de habilitar a comunicação segura no domínio, 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.

Se você usar a criptografia RSA, deverá usar 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`.

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_keystore.pem` e um armazenamento de chaves no formato JKS denominado `infa_keystore.jks`.

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.

Para obter mais informações sobre como criar um armazenamento de chaves e truststore personalizado, consulte o artigo da Informatica How-To Library Como Criar Arquivos de Armazenamento de Chaves e Truststore para Comunicação Segura no Domínio Informatica:

<https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf>

Após proteger o domínio, configure os aplicativos cliente Informatica para operar com um domínio seguro.

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 e truststore 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
<code>-DomainOptions</code> <code>-do</code>	<code>option_name=value</code>	Defina a seguinte opção para configurar a comunicação segura no domínio: <code>TLSMode=True</code>

3. Desative 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. Obrigatório se você usar seu certificado SSL. Diretório que contém os arquivos de truststore. O domínio Informatica exige que o certificado SSL esteja no formato PEM e em arquivos Java Keystore (JKS). O diretório deve conter arquivos de truststore nos formatos PEM e JKS. Os arquivos de truststore devem ser denominados infa_truststore.jks e infa_truststore.pem. 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. Obrigatório se você usar seu certificado SSL. 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 e de truststore para todos os nós no domínio.

6. Reinicie o domínio.

Depois de concluir a atualização de todos os nós no domínio, você deve atualizar as máquinas que hospedam as ferramentas do cliente Informatica. Defina a localização dos certificados SSL nas variáveis de ambiente de truststore da Informatica.

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 e truststore quando você 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. Desative 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.
-NodeTruststore -nt	node_truststore_directory	Opcional se você usar o certificado SSL padrão da Informatica. Obrigatório se você usar seu certificado SSL. Diretório que contém os arquivos de truststore. O domínio Informatica exige que o certificado SSL esteja no formato PEM e em arquivos Java Keystore (JKS). O diretório deve conter arquivos de truststore nos formatos PEM e JKS. Os arquivos de truststore devem ser denominados infa_truststore.jks e infa_truststore.pem. 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. Obrigatório se você usar seu certificado SSL. 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 e de truststore para todos os nós no domínio.

9. Reinicie o domínio.

Depois de concluir a atualização de todos os nós no domínio, você deve atualizar as máquinas que hospedam as ferramentas do cliente Informatica. Defina a localização dos certificados SSL nas variáveis de ambiente de truststore da Informatica.

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.

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 de host da máquina que hospeda o banco de dados seguro. Se você especificar um nome de host, o Informatica validará o nome de host incluído na cadeia de conexão em relação ao nome de host no certificado SSL.

cryptoProtocolVersion

Obrigatório. 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 5
-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 de host da máquina que hospeda o banco de dados seguro. Se você especificar um nome de host, o Informatica validará o nome de host incluído na cadeia de conexão em relação ao nome de host no certificado SSL.

cryptoProtocolVersion

Obrigatório. 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 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.

Se você usar a criptografia RSA, deverá usar 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 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">- HTTP. Executa o Hub de Serviços da Web somente em HTTP.- HTTPS. Executa o Hub de Serviços da Web somente em HTTPS.- HTTP e HTTPS. Executa o Hub de Serviços da Web nos modos HTTP e HTTPS.
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. Nota: 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 Esquema de URL 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. Nota: 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 [Apêndice C, “Lista padrão de pacotes de criptografia” na página 254](#)

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 v1.1 ou 1.2.
- A lista efetiva deve ser um pacote de criptografia válido para Windows, Java Runtime Environment e OpenSSL.

Configurar o Domínio Informatica para Usar Codificações Avançadas

Se quiser usar conjuntos de codificação avançados que usam o AES-256 para fornecer um nível maior de segurança, você deverá substituir os arquivos de política Java Cryptography Extension (JCE) instalados com o Java Runtime Environment (JRE) em cada nó no domínio pelos arquivos de diretiva JCE com intensidade ilimitada. Os arquivos de diretiva JCE com intensidade ilimitada não contêm restrições em intensidades de criptografia.

1. Baixe o arquivamento Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8.
2. Desligue o domínio.

3. Vá para o seguinte diretório no nó de domínio:

<Diretório de instalação Informatica>\java\jre\lib\security\

4. Substitua os seguintes arquivos JAR pelos arquivos JAR extraídos do arquivamento:

- local_policy.jar
- US_export_policy.jar

5. Reinicie o domínio.

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.

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 listCiphers -l EFFECTIVE -dc true
```

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 de host da máquina que hospeda o banco de dados seguro. Se você especificar um nome de host, o Informatica validará o nome de host incluído na cadeia de conexão em relação ao nome de 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.

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 usa uma palavra-chave que você especificar para criar uma chave de criptografia para criptografar dados confidenciais.

Durante a instalação, você deve especificar uma palavra-chave para o instalador usar para gerar a chave de criptografia do domínio. Todos os nós em um domínio devem usar a mesma chave de criptografia. Se você instalar em vários nós, o instalador usará a mesma chave de criptografia para todos os nós no domínio. Para obter mais informações sobre como gerar uma chave de criptografia para o domínio durante a instalação, consulte os guias de instalação da Informatica.

Após a instalação, você poderá alterar a chave de criptografia do domínio. Execute o comando `infasetup` para gerar uma chave de criptografia e alterá-la no domínio. Depois de alterar a chave de criptografia do domínio, você deverá atualizar o conteúdo dos repositórios no domínio para atualizar os dados criptografados.

Nota: Você deve manter o nome do domínio, a palavra-chave para a chave de criptografia e o arquivo de chave de criptografia em uma localização segura. O nome do domínio, a palavra-chave e a chave de criptografia são necessários para alterar a chave de criptografia do domínio ou mover um repositório para outro domínio. Em caso de perda do arquivo de chave de criptografia, a palavra-chave será necessária para gerar a chave de criptografia novamente. Em caso de perda da palavra-chave e da chave de criptografia, você não poderá alterar a chave de criptografia do domínio nem mover um repositório para outro domínio.

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 *ediga* possui o diretório e pertence ao grupo *infaadmin*. A conta de usuário *ediga* e o grupo *infaadmin* têm as seguintes permissões: `-wx-wx---`

A conta de usuário *ediga* 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 vai renomeá-lo para *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 as seguintes opções necessárias para gerar uma chave de criptografia:

Opção	Argumento	Descrição
-keyword -kw	keyword	A cadeia de texto usada como a palavra de base para gerar uma chave de criptografia. A palavra-chave deve atender aos seguintes critérios: <ul style="list-style-type: none">- Ter entre 8 e 20 caracteres- Incluir pelo menos uma letra maiúscula- Incluir pelo menos uma letra minúscula- Incluir pelo menos um número- Não conter espaços
-domainName -dn	domain_name	Nome do domínio Informatica.
-encryptionKeyLocation -kl	encryption_key_location	Diretório que armazena 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.

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
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	<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>Nota: 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>
-IsDomainMigrated -mig	is_domain_migrated	<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 Verdadeiro.</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.

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 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.
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 Analyst (Banco de dados de preparação)	Nenhuma porta padrão. Insira o número da porta de banco de dados.

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 do Diretor de Dados

A seguinte tabela lista a porta padrão associada ao Serviço do Diretor de Dados:

Tipo	Porta Padrão
Serviço do Diretor de Dados (HTTP)	Nenhuma porta padrão. Insira o número da porta quando você criar o serviço.
Serviço do Diretor de Dados (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)	8085
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.

Tipo	Porta Padrão
Banco de Dados do Depósito de Criação de Perfil	Nenhuma porta padrão. Insira o número da porta de banco de dados.
Banco de dados de tarefas humanas	Nenhuma porta padrão. Insira o número da porta de banco de dados.

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)	O padrão é 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 DBMOVE.

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 DBMOVE.

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 6

Logon único para aplicativos da Web Informatica

Este capítulo inclui os seguintes tópicos:

- [Visão geral do logon único com base em SAML, 80](#)
- [Processo de autenticação do logon único com base em SAML, 80](#)
- [Experiência de usuário de aplicativos da Web, 81](#)
- [Configuração do logon único com base em SAML, 81](#)

Visão geral do logon único com base em SAML

É possível configurar o logon único (SSO) usando a SAML (Security Assertion Markup Language) para a ferramenta Administrator, a ferramenta Analyst e a ferramenta Monitoring.

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. Em um domínio Informatica, o aplicativo da Web Informatica é o provedor de serviços. O Microsoft Active Directory Federation Services (AD FS) 2.0 é o provedor de identidade que autentica os usuários de aplicativos da Web com o repositório de identidade LDAP ou Active Directory da sua organização.

Nota: O logon único com base em SAML não pode ser usado em um domínio Informatica configurado para usar a autenticação Kerberos.

Processo de autenticação do logon único com base em SAML

Aplicativos da Web Informatica e o Active Directory Federation Services trocam informações de autenticação e autorização para permitir o logon único em um domínio Informatica

As etapas a seguir descrevem o fluxo de autenticação de logon único baseado em SAML:

1. Um usuário faz logon em um aplicativo da Web Informatica.
2. O aplicativo envia uma solicitação de autenticação SAML ao AD FS.

3. O AD FS autentica as credenciais do usuário com base nas informações de contas de usuário no repositório de identidade LDAP ou Active Directory.
4. O AD FS cria uma sessão para o usuário e envia um token de assertiva SAML contendo informações relacionadas à segurança sobre o usuário para o aplicativo da Web.
5. O aplicativo valida a afirmação.

Experiência de usuário de aplicativos da Web

Os usuários fazem login em aplicativos da Web Informativa habilitados para usar o login único com base em SAML através de um domínio de segurança que contém contas de login único.

Ao fazer login em um aplicativo da Web, o usuário seleciona o domínio de segurança para login através de login do aplicativo. Usuários habilitados para usar o login único selecionam o domínio de segurança LDAP contendo contas de login único. O usuário então insere seu nome de usuário e senha. As credenciais são enviadas em uma solicitação de autenticação SAML ao AD FS, e o usuário é autenticado.

A autenticação subsequente é gerenciada por meio de cookies de sessão definidos no navegador da Web durante a autenticação inicial. Quando a autenticação é concluída, o usuário pode acessar outro aplicativo da Web Informativa configurado para usar o login único com base em SAML na mesma sessão do navegador, selecionando o domínio de segurança LDAP na página de login do aplicativo. O usuário não precisa fornecer um nome de usuário ou senha.

Quando a autenticação for concluída, o usuário permanecerá conectado a todos os aplicativos da Web Informativa que estiverem em execução na mesma sessão do navegador. Se o AD FS estiver configurado para emitir cookies persistentes, o usuário permanecerá conectado depois de fechar e reiniciar o navegador.

No entanto, se o usuário fizer logout de um aplicativo da Web Informativa, o usuário também será desconectado de outros aplicativos da Web Informativa executados na mesma sessão do navegador.

Usuários não habilitados para usar o login único com base em SAML selecionam o domínio de segurança nativo na página de login do aplicativo da Web e, em seguida, fornecem o nome de usuário e a senha para a conta nativa.

Configuração do login único com base em SAML

Configure o Active Directory Federation Services (AD FS) e o domínio Informativa para usar o login único com base em SAML.

Para configurar o login único com base em SAML para aplicativos da Web Informativa com suporte, execute as seguintes tarefas:

1. Crie um domínio de segurança LDAP para contas de usuário de aplicativos da Web Informativa e, em seguida, importe os usuários para o domínio do Active Directory.
2. Exporte o certificado de assinatura de assertiva do provedor de identidade do AD FS.
3. Importe o certificado de Assinatura de Declaração do Provedor de Identidade para o arquivo de truststore padrão Informativa em cada nó de gateway do domínio.
4. Adicione o Informativa como uma confiança de parte dependente no AD FS e mapeie atributos LDAP para os tipos correspondentes usados em tokens de segurança emitidos pelo AD FS.

5. Adicione a URL para cada aplicativo da Web Informatica ao AD FS.
6. Ative o logon único para aplicativos da Web Informatica no domínio Informatica.

Antes de habilitar o logon único

Certifique-se de que a rede Windows e os nós de gateway do domínio Informatica estejam configurados para usar o logon único.

Valide os seguintes requisitos para garantir que o domínio Informatica possa usar o logon único:

Verifique se os serviços necessários estão implantados e configurados na rede Windows.

O logon único requer os seguintes serviços:

- Microsoft Active Directory
- Microsoft Active Directory Federation Services 2.0

Verifique se os serviços de aplicativos da Web Informatica usam conexões HTTPS seguras.

Por padrão, o AD FS requer que as URLs de aplicativos da Web usem o protocolo HTTPS.

Certifique-se de que os relógios do sistema no host do AD FS e todos os nós de gateway no domínio estejam sincronizados.

O tempo de vida de tokens SAML emitidos pelo AD FS é definido de acordo com o relógio do sistema host do AD FS. Certifique-se de que os relógios do sistema no host do AD FS e todos os nós de gateway no domínio estejam sincronizados.

Para evitar problemas de autenticação, o tempo de vida de um token SAML emitido pelo AD FS será válido se a hora de início e a hora de término definidas no token estiver dentro de 120 segundos da hora do sistema do nó de gateway.

Etapa 1. Criar um domínio de segurança para contas de usuário de aplicativos da Web

Crie um domínio de segurança para contas de usuário de aplicativos da Web que usarão o logon único com base em SAML e, em seguida, importe cada conta de usuário LDAP do Active Directory para o domínio.

Você deve importar as contas LDAP para todos os usuários que usam o logon único com base em SAML para acessar a ferramenta Administrator, a ferramenta Analyst e a ferramenta Monitoring para o domínio de segurança. Depois de importar as contas para o domínio, atribua as funções, os privilégios e as permissões de domínio Informatica apropriados para as contas dentro do domínio de segurança LDAP.

1. Na ferramenta Administrator, clique na guia **Usuários** e selecione a exibição **Segurança**.
2. Clique no menu **Ações** e selecione **Configuração LDAP**.
A caixa de diálogo **Configuração LDAP** é aberta.
3. Clique na guia **Conectividade LDAP**.
4. Configure as propriedades de conexão para o servidor Active Directory.

A seguinte tabela descreve as propriedades de conexão do servidor:

Propriedade	Descrição
Nome do Servidor	Nome do host ou endereço IP do servidor Active Directory.
Porta	Porta de escuta do servidor. O valor padrão é 389.
Serviço de Diretório LDAP	Selecione Microsoft Active Directory.
Nome	Nome diferenciado (DN) do usuário LDAP de entidade de segurança. 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.
Senha	Senha do usuário LDAP principal.
Usar Certificado SSL	Indica que o servidor LDAP usa o protocolo SSL (Secure Socket Layer). Se o servidor LDAP usar SSL, você deverá importar o certificado para um arquivo de truststore em cada nó do gateway dentro no domínio Informatica. Você também deve definir as variáveis de ambiente INFA_TRUSTSTORE e INFA_TRUSTSTORE_PASSWORD se não importar o certificado para o truststore do Informatica padrão.
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. Ative essa opção.
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 (nomes distintos) 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. 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 valor padrão é 1000.

A seguinte imagem mostra os detalhes de conexão para um servidor LDAP definido no painel Conectividade LDAP da caixa de diálogo **Configuração LDAP**.

LDAP Configuration

Fields marked with an asterisk (*) are required.

LDAP Connectivity Security Domains Schedule

Server name and port for the LDAP server

Server Name *

Port *

LDAP Directory Service *

Distinguished name and password of the principal user (Leave blank for anonymous login)

Name

Password

☐ Modify Password

SSL certificate for the LDAP server

☒ Use SSL Certificate

☐ Trust LDAP Certificate

☐ Not Case Sensitive

Group attribute definition

Group Membership Attribute

Maximum number of users to import for a security domain

Maximum size *

Test connection

Synchronize Now **OK** **Cancel**

5. Clique em **Testar Conexão** para verificar se a conexão com o servidor Active Directory é válida.
6. Clique na guia **Domínios de Segurança**.
7. Clique em **Adicionar** para criar um domínio de segurança.
8. Insira as propriedades do domínio de segurança.

A seguinte tabela descreve as propriedades do domínio de segurança:

Propriedade	Descrição
Domínio de Segurança	<p>Nome do domínio de segurança LDAP. O nome não faz distinção entre maiúsculas e minúsculas, e deve ser exclusivo no domínio. O nome não pode ter mais de 128 caracteres, nem conter os seguintes caracteres especiais:</p> <p>, + / < > @ ; \ % ?</p> <p>O nome pode conter um caractere de espaço ASCII, exceto para o primeiro e o último caracteres. Nenhum outro caractere de espaço é permitido.</p>
Base de pesquisa do usuário	<p>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.</p> <p>No Active Directory, o nome distinto de um objeto de usuário pode ser cn=UserName,ou=OrganizationalUnit,dc=DomainName, em que a série de nomes distintos relativos indicada por dc=DomainName identifica o domínio DNS do objeto.</p>

Propriedade	Descrição
Filtro de usuário	Uma sequência de consulta LDAP que especifica os critérios de pesquisa por usuários no Active Directory. O filtro pode especificar os tipos de atributos, os valores de declaração e os critérios de correspondência. Para o Active Directory, formate a cadeia de consulta como: sAMAccountName=<account>
Base de pesquisa do grupo	Nome distinto (DN) da entrada que serve como ponto de partida para procurar nomes de grupos no Active Directory.
Filtro de grupo	Uma cadeia de consulta LDAP específica os critérios para pesquisar grupos no serviço de diretório.

A seguinte imagem mostra as propriedades para um domínio de segurança LDAP chamado SAML_USERS, definido no painel Domínios de Segurança da caixa de diálogo **Configuração LDAP**. O filtro de usuário é definido para importar todos os usuários que começam com a letra "s".

LDAP Configuration

Fields marked with an asterisk (*) are required.

LDAP Connectivity **Security Domains** Schedule

You can specify multiple security domains for LDAP users and groups. Click Add to add a new security domain. + Add

▼ Add new Security Domain Preview Cancel

Security Domain *	SAML_USERS
User search base	CN=USERS,DC=PLATFORMKRB,DC=COM
User filter	samAccountName=s*
Group search base	
Group filter	

Synchronize Now
OK
Cancel

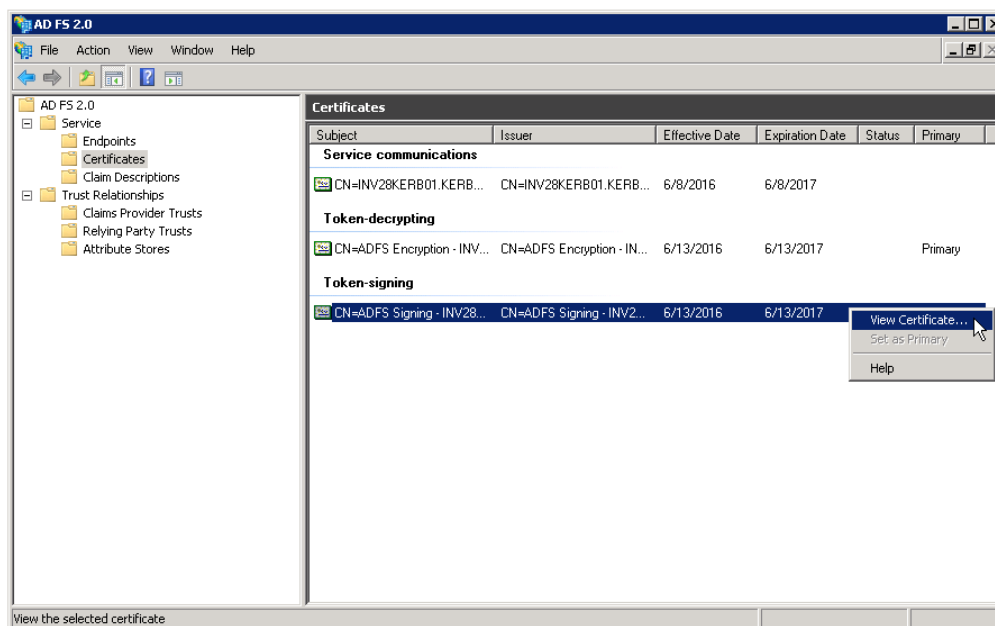
9. Clique em **Sincronizar Agora**.
O domínio de segurança aparece na exibição Usuários.
10. Expanda o domínio no Navegador para visualizar as contas de usuário importadas.
11. Defina as funções, os privilégios e as permissões apropriados das contas de usuário que acessarão cada aplicativo da Web.

Etapa 2. Exportar o certificado do AD FS

Exporte o certificado de Assinatura de Declaração do AD FS.

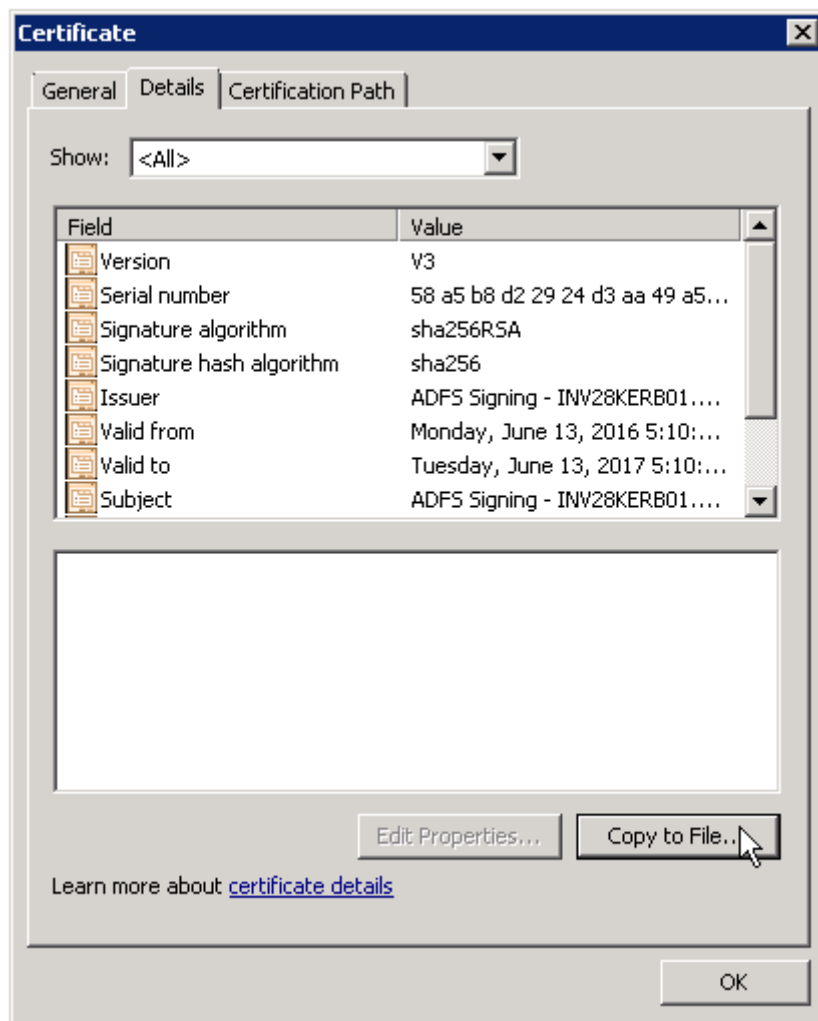
O certificado é um certificado X.509 padrão usado para assinar as afirmações nos tokens SAML que o AD FS emite para aplicativos da Web Informatica. É possível gerar um certificado SSL (Secure Sockets Layer) autoassinado para o AD FS ou pode obter um certificado de uma autoridade de certificação e importá-lo para o AD FS.

1. Faça logon no Console de Gerenciamento do AD FS.
2. Expanda a pasta **Serviço > Certificados**.
3. Clique com o botão direito do mouse no certificado em Assinatura de token no painel Certificados e selecione **Exibir Certificado**, como mostra a imagem a seguir:



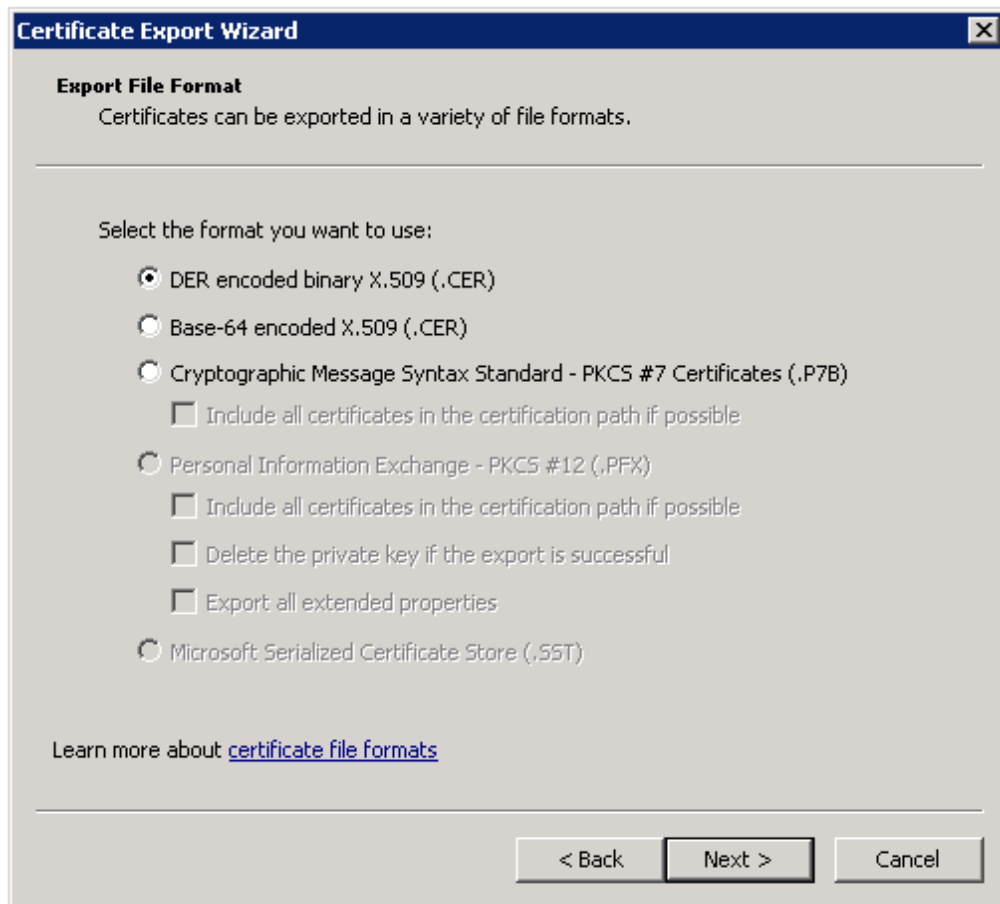
A caixa de diálogo **Certificado** é exibida.

4. Clique na guia **Detalhes** e depois clique em **Copiar para**, como mostra a imagem a seguir:



O **Assistente de Exportação de Certificado** é exibido.

5. Selecione **Binário codificado em DER X.509 (.CER)** como o formato, como mostra a imagem a seguir:



6. Clique em **Avançar**.
7. Insira o nome do arquivo de certificado e a localização para exportá-lo para e clique em **Avançar**.
8. Clique em **OK** e, em seguida, em **Concluir** para concluir a exportação.

Etapa 3. Importar o certificado para o truststore do Truststore

Importe o certificado de Assinatura de Declaração para o arquivo de truststore Informatica padrão em cada nó do gateway no domínio Informatica.

Use o utilitário de gerenciamento de chaves e certificados Java keytool para importar o certificado para o arquivo de truststore Informatica. O arquivo de truststore padrão, `infa_truststore.jks`, é instalado no seguinte diretório em cada nó:

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

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:

```
<diretório de instalação Informatica>\java\jre\bin
```
3. Na linha de comando, execute o seguinte comando:


```
keytool -importcert -alias <nome do arquivo de certificado> -file <caminho do
certificado>\<nome do arquivo de certificado> -keystore <diretório de instalação
Informatica>\services\shared\security\infa_truststore.jks -storepass <senha>
```

Observe que você deve incluir a senha para o truststore padrão Informatica.

4. Reinicie o nó.

Etapa 4. Configurar o Active Directory Federation Services

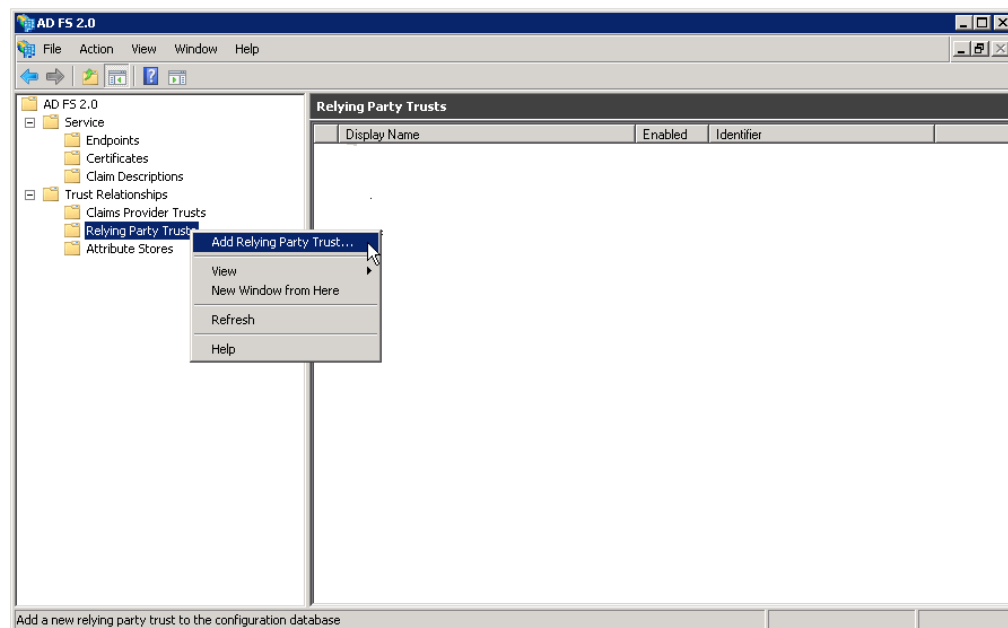
Configure o AD FS para emitir tokens SAML para aplicativos da Web Informatica.

Use o AD FS Management Console para realizar as seguintes tarefas:

- Adicione o Informatica como uma confiança de parte dependente no AD FS. A definição de confiança de parte dependente permite que o AD FS aceite solicitações de autenticação de aplicativos da Web Informatica.
- 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 AD FS.

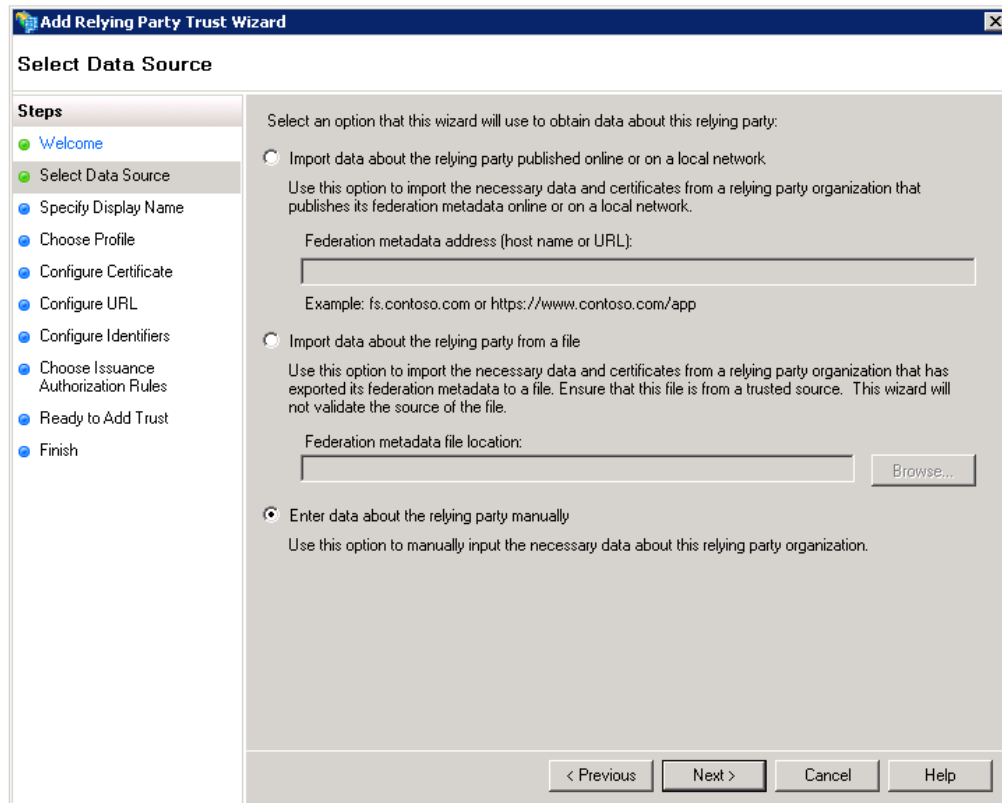
Nota: Todas as cadeias fazem distinção entre maiúsculas e minúsculas no AD FS, incluindo URLs.

1. Faça login no Console de Gerenciamento do AD FS.
2. Expanda a pasta **Relacionamentos de Confiança > Confianças de Parte Dependente**.
3. Clique com o botão direito do mouse na pasta **Confianças de Parte Dependente** e selecione **Adicionar Confiança de Parte Dependente**, como mostra a imagem a seguir:

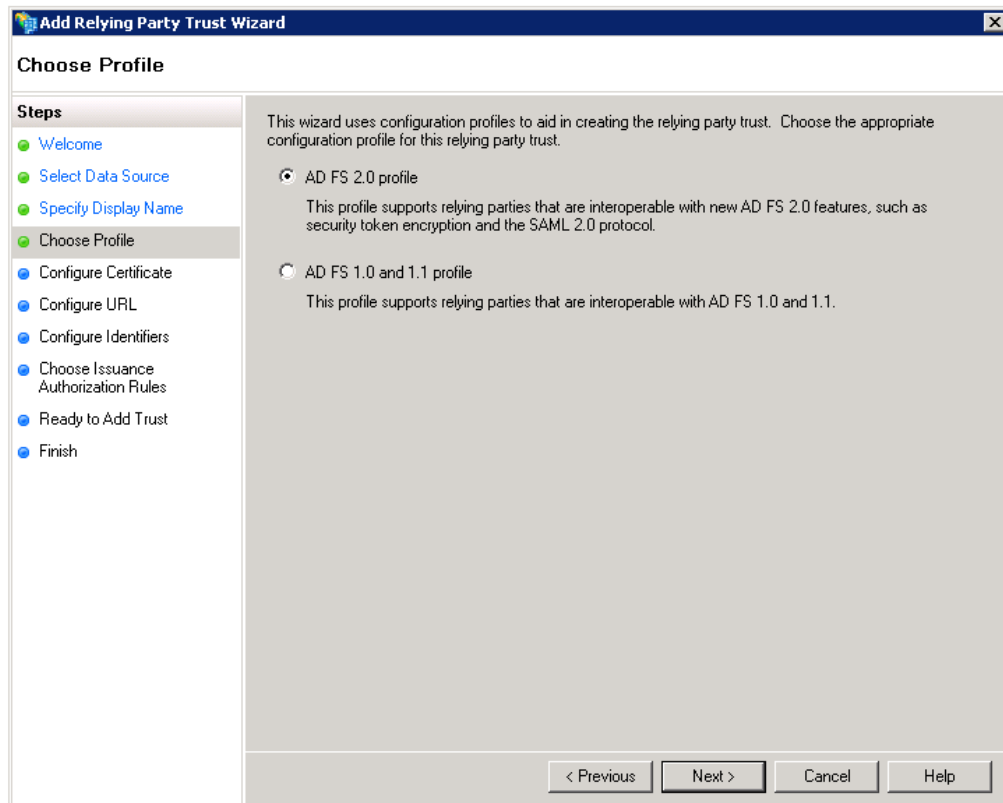


O **Assistente para Adicionar Confiança de Parte Confiável** é exibido.

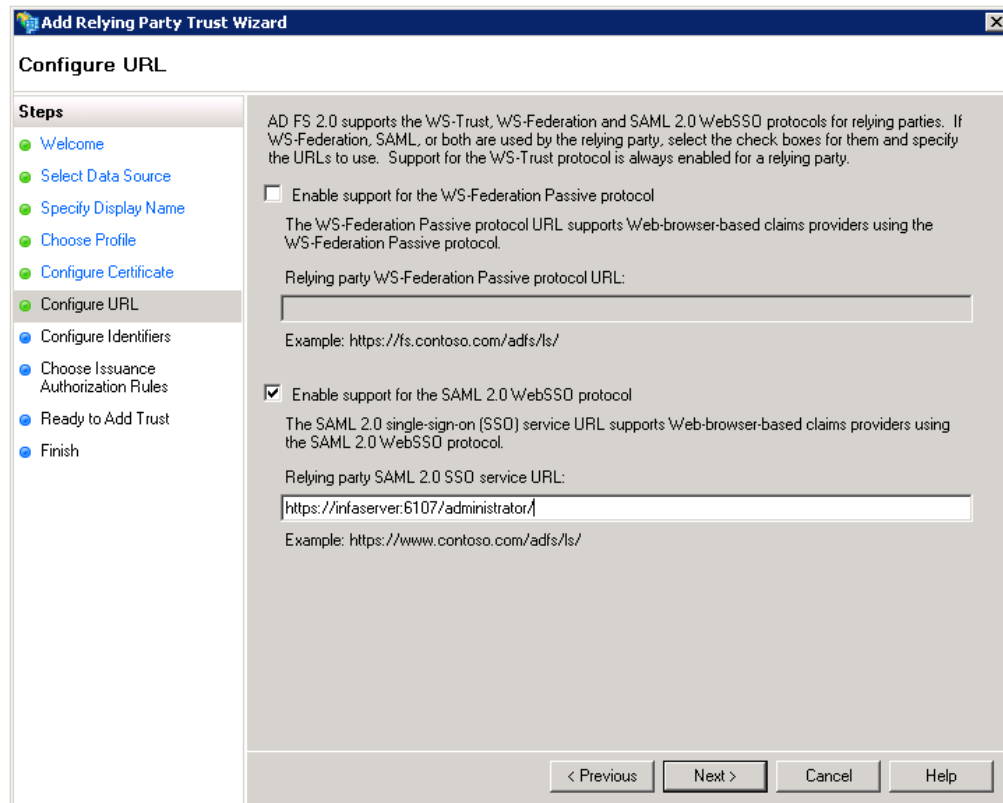
4. Clique em **Iniciar**.
O painel **Selecionar Fonte de Dados** é exibido.
5. Clique em **Inserir dados sobre a parte dependente manualmente**, como mostra a seguinte imagem:



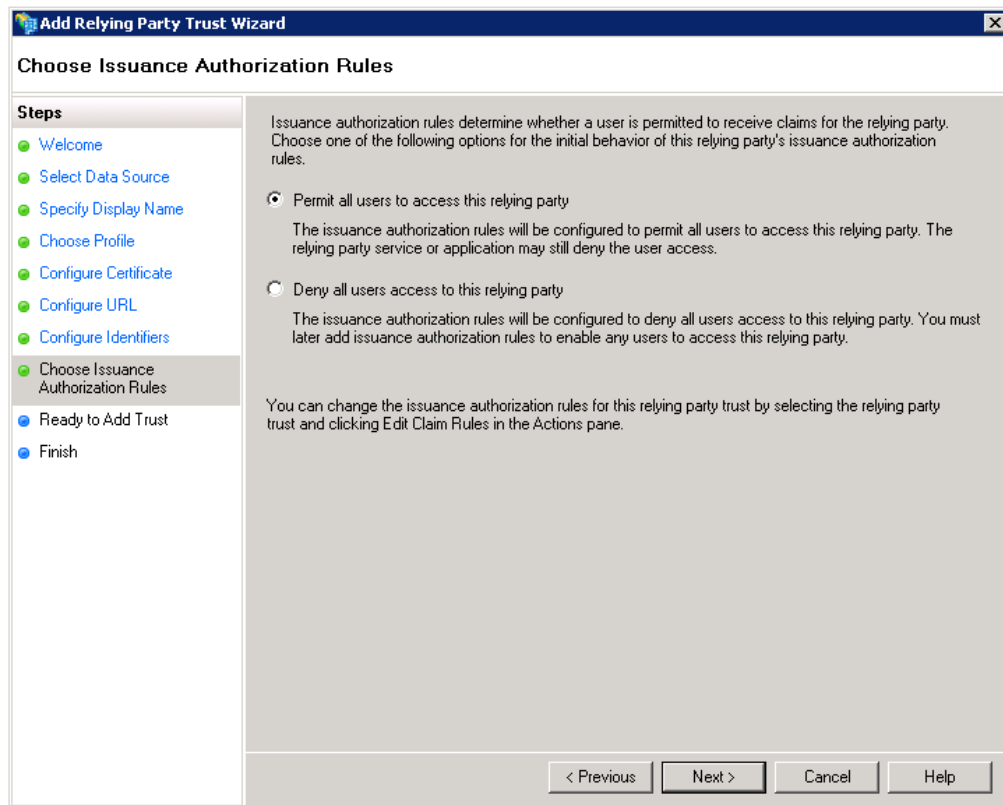
6. Clique em **Avançar**
7. Insira "Informatica" como o nome para exibição e clique em **Avançar**.
8. Clique em **AD FS 2.0 profile** conforme mostrado na imagem a seguir:



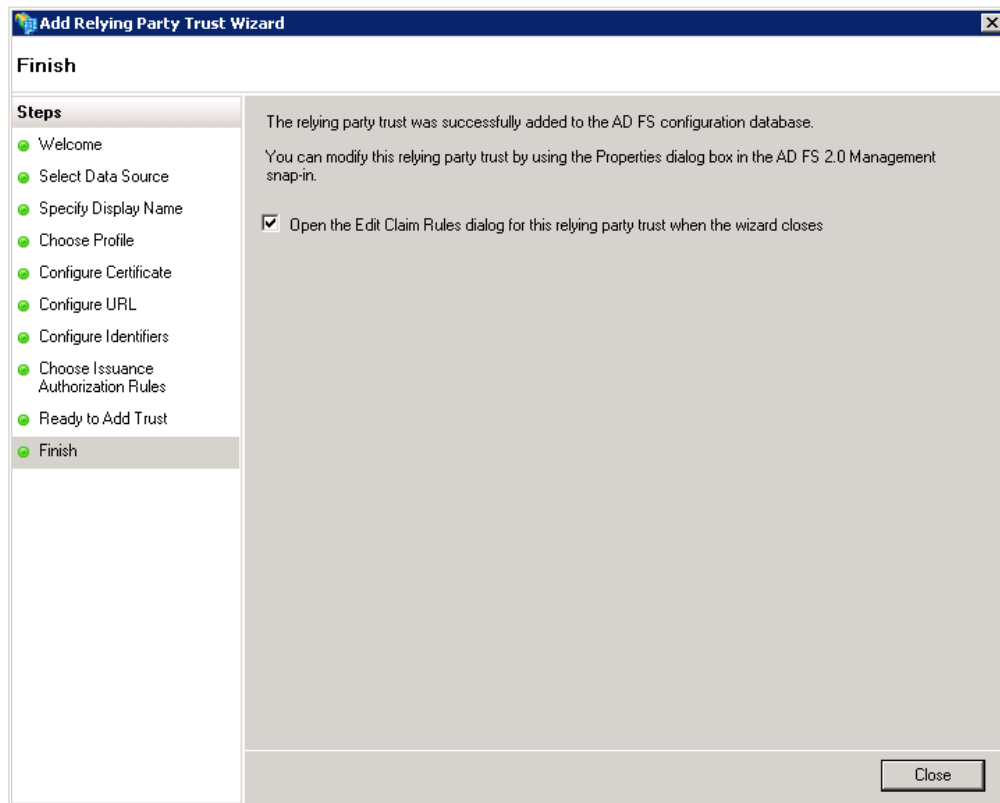
9. Clique em **Avançar**.
Ignore o painel de configuração do certificado no assistente.
10. Marque **Ativar suporte para protocolo SAML WebSSO** e, em seguida, insira a URL completa para a ferramenta Administrator, conforme mostrado na imagem a seguir:



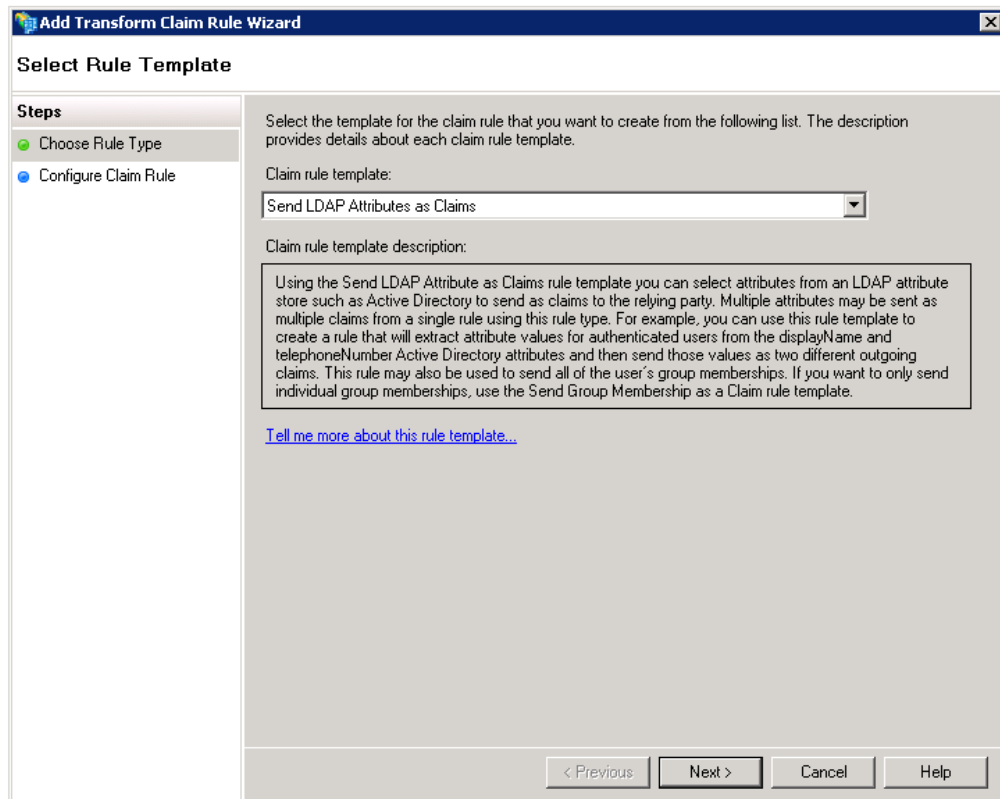
11. Clique em **Avançar**.
12. Insira "Informatica" no Identificador de confiança de parte dependente. Clique em **Adicionar** e depois em **Avançar**.
13. Selecione **Permitir que todos os usuários acessem a parte dependente**, como mostra a seguinte imagem:



14. Clique em **Avançar**.
15. Marque **Abrir a caixa de diálogo Editar Regras de Reivindicação para esta parte dependente quando o assistente for fechado**, como mostra a imagem a seguir:



16. Clique em **Fechar**.
A caixa de diálogo **Editar Regras de Reivindicação para o Informatica** é exibida.
17. Clique em **Adicionar Regra**.
O **Assistente para adicionar regra de reivindicação de transformação** é aberto.
18. Selecione **Enviar Atributos LDAP como Reivindicações** no menu, como mostra a imagem a seguir:



19. Clique em **Avançar**.
20. Insira qualquer cadeia como o nome da regra de reivindicação, como mostra a imagem abaixo:

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute	Outgoing Claim Type
SAM-Account-Name	username
*	

< Previous Finish Cancel Help

21. Selecione Active Directory no menu **Repositório de atributos**.
22. Selecione Nome da conta SAM no menu **Mapeamento LDAP**.
23. Insira "nome de usuário" no campo **Tipo de Reivindicação de Saída**.
24. Clique em **Concluir** e depois em **OK** para fechar o assistente.

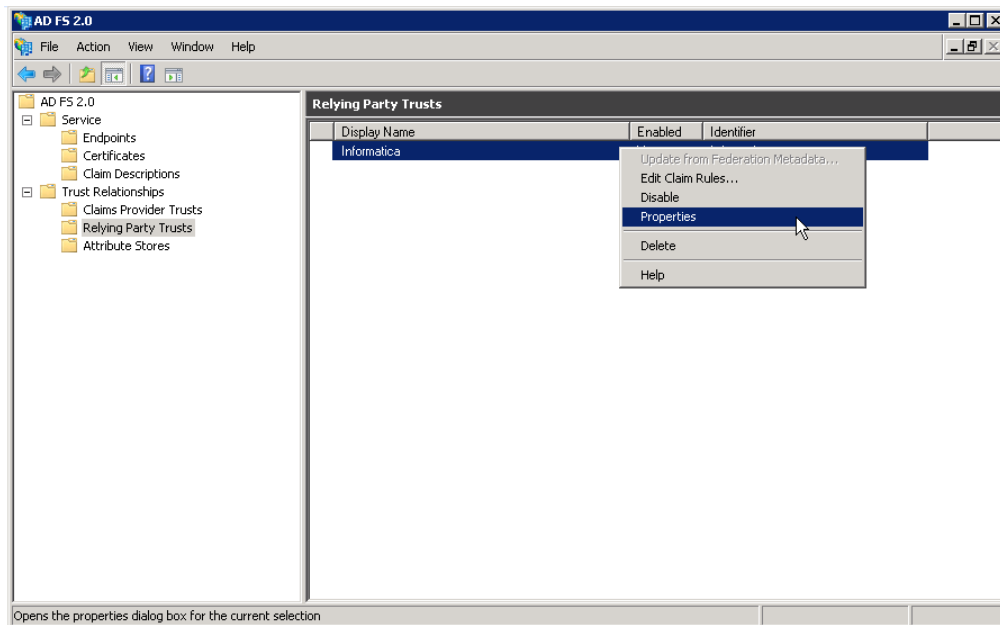
Etapa 5. Adicionar URLs de aplicativos da Web Informatca ao AD FS

Adicione a URL para cada aplicativo da Web Informatca usando o logon único com o AD FS.

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

Você não precisa adicionar a URL da ferramenta Administrator, desde que já a tenha inserido como parte da configuração do AD FS.

1. Faça logon no Console de Gerenciamento do AD FS.
2. Expanda a pasta **Relacionamentos de Confiança > Confianças de Parte Dependente**.
3. Clique com o botão direito do mouse na entrada **Informatca** e selecione **Propriedades**, como mostra a imagem abaixo:

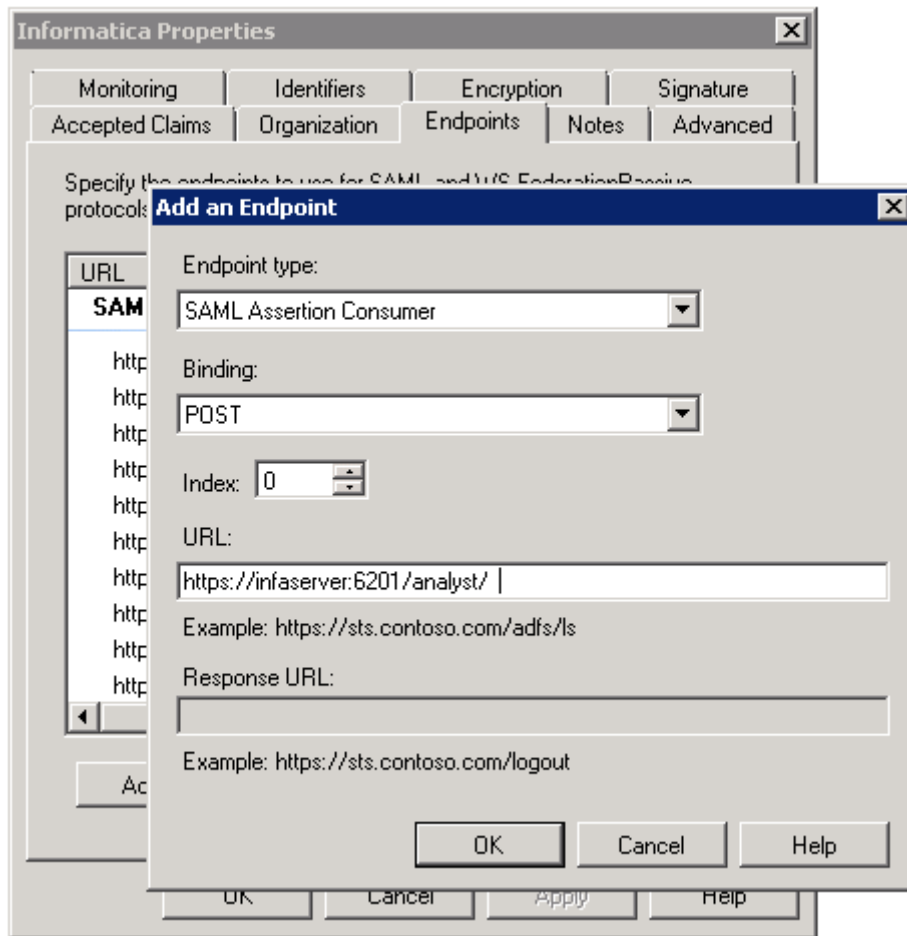


A caixa de diálogo **Propriedades do Informatica** é exibida.

4. Clique na guia **Ponto de Extremidade**.

A caixa de diálogo **Adicionar um Ponto de Extremidade** é exibida.

5. Selecione **Consumidor de Assertivas SAML** no menu de tipo **Ponto de Extremidade** e depois selecione **POST** no menu **Associação**, como mostra a imagem abaixo:



6. Insira a URL completa para um aplicativo da Web Informatica com suporte e, em seguida, clique em **OK**. Repita este procedimento para cada aplicativo da Web.

Etapa 6. Ativar logon único com base em SAML

Você pode ativar o logon único com base em SAML em um domínio Informatica existente ou pode ativá-lo ao instalar ou criar um domínio.

Selecione uma das seguintes opções:

Ative o logon único ao instalar serviços Informatica.

Você pode ativar o logon único com base em SAML e especificar a URL do provedor de identidade ao configurar o domínio como parte do processo de instalação.

Ative o logon único em um domínio existente.

Use o comando `infasetup updateSamlConfig` para ativar o logon único em um domínio Informatica existente. É possível executar o comando em qualquer nó de gateway no domínio.

Desligue o domínio antes de executar o comando.

Especifique a URL do provedor de identidade como o valor para a opção `-iu`. O exemplo a seguir mostra o uso do comando:

```
infasetup updateSamlConfig -saml true -iu https://server.company.com/adfs/ls/
```

Ative o logon único ao criar um domínio.

Use o comando `infasetup defineDomain` para ativar o logon único quando você criar um domínio.

O exemplo a seguir mostra as opções SAML como as duas opções finais na linha de comando:

```
infasetup defineDomain -dn TestDomain -nn TestNode1 -na host1.company.com -cs
"jdbc:informatica:oracle://host:1521;sid=xxxx" -du test_user -dp test_user -dt oracle -rf
$HOME/ISP/BIN/nodeoptions.xml -ld $HOME/ISP/1011/source/logs -mi 10000 -ma 10200 -ad
test_admin -pd test_admin -saml true -iu https://server.company.com/adfs/ls/
```

Opções de comandos `infasetup`

Defina as opções SAML no comando `infasetup updateSamlConfig` para ativar o logon único em um domínio ou no comando `infasetup defineDomain` quando você criar um domínio.

A tabela a seguir descreve as opções e os valores:

Opção	Argumento	Descrição
-EnableSaml -saml	verdadeiro falso	Obrigatório. Defina esse valor como <code>true</code> para ativar o logon único com base em SAML para aplicativos da Web Informatica com suporte no domínio Informatica. Defina esse valor como <code>false</code> para desativar a SSO com base em SAML para aplicativos da Web Informatica com suporte no domínio Informatica.
-IdpUrl -iu	identity_provider_url	Necessário se a opção <code>-saml</code> for <code>true</code> . Especifique a URL do provedor de identidade para o domínio. Você deve especificar a cadeia de URL completa.

Consulte a *Referência de Comandos da Informatica* para obter instruções sobre como usar os comandos `infasetup updateSamlConfig` e `infasetup defineDomain`.

Obtendo a URL do Provedor de Identidade

Você deve fornecer a URL SAML 2.0/WS-Federation do servidor AD FS para habilitar o logon único.

Você define essa URL como o valor para a opção `-iu` quando você executa o comando `infasetup updateSamlConfig` ou `infasetup defineDomain`. Use o Windows PowerShell no servidor AD FS para obter a URL.

1. Abra a janela de prompt de comando do Windows PowerShell no servidor AD FS. Selecione a opção Executar como administrador ao abrir o prompt de comando.
2. Digite o seguinte comando no prompt de comando do Windows PowerShell:

```
Get-ADFSEndpoint
```

3. Encontre o valor de FullUrl retornado para o protocolo SAML 2.0/WS-Federation, conforme mostrado na imagem abaixo:

```
ClientCredentialType : Anonymous
Enabled              : True
FullUrl              : https://adfs.company.com/adfs/ls/
Proxy                : False
Protocol             : SAML 2.0/WS-Federation
SecurityMode         : Transport
AddressPath          : /adfs/ls/
Version              : default
```

CAPÍTULO 7

Gerenciamento de Segurança no Informatica Administrator

Este capítulo inclui os seguintes tópicos:

- [Usando a visão geral do Informatica Administrator, 101](#)
- [Segurança do Usuário, 102](#)
- [Guia Segurança, 105](#)
- [Gerenciamento de Senha, 108](#)
- [Gerenciamento de segurança do domínio, 108](#)
- [Gerenciamento de segurança do usuário, 109](#)

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 do domínio. Gerencie logs, objetos de domínio e permissões de usuário. Monitore tarefas e aplicativos do Serviço de Integração de Dados.
- Tarefas administrativas do domínio. Gerencie logs, objetos de domínio e permissões de usuário.
- Tarefas administrativas de segurança. Gerencie usuários, grupos, funções e privilégios.

Nota: Se você tem o PowerCenter Express Personal Edition, não tem acesso aos recursos de segurança.

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.
- **Monitorar.** Exiba o status de trabalhos de perfil, trabalhos de visualização, trabalhos de mapeamento e fluxos de trabalho para o Serviço de Integração de Dados.
- **Monitorar.** Exiba e monitore as implantações do Ultra Messaging.
- **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.
- **Segurança.** Gerencie usuários, grupos, funções e privilégios. Se você tiver o PowerCenter Express Personal Edition, não terá acesso à guia Segurança.
- **Nuvm.** 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.
- **Ajuda.** Acesse a ajuda da guia atual, determine a versão do Informatica e configure a diretiva de uso de dados.

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 alguns serviços de aplicativo controlam a segurança do usuário em aplicativos clientes. Os aplicativos clientes incluem o Informatica Administrator e o Informatica Developer. O Gerenciador de Serviços e alguns serviços de aplicativo controlam a segurança do usuário em aplicativos clientes. O cliente do aplicativo inclui o Informatica Administrator.

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 do Metadata Manager
- Serviço Web Service Hub

Também é possível usar HTTPS para conexão segura com o domínio e os serviços de aplicativo. Os seguintes serviços de aplicativo oferecem suporte para conexão HTTPS junto com o domínio Informatica:

- Serviço de Integração de Dados
- Serviço Analyst

Também é possível usar HTTPS para conexão segura com o domínio e os serviços de aplicativo.

Criptografia

A Informatica criptografa senhas enviadas dos clientes do aplicativo para o Service Manager. A Informatica usa a criptografia AES com várias chaves de 128 bits para criptografar senhas e armazena as senhas criptografadas no banco de dados de configuração do domínio. Configure HTTPS para criptografar as senhas enviadas ao Service Manager de clientes de aplicativo.

Autenticação

O Service Manager autentica os usuários que fazem login nos clientes de aplicativo.

Na primeira vez que você fizer login 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 login 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 login 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.

Quando você faz login 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.

Quando você faz login 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.

Sign-On único

Depois de efetuar login em um aplicativo cliente, o Gerenciador de Serviços permitirá ativar outro aplicativo cliente ou acessar vários repositórios no aplicativo cliente. Não é necessário efetuar login 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

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 de Repositório do Modelo

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.

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 de Repositório do Modelo.

- Você adicionar ou remover usuários ou grupos nativos.

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 os perfis de sistema operacional e LDAP. Também é possível exibir usuários que tenham privilégios para um serviço.

Nota: Se tiver o PowerCenter Express Edição Pessoal, você não terá acesso à guia Segurança

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.

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 incluir um menu Ações para gerenciar grupos, usuários ou funções. Selecione um objeto no Navegador e clique no menu Ações para criar, excluir ou mover grupos, usuários ou funções.
- 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 de criação, exclusão e movimentação 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.

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 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.

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. Clique com o botão direito do mouse em um grupo e selecione Navegar até o Item para exibir detalhes do grupo no painel de conteúdo.

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.

Usuários

Um usuário com uma conta no domínio Informatica pode efetuar logon nos aplicativos clientes a seguir.

- Informatica Administrator
- Cliente do PowerCenter
- Metadata Manager
- Informatica Developer

- Informatica Analyst

Um usuário com uma conta no domínio Informatica pode efetuar login nos aplicativos clientes a seguir.

- Informatica Administrator
- Informatica Developer

Um usuário com uma conta no domínio Informatica pode fazer login no Informatica Administrator.

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.

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 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.

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. Clique com o botão direito do mouse em um usuário e selecione Navegar até o item para exibir os detalhes do usuário no painel de conteúdo.

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.

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. Clique com o botão direito do mouse em uma função e selecione Navegar até o item para exibir os detalhes da função no painel de conteúdo.

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.

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.

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 logon na ferramenta Administrator.

1. Na área de cabeçalho da ferramenta Administrator, 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.

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. Objetos de domínio incluem o domínio, o nó a licença, conexões de banco de dados e 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.

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.

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.

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.

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](#), 110
- [Grupos Padrão](#), 111
- [Entendendo as contas de usuário](#), 112
- [Gerenciando usuários](#), 114
- [Gerenciando grupos](#), 122
- [Gerenciando perfis do sistema operacional](#), 124
- [Bloqueio de conta](#), 132

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. As tarefas que você pode executar dependem do tipo de conta de usuário e do tipo de licença do PowerCenter Express que você tem.

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.

Nota: Se instalar o PowerCenter Express Edição Pessoal, você deverá usar a conta de administrador padrão para todas as operações. Não é possível criar usuários ou grupos e gerenciar permissões.

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.
- **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.

- Autenticação. Quando um usuário efetua login 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.
- 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 login 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.
- Bloqueio de conta. Você pode configurar o bloqueio de conta para bloquear uma conta de usuário quando o usuário especifica um login incorreto na ferramenta Administrador ou na Developer tool. Você também pode desbloquear uma conta de usuário.
- Bloqueio de conta. Você pode configurar o bloqueio de conta para bloquear uma conta de usuário quando o usuário especifica um login incorreto na ferramenta Administrador. 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

Um domínio Informatica pode ter os seguintes tipos de contas:

- Administrador padrão
- Administrador de domínio
- Administrador de cliente de aplicativo
- Usuário

O domínio Informatica tem uma conta de administrador padrão.

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 login 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 login em qualquer cliente do aplicativo.

O administrador padrão é uma conta de usuário no domínio de segurança nativo. Não é possível criar um administrador padrão. 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 login na ferramenta Administrador e criar e configurar serviços de aplicativo no domínio. No entanto, por padrão, o administrador de domínio não pode efetuar login 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.

O administrador de domínio pode efetuar login na ferramenta Administrador e configurar serviços de aplicativo no domínio. No entanto, por padrão, o administrador de domínio não pode efetuar login 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 logon 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 logon 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 logon 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 criar, editar e excluir usuários, dependendo do tipo de licença do PowerCenter Express. Você pode atribuir funções, permissões e privilégios a uma conta de usuário. As funções, permissões e privilégios atribuídos ao usuário determinam as tarefas que o usuário pode executar no domínio Informatica. Se tiver o PowerCenter Express Edição Pessoal, você não poderá criar usuários ou grupos. Você deve usar o usuário Administrador padrão para executar todas as tarefas.

Você pode criar, editar e excluir usuários, dependendo do tipo de licença. Você pode atribuir funções, permissões e privilégios a uma conta de usuário. As funções, permissões e privilégios atribuídos ao usuário determinam as tarefas que o usuário pode executar no domínio Informatica.

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 NativosCriando UsuáriosCriando Usuários

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.
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 Administrador, 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 usuários LDAP a um grupo, selecione um usuário LDAP na coluna Todos os Usuários e clique em Adicionar.
5. Para remover usuários LDAP de um grupo, selecione um usuário LDAP 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 login 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 login nos clientes do aplicativo.

Os usuários com contas ativas podem fazer login 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. Quando você desativa uma conta de usuário, o usuário não pode fazer login 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 Administrador 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 Administrador.

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 login na ferramenta Administrador, 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 oie 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 o comando `infacmd isp getUserActivityLog` ou a guia Logs da ferramenta Administrator para exibir os logs de atividade do usuário. Exiba os eventos de log de atividade do usuário para determinar quando um usuário criou, atualizou ou removeu serviços, nós, grupos de usuários ou funções.

Execute o seguinte comando para exibir os eventos de log de atividade do usuário para todos os usuários:

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

O comando requer a função Administrator ou a associação no grupo Administrator.

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

Você pode exibir os eventos de log na linha de comando ou gravá-los em um arquivo com os 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.

Para obter mais informações sobre os logs de atividade do usuário e a guia Logs da ferramenta Administrator, consulte o *Guia do Informatica Administrator*.

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.

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.

Você pode atribuir funções, permissões e privilégios a um grupo. As funções, as permissões e os privilégios atribuídos ao grupo determinam as tarefas que os usuários no grupo podem executar no domínio Informatica.

Você pode atribuir funções, permissões e privilégios a um grupo. 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.

Um grupo nativo pode conter contas de usuário 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.

Um grupo nativo pode conter contas de usuário 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.

Gerenciando perfis do sistema operacional

Crie e gerencie perfis do sistema operacional na guia Segurança da ferramenta Administrator ou a partir da linha de comando. Você pode criar, editar e excluir perfis do sistema operacional. Também pode atribuir ou alterar o perfil do sistema operacional padrão para usuários e grupos.

Se o Serviço de Integração de Dados estiver configurado para usar perfis do sistema operacional, ele executará mapeamentos, perfis e fluxos de trabalho com o perfil do sistema operacional. Se o Serviço de Integração do PowerCenter estiver configurado para usar perfis do sistema operacional, ele executará fluxos de trabalho com o perfil do sistema operacional.

Crie, edite e exclua perfis do sistema operacional na exibição **Perfis do Sistema Operacional** da guia **Segurança**.

Conclua as seguintes etapas para criar um perfil do sistema operacional:

1. Insira um nome de perfil do sistema operacional e um nome de usuário do sistema.
2. Selecione os Serviços de Integração e configure as propriedades do perfil do sistema operacional.

3. Opcionalmente, atribua permissões no perfil do sistema operacional.

Você pode atribuir usuários e grupos a perfis do sistema operacional e atribuir um perfil padrão a usuários e grupos depois de criar um perfil do sistema operacional.

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.

Propriedade	Descrição
\$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.
\$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 nem 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.

Propriedade	Descrição
\$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.
\$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.
\$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 Usar o Usuário Especificado como Usuário de Representação do Hadoop e insira um nome de usuário.

Propriedade	Descrição
Variáveis de Ambiente	<p>Nome e valor das variáveis de ambiente usadas pelo Serviço de Integração em tempo de execução.</p> <p>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.</p> <p>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.</p> <p>Nota: 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.</p>
Diretório de cache de arquivo simples	<p>Diretório de cache de arquivo simples no qual a ferramenta Analyst armazena os arquivos simples carregados.</p> <p>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.</p>

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.

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 diferencia maiúsculas de 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. Nota: 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 um ou ambos os Serviços de Integração que usarão o perfil do sistema operacional.

- Serviço de Integração do PowerCenter
- Serviço de Integração de Dados

6. Configure as propriedades do perfil do sistema operacional para os Serviços de Integração.

7. Se o Serviço de Integração de Dados executar mapeamentos, perfis e fluxos de trabalho em um ambiente Hadoop, configure as propriedades de representação do Hadoop da seguinte maneira:

- Selecione **Ativar Propriedades de Representação do Hadoop**.
- 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:

- Para atribuir grupos específicos ao perfil do sistema operacional, selecione um ou mais grupos e clique em **Adicionar**.
- 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:

- Para atribuir usuários específicos ao perfil do sistema operacional, selecione um ou mais usuários e clique em **Adicionar**.
- 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 **Serviço de Integração de Dados** ou o **Serviço de Integração do PowerCenter** que você deseja configurar.
6. Editar as propriedades do Serviço de Integração.
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.

Trabalhando com Perfis do Sistema Operacional em um Domínio Seguro

Você pode usar perfis do sistema operacional em um domínio Informatica que tem a comunicação segura habilitada.

Considere as seguintes regras e diretrizes quando você usar perfis do sistema operacional em um domínio que tenha a comunicação segura habilitada:

- Você deve definir a seguinte variável de ambiente para o perfil do sistema operacional:

INFA_TRUSTSTORE

Defina o valor como o diretório que contém os arquivos de truststore dos certificados SSL do domínio seguro. O diretório deve conter um arquivo de truststore denominado infa_truststore.pem.

INFA_TRUSTSTORE_PASSWORD

Se você usar um truststore personalizado, defina o valor como a senha do infa_truststore.pem que contém o certificado SSL para o domínio seguro. A senha deve ser criptografada. Use o programa de linha de comando pmpasswd para criptografar a senha.

- Além disso, se o Serviço de Integração do PowerCenter usar a opção Sessão na Grade, você deverá definir a seguinte variável de ambiente do perfil do sistema operacional:

INFA_KEYSTORE

Defina o valor como o diretório que contém os arquivos de armazenamento de chaves dos certificados SSL do domínio seguro. O diretório deve conter um arquivo de armazenamento de chaves denominado infa_keystore.pem.

Você pode definir as variáveis de ambiente do perfil do sistema operacional na ferramenta Administrator. Para definir as variáveis de ambiente do perfil do sistema operacional, clique em **Segurança > Perfis de Sistema Operacional**. Edite as propriedades do perfil do sistema operacional e defina as variáveis de ambiente.

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.

Você pode definir as variáveis de ambiente do perfil do sistema operacional na ferramenta Administrator. Para definir as variáveis de ambiente do perfil do sistema operacional, clique em **Segurança > Perfis de Sistema Operacional**. Edite as propriedades do perfil do sistema operacional e defina as variáveis de ambiente.

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 Ativar Bloqueio de Conta de Administrador 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 Ativar Bloqueio de Conta 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:

- [Visão geral de privilégios e funções, 134](#)
- [Privilégios do domínio, 136](#)
- [Privilégios do Serviço Analyst, 145](#)
- [Privilégios do Serviço do Gerenciamento de Conteúdo, 146](#)
- [Privilégios do Data Integration Service, 147](#)
- [Privilégios do Serviço do Metadata Manager, 147](#)
- [Privilégios do Serviço de Repositório do Modelo, 151](#)
- [Privilégios do Serviço de Repositório do PowerCenter, 152](#)
- [Privilégios do Serviço do Ouvinte do PowerExchange, 167](#)
- [Privilégios do Serviço do Agente de Log do PowerExchange, 167](#)
- [Privilégios do Serviço de Agendador, 168](#)
- [Privilégios do Serviço do Test Data Manager, 169](#)
- [Gerenciando Funções, 177](#)
- [Atribuindo privilégios e funções aos usuários e grupos, 181](#)
- [Exibindo usuários com privilégios para um serviço, 183](#)
- [Solucionando problemas de privilégios e funções, 183](#)

Visão geral de privilégios e funções

Você gerencia a segurança do usuário com privilégios e funções.

Você pode modificar privilégios e funções, dependendo do tipo de licença do PowerCenter Express.

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.
- Privilégios de domínio. Determinar ações no domínio Informatica que os usuários podem executar usando a ferramenta Administrator.

- 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 Integração de Dados. Determinar ações que os usuários podem executar nos aplicativos usando a ferramenta Administrator. Este privilégio também determina se os usuários podem fazer uma busca detalhada e exportar os resultados do perfil.
- 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.
- Privilégio do Serviço de Repositório do Modelo. Determinar ações em projetos que os usuários podem executar usando o 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.

Os privilégios determinam as ações que os usuários podem executar nos aplicativos clientes. A Informatica inclui os privilégios do domínio, que determinam as ações que os usuários podem executar usando a ferramenta Administrator .

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 do domínio. Inclui privilégios para gerenciar o domínio, pastas, nós, grades, licenças e serviços de aplicativo.

- Administração do domínio. Inclui privilégios para gerenciar o domínio, pastas e serviços de aplicativo.
- Administração de Segurança. Inclui privilégios para gerenciar usuários, grupos, funções e privilégios.
- Administração do Domínio. Inclui privilégios para gerenciar o domínio, pastas, nós, grades, licenças e serviços de aplicativo.
- Ferramentas. Inclui privilégios para fazer logon na ferramenta Administrator.
- Monitoramento. Inclui privilégios para monitorar implantações do Ultra Messaging e exibir as estatísticas.

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 "Como fazer" sobre bibliotecas da Informatica:

<https://kb.informatica.com/h2l/HowTo%20Library/1/0236-GroupsAndRolesToManageAccessControl.pdf>.

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.

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.

Os privilégios do domínio determinam as ações que usuários podem executar usando a ferramenta Administrator.

A tabela a seguir descreve cada grupo de privilégio 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, as pastas, os nós, as grades, as licenças, os serviços de aplicativo e as conexões.
Monitoramento	Incluir 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 Privilégios	Descrição
Administração de Segurança	Inclui privilégios para gerenciar usuários, grupos, funções e privilégios.
Administração de Domínio	Inclui privilégios para gerenciar o domínio, os serviços de aplicativo e as conexões.
Monitoramento	Incluir 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.

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, os serviços de aplicativo e as conexões.
Monitoramento	Inclui privilégios para monitorar implantações do UM e exibir as estatísticas.
Ferramentas	Inclui privilégios para fazer logon na ferramenta Administrator.

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.

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">- Atribuir privilégios e funções para usuários e grupos do domínio ou serviço de aplicativo.- Editar e remover as funções e os privilégios atribuídos a usuários e grupos.

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">- Configurar a autenticação LDAP para o domínio.- Criar, editar e excluir usuários, grupos e funções.- Importar usuários e grupos LDAP.
Perfil do sistema operacional	O usuário é capaz de editar propriedades de perfil do sistema operacional.

Grupo de privilégio 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.
- 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"> - Exibir propriedades do domínio e eventos de log. - Configurar as definições de monitoramento.
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"> - 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. - Receber alertas de serviços de aplicativo.

Permissão Ativada	Descrição
Serviço de aplicativo	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none"> - Ativar e desativar serviços de aplicativo e processos de serviço. - Receber alertas de serviços de aplicativo.

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"> - Configurar serviços de aplicativo. - Conceder permissão para serviços de aplicativo.
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"> - Fazer backup do conteúdo de repositório do Metadata Manager. - Excluir o conteúdo de repositório do Metadata Manager. - Fazer upgrade do conteúdo do Serviço do Metadata Manager. <p>Nota: 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"> - Criar e excluir conteúdo do repositório do Modelo. - Criar, excluir e reindexar o índice de pesquisa. - Atualizar o conteúdo do Serviço de Repositório do Modelo do menu Ações 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.
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"> - Fazer backup, restauração e upgrade do repositório do PowerCenter. - Configurar linhagem de dados para o repositório do PowerCenter. - Copiar conteúdo de outro repositório do PowerCenter. - Fechar conexões do usuário e liberar bloqueios do repositório do PowerCenter. - Criar e excluir conteúdo do repositório do PowerCenter. - Criar, editar e excluir extensões reutilizáveis de metadados no Gerente de repositório do PowerCenter. - Ativar controle de versão para o repositório do PowerCenter. - Gerenciar um domínio de repositório do PowerCenter. - Executar uma limpeza avançada das versões de objeto no nível de repositório do PowerCenter Repository Manager. - Registrar e cancelar o registro de plug-ins do repositório do PowerCenter. - Executar o repositório do PowerCenter em modo exclusivo. - Enviar notificações de repositório do PowerCenter aos usuários. - Atualizar estatísticas do repositório do PowerCenter. - Atualizar o conteúdo do Serviço do Repositório do PowerCenter.
Serviço do Test Data Manager	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"> - Criar e excluir o conteúdo do repositório do Test Data Manager. - Atualizar o conteúdo do Serviço do Test Data Manager.
Objeto de licença	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"> - Editar objetos de licença. - Conceder permissão para objetos de licença.
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.

Permissão Ativada	Descrição
O domínio onde é executado o serviço de aplicativo e qualquer serviço de aplicativo associado	O usuário pode criar serviços de aplicativo.
Serviço de aplicativo	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"> - Configurar serviços de aplicativo. - Conceder permissão para serviços de aplicativo.
Serviço de Repositório do Modelo	<p>O usuário pode realizar as seguintes ações:</p> <ul style="list-style-type: none"> - Criar e excluir conteúdo do repositório do Modelo. - Criar, excluir e reindexar o índice de pesquisa.

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	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none">- Configurar e encerrar nós e grades.- Conceder permissão para nós e grades.
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">- Editar pastas.- Conceder permissão para pastas.
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 podem criar, editar e excluir conexões na ferramenta Administrator, na ferramenta Desenvolvedor e no 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.

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.
- Visualizar dados ou executar um mapeamento 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.
Gravar na conexão	O usuário é capaz de copiar, editar e excluir conexões.
Conceder conexão	O usuário é capaz de conceder e revogar permissões nas conexões.

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.
Exibir	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.
Exibir	Exibir Estatísticas	Domínio	O usuário pode visualizar a exibição Estatísticas de Resumo e as estatísticas de objetos de domínio. Nota: 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.

Privilégio pai	Privilégio	Permissão Ativada	Descrição
Exibir	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: <ul style="list-style-type: none"> - 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"> - Efetue login na ferramenta Administrator. - Gerencie a conta do usuário na ferramenta Administrator. - Exporte eventos de log.

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. Nota: A seleção desse privilégio também concede o privilégio Acessar Especificações de Mapeamento 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.

Privilégio	Permissão	Descrição
Acesso a Espaços de Trabalho	-	O usuário pode acessar os seguintes espaços de trabalho na ferramenta Analyst: - Design - Descoberta - Glossário - Scorecards Nota: A seleção desse privilégio também concede acesso aos projetos na ferramenta Analyst. Caso o usuário não tenha esse privilégio, ele deverá ter o privilégio Espaço de Trabalho de Design , Espaço de Trabalho de Descoberta , Espaço de Trabalho de Glossário ou Espaço de Trabalho de Scorecards para acessar projetos.
Espaço de Trabalho Design	-	O usuário pode acessar o espaço de trabalho Design .
Espaço de Trabalho Descoberta	-	O usuário pode acessar o espaço de trabalho Descoberta .
Espaço de Trabalho Glossário	-	O usuário pode acessar o espaço de trabalho Glossário .
Espaço de Trabalho Scorecards	-	O usuário pode acessar o espaço de trabalho Scorecards .

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"> - Crie uma tabela de referência nas ferramentas Analyst e Developer. - Crie uma tabela de referência usando <code>infacmd rtm import</code>. - Importe um objeto de tabela de referência para o repositório do Modelo. - Copie uma tabela de referência nas ferramentas Analyst e Developer. - Crie uma tabela de referência a partir de dados do perfil. Nota: 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"> - Edite os valores dos dados de tabela de referência nas ferramentas Developer e Analyst. - Adicione um perfil de dados a uma tabela de referência. - Adicione ou exclua colunas em uma tabela de referência. Altere os metadados da tabela de referência, como nomes de coluna, descrições e valores padrão.

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.

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 a ferramenta 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	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none">- Faça backup e restaure um aplicativo para um arquivo.- Implantar um aplicativo em um Data Integration Service e resolver conflitos de nomes.- Iniciar um aplicativo depois da implantação.- Localizar um aplicativo.- Inicie ou interrompa objetos em um aplicativo.- Configurar propriedades do aplicativo.

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">- Faça uma busca detalhada nos resultados da criação de perfil.- Exportar os resultados de criação de perfil.

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.

Grupo de Privilégio	Descrição
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"> - Execute análise da linhagem de dados em objetos dos metadados, categorias e termos de negócios. - Execute a análise da linhagem de dados do PowerCenter Designer. Os usuários devem ter também permissão de leitura na pasta de repositório do PowerCenter.
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"> - Exiba recursos e objetos de metadados no catálogo de metadados. - Pesquise o catálogo de metadados.
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.

Privilégio	Inclui Privilégios	Permissão	Descrição
Excluir Comentários	<ul style="list-style-type: none"> - Publicar Comentários - Exibir Comentários 	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.
Exibir Glossário	n/d	Leitura	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> - Exiba glossários comerciais na exibição Glossário. - Pesquise glossários de negócios.
Gerenciar Objetos	n/d	Gravação	O usuário pode realizar as seguintes ações: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - Criar e editar agendamentos. - Adicionar agendamentos aos recursos.

Privilégio	Inclui Privilégios	Permissão	Descrição
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: - Atribua aos usuários e grupos permissões de recursos, objetos de metadados, categorias e termos comerciais. - Edite permissões de recursos, objetos de metadados, categorias e termos comerciais.

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.

Os privilégios do Serviço de Repositório do Modelo determinam as ações que os usuários podem executar nos projetos usando 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">- Editar projetos.- Excluir projetos, se o usuário os tiver criado.- Atualizar o conteúdo do Serviço de Repositório do Modelo. Para atualizar o serviço no menu Ações 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.
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 Administração de Domínio de Dados .
Gerenciar Notificações	N/D	O usuário pode configurar notificações de scorecard. Esse privilégio faz parte do grupo de privilégio de Administração de Perfil .

Privilégio	Permissão	Descrição
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"> - Nomes de projetos para os quais os usuários não têm permissão de leitura. - Detalhes de mensagens de erro e de aviso.

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 Developer	N/D	O usuário pode acessar o repositório do Modelo na Developer tool.
Criar, Editar e Excluir Projetos	N/D	O usuário pode executar as seguintes ações: <ul style="list-style-type: none"> - Criar projetos. - Atualizar o Serviço de Repositório do Modelo.
Criar, Editar e Excluir Projetos	Gravar no projeto	O usuário pode executar as seguintes ações: <ul style="list-style-type: none"> - Editar projetos. - Excluir projetos, se o usuário os tiver criado.
Mostrar Detalhes de Segurança	N/D	O usuário pode visualizar os seguintes detalhes: <ul style="list-style-type: none"> - Nomes de projetos para os quais os usuários não têm permissão de leitura. - Detalhes de mensagens de erro e de aviso.

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.

Grupo de Privilégio	Descrição
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">- Compare pastas.- Veja objetos em pastas.

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 de 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">- Altere o status das pastas.- Execute uma limpeza avançada das versões de objeto no nível da pasta.

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
- Mapplets
- 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"> - Comparar os objetos de design. - Copiar os objetos de design como uma imagem. - Exportar os objetos de design. - Gerar código para transformação Personalizada e procedimentos externos. - Receber mensagens de notificação do repositório do PowerCenter. - 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. - Pesquisar objetos de design. - Exibir objetos de design, dependências de objeto de design e histórico de objeto de design.
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">- Copiar objetos de design de uma pasta para outra.- 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.
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none">- Alterar comentários de um objeto de design com versão.- Fazer check-in e desfazer um check-out de objetos de design cujo check-out tenha sido feito pela própria conta do usuário.- Fazer check-out de objetos de design.- Copiar e colar objetos de design na mesma pasta.- 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.- Criar, editar e excluir objetos de design.- Gerar e limpar programas SAP ABAP.- Gerar mapeamentos de integração do conteúdo comercial. Os usuários também devem ter privilégios para Criar, Editar e Excluir Origens e Destinos.- Importar objetos de design usando o Designer. Os usuários também devem ter privilégios para Criar, Editar e Excluir Origens e Destinos.- 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.- Reverter para uma versão de objeto de design anterior.- Validar funções de mapeamentos, mapplets e definidas pelo usuário.

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"> - Alterar o status dos objetos de design. - Fazer check-in e desfazer check-outs de objetos de design cujo check-out foi feito por outros usuários. - Limpar versões de objetos de design. - Recuperar objetos de design excluídos.

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"> - Compare os objetos de origem e destino. - Exporte os objetos de origem e destino. - Visualize os dados de origem e destino. - Receber mensagens de notificação do repositório do PowerCenter. - 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. - Procure os objetos de origem e destino. - Exiba os objetos de origem e destino, dependências de objeto de origem e destino e histórico de objeto de origem e destino.
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">- Copiar os objetos de origem e destino para outra pasta.- 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.
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none">- Alterar comentários de um objeto de origem ou destino com versão.- 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.- Fazer check-out dos objetos de origem e destino.- Copiar e colar objetos de origem e destino na mesma pasta.- Criar, editar e excluir objetos de origem e destino.- Importar funções SAP.- Importar objetos de origem e destino usando o Designer. Os usuários também devem ter o privilégio Criar, Editar e Excluir Objetos de Design.- 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.- Gerar e executar SQL para criar destinos em um banco de dados relacional.- Reverter para uma versão de objeto de origem ou destino anterior.

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">- Alterar o status de objetos de origem e destino.- Fazer check-in e desfazer check-outs de objetos de origem e destino cujo check-out foi feito por outros usuários.- Limpar versões de objetos de origem e destino.- Recuperar objetos de origem e destino excluídos.

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">- Comparar objetos em tempo de execução.- Exportar objetos em tempo de execução.- Receber mensagens de notificação do repositório do PowerCenter.- Procurar objetos em tempo de execução.- Usar parâmetros e variáveis de mapeamento em uma sessão.- Exibir objetos em tempo de execução, dependências de objetos em tempo de execução e o histórico do objeto em tempo de execução.
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">- Copiar tarefas, fluxos de trabalho ou worklets de uma pasta para outra.- 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.
Ler e Gravar na pasta	O usuário é capaz de executar as seguintes ações: <ul style="list-style-type: none">- Atribuir um Serviço de Integração do PowerCenter a um fluxo de trabalho nas propriedades do fluxo de trabalho.- Atribuir um nível de serviço a um fluxo de trabalho.- Alterar os comentários de um objeto em tempo de execução com versão.- Fazer check-in e desfazer um check-out de objetos em tempo de execução com check-out feito pela própria conta de usuário deles.- Fazer check-out de objetos em tempo de execução.- Copiar e colar tarefas, fluxos de trabalho e worklets na mesma pasta.- 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.- Criar, editar e excluir objetos de configuração de sessão.- Excluir e validar tarefas, fluxos de trabalho e worklets.- 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.- Importar objetos em tempo de execução usando o Workflow Manager.- Reverter para uma versão do objeto anterior.
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">- Criar e editar tarefas, fluxos de trabalho e worklets.- Substituir uma conexão de banco de dados relacional por todas as sessões que usam a conexão.

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"> - Alterar o status de objetos em tempo de execução. - Fazer check-in e desfazer os check-outs de objetos em tempo de execução com check-out de outros usuários. - Limpar versões de objetos em tempo de execução. - Recuperar objetos em tempo de execução excluídos.

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"> - Exibir as propriedades de objetos em tempo de execução no Workflow Monitor.* - Exibir os logs de sessão e fluxo de trabalho no Workflow Monitor.* - Exibir detalhes de objeto em tempo de execução e desempenho no Workflow Monitor.* <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"> - Iniciar, inicializar a frio e reiniciar tarefas e fluxos de trabalho. - Recuperar tarefas e fluxos de trabalho iniciados pela própria conta de usuário deles. 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"> - Interromper e anular tarefas e fluxos de trabalho iniciados por outros usuários. - Interromper e anular tarefas que foram recuperadas automaticamente. - Cancelar agendamento de fluxos de trabalho. 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"> - Recuperar tarefas e fluxos de trabalho iniciados por outros usuários. - Recuperar tarefas que foram recuperadas automaticamente. <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"> - Criar e editar um agendador reutilizável a partir do menu Fluxos de Trabalho > Agendadores. - Editar um agendador não reutilizável a partir das propriedades do fluxo de trabalho. - 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. <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"> - Editar grupos de implantação. - Remover objetos de um grupo de implantação.
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">- Serviço de Agendador- O Serviço de Integração de Dados que executa os trabalhos que o usuário deseja agendar
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">- Serviço de Agendador- O Serviço de Integração de Dados que executa os trabalhos que o usuário deseja agendar
Excluir Agendamento	O usuário pode excluir agendamentos.	Serviço de Agendador
Exibir Agendamentos	O usuário pode visualizar a exibição Agendamentos 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, 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. Nota: 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.
Subconjunto de Dados	Inclui privilégios para exibir e gerenciar objetos de subconjunto, incluindo entidades, grupos e modelos 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.
Regras	Inclui privilégios para exibir e gerenciar regras de mascaramento e geração no Test Data Manager.
Geração de Dados	Inclui privilégios para exibir e gerenciar a geração de dados de teste 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:

Privilégio	Inclui Privilégios	Permissão	Descrição
Gerenciar Preferências	-	Gravação	<p>O usuário pode realizar as seguintes ações no Informatica Administrator e no Test Data Manager:</p> <ul style="list-style-type: none">- Criar funções.- Editar funções.- Excluir funções.- Exibir funções.- Associar funções a usuários.- Associar privilégios a usuários.- Associar funções a grupos de usuários.- Associar privilégios a grupos de usuários.- Adicionar licenças.- Configurar o repositório do TDM.- Configurar o repositório do PowerCenter.- Configurar os níveis de sensibilidade do domínio de dados.- Configure um repositório do Test Data Warehouse.- Configure um Test Data Warehouse.- Configurar os atributos personalizados do projeto.- Configurar os atributos de geração de fluxo de trabalho.- Ativar a descoberta de dados.- Configurar serviços de criação de perfil.- Exibir objetos de administração.- Configure opções de indexação de pesquisa de palavra-chave.
Exibir Conexões	-	Leitura	<p>O usuário pode realizar as seguintes ações na página Conexões do Test Data Manager:</p> <ul style="list-style-type: none">- Exibir conexões.- Testar conexões.
Gerenciar Conexões	Exibir Conexões	Gravação	<p>O usuário pode realizar as seguintes ações na página Conexões do Test Data Manager:</p> <ul style="list-style-type: none">- Criar conexões.- Editar conexões.- Excluir conexões.- Exibir conexões.- Testar conexões.- Configure um repositório do Test Data Warehouse.- Configure um Test Data Warehouse.

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">- Criar conexões.- Editar conexões.- Excluir conexões.- Exibir conexões.- Testar conexões.

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">- Criar domínios de dados.- Editar domínios de dados.- Excluir domínios de dados.- Exibir domínios de dados.

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">- Adicionar atribuições de regra e diretiva.- Excluir atribuições de regra e diretiva.- Substituir as propriedades de regra.- Exibir atribuições de mascaramento de dados.

Grupo de Privilégio 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:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Subconjunto de Dados	-	Ler	O usuário pode realizar as seguintes ações de subconjunto de dados no Test Data Manager: <ul style="list-style-type: none">- Exibir grupos.- Exibir modelos.- Exibir entidades.- Exibir objetos de projeto recentes.
Gerenciar Subconjunto de Dados	Exibir Subconjunto de Dados	Gravar	O usuário pode realizar as seguintes ações de subconjunto de dados no Test Data Manager: <ul style="list-style-type: none">- Criar grupos.- Editar grupos.- Excluir grupos.- Adicionar parâmetros de grupo.- Criar modelos.- Editar modelos.- Excluir modelos.- Adicionar parâmetros de modelo.- Criar a entidade.- Editar a entidade.- Excluir a entidade.- Adicionar critérios da entidade.- Ativar relacionamentos.- Desativar relacionamentos.- Editar relacionamentos.- Revisar e agir quando houver alterações.- Marcar a análise de alterações como concluída.

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">- Criar diretivas.- Editar diretivas.- Excluir diretivas.- Exibir diretivas.

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:

Privilégio	Inclui Privilégios	Permissão	Descrição
Exibir Projeto	-	Leitura	<p>O usuário pode realizar as seguintes ações em projetos no Test Data Manager:</p> <ul style="list-style-type: none">- Exibir projetos.- Exibir planos.- Exibir relatórios detalhados de planos.- Exibir relatórios de auditoria de planos.- Exibir projetos recentes.- Criar planos do Test Data Warehouse- Gerenciar planos do Test Data Warehouse- Gerar planos do Test Data Warehouse- Executar planos do Test Data Warehouse
Gerenciar Projeto	Exibir Projeto	Gravação	<p>O usuário pode realizar as seguintes ações em projetos no Test Data Manager:</p> <ul style="list-style-type: none">- Criar projetos.- Editar projetos.- Excluir projetos.- Exibir projetos.- Associar usuários a projetos.- Associar grupos de usuários a projetos.- Associar ou remover regras de projetos.- Associar ou remover diretivas de projetos.- Criar planos.- Editar planos.- Excluir planos.- Gerar planos.

Privilégio	Inclui Privilégios	Permissão	Descrição
Descobrir Projeto	-	Gravação	<p>O usuário pode realizar as seguintes ações de descoberta em projetos no Test Data Manager:</p> <ul style="list-style-type: none"> - Classificar tabelas. - Marcar descoberta como concluída. - Associar domínios de dados a colunas. - Marcar colunas como restritas. - Marcar colunas como confidenciais - Definir coluna de valores semelhantes - Remover colunas de valores semelhantes - Adicionar chaves primárias - Remover Chaves primárias - Criar restrições lógicas - Exibir restrições lógicas - Editar Restrições lógicas - Excluir Restrições Lógicas - Exibir projetos. - Exibir domínios de dados com perfil. - Aprovar ou rejeitar domínios de dados de perfil. - Marcar classificação de domínio de dados como concluída. - Exibir chaves primárias com perfil. - Aprovar ou rejeitar chaves primárias com perfil. - Marcar descoberta de chave primária como concluída. - Exibir entidades com perfil. - Aprovar ou rejeitar entidades com perfil. - Marcar descoberta de entidade como concluída. - Exibir análise de riscos do projeto. - Exibir distribuição de dados confidenciais de projeto recentes.
Gerar Projeto	-	Gravação	O usuário pode gerar fluxos de trabalho no Test Data Manager.
Executar Projeto	-	Gravação	<p>O usuário pode realizar as seguintes ações de execução em projetos no Test Data Manager:</p> <ul style="list-style-type: none"> - Executar planos. - Executar fluxos de trabalho. - Interromper fluxos de trabalho. - Anular fluxos de trabalho. - Recuperar fluxos de trabalho. - Exibir execução do plano.
Monitorar Projeto	-	Leitura	<p>O usuário pode realizar as seguintes ações de monitoramento em projetos no Test Data Manager:</p> <ul style="list-style-type: none"> - Monitorar trabalhos do projeto. - Exibir logs do trabalho do projeto. - Monitorar trabalhos em projetos. - Exibir logs do trabalho em projetos.
Auditar Projeto	-	Leitura	O usuário pode exibir a atividade recente em projetos e planos no Test Data Manager.
Importar Metadados	-	Gravação	<p>O usuário pode realizar as seguintes ações em projetos no Test Data Manager:</p> <ul style="list-style-type: none"> - Importar origens. - Excluir origens.

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.
- Exibir a geração de regras do grupo de privilégios Regras. Para criar um plano com a geração de componentes.

Grupo de Privilégio Regras

Os privilégios no grupo de privilégio Regras determinam as tarefas que os usuários podem realizar em regras de mascaramento e geração de dados no Test Data Manager.

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 Regras de Mascaramento	-	Ler	O usuário pode exibir regras de mascaramento no Test Data Manager.
Gerenciar Regras de Mascaramento	Exibir Regras de Mascaramento	Gravar	O usuário pode realizar as seguintes ações em regras de mascaramento de dados no Test Data Manager: <ul style="list-style-type: none">- Criar regras de mascaramento.- Editar regras de mascaramento.- Excluir regras de mascaramento.- Exibir regras de mascaramento.
Exibir Regras de Geração	-	Ler	O usuário pode exibir regras de geração no Test Data Manager.
Gerenciar Regras de Geração	Exibir Regras de Geração	Gravar	O usuário pode realizar as seguintes ações em regras de geração de dados no Test Data Manager: <ul style="list-style-type: none">- Criar regras de geração.- Editar regras de geração.- Excluir regras de geração.- Exibir regras de geração.

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">- Exibir atribuições de regra de geração de dados.- Adicionar atribuições de regra de geração de dados.- Excluir atribuições de regra de geração de dados.- Substituir atribuições de regra de geração de dados.

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.

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.

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.

O UMSM tem os seguintes tipos de funções:

- Administrador. Essa é uma função definida pelo sistema que tem privilégios para administrar a ferramenta Administrator. Com essa função, você pode criar e gerenciar contas de usuário, criar o Serviço do Ultra Messaging e configurá-lo, configurar os componentes do UMSM e implantações do UM.
- Operador. Essa é uma função personalizada que tem privilégios para monitorar implantações do UM.

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 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.

Quando você atribui a função Administrador a um usuário ou grupo para o domínio, o Serviço de Integração de Dados ou o Serviço de Repositório do Modelo, o usuário ou grupo recebe todos os privilégios para o serviço. A função de Administrador ignora a verificação de permissão. Usuários com a função de administrador podem acessar todos os objetos gerenciados pelo serviço.

Quando você atribui a função Administrador a um usuário ou grupo para o domínio ou o Serviço do Ultra Messaging, o usuário ou grupo recebe todos os privilégios para o 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.

Quando você atribui a função Administrador a um usuário ou grupo para o domínio ou Serviço de Integração de Dados, o usuário ou grupo pode realizar algumas tarefas, que são determinadas pela função Administrador, não por privilégios ou permissões.

Quando você atribui a função Administrador a um usuário ou grupo para o domínio ou Serviço do Ultra Messaging, o usuário ou grupo pode realizar algumas tarefas, que são determinadas pela função Administrador, 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.

Você pode atribuir a um usuário ou grupo todos os privilégios para o domínio ou Serviço de Integração de Dados e, em seguida, conceder ao usuário ou grupo permissões completas sobre todos os objetos de domínio. No entanto, esse usuário ou grupo não pode executar as tarefas determinadas pela função Administrador.

Você pode atribuir a um usuário ou grupo todos os privilégios para o domínio ou Serviço do Ultra Messaging e, em seguida, conceder ao usuário ou grupo permissões completas sobre todos os objetos de domínio. 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 Administrador. 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, Serviço de Integração de Dados, e do Serviço do Repositório do PowerCenter:

A tabela a seguir lista as tarefas determinadas pela função Administrador para o domínio ou Serviço de Integração de Dados:

A tabela a seguir lista as tarefas determinadas pela função Administrador para o domínio ou Serviço do Ultra Messaging:

Serviço	Tarefas
Domínio	<ul style="list-style-type: none"> - Configure as propriedades do domínio. - Criar perfis do sistema operacional. - Excluir perfis do sistema operacional. - Conceder permissão nos perfis de domínio e sistema operacional. - Gerencie e limpe os eventos de log. - Receba alertas de domínio. - Executar o Relatório da Licença. - Exiba os eventos de log de atividade do usuário. - Desligar o domínio. - Acesse o assistente de atualização de serviço.
Serviço de Integração de Dados	<ul style="list-style-type: none"> - Atualizar o Serviço de Integração de Dados usando o menu Ações.
Serviço do Repositório do PowerCenter	<ul style="list-style-type: none"> - Atribuir perfis de sistema operacional a pastas de repositório se o Serviço de Integração do PowerCenter usar perfis de sistema operacional.* - Alterar o proprietário de pastas e objetos globais.* - Configurar permissões de pastas e objetos globais.* - 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. - Exclua um Serviço de Integração do PowerCenter no navegador do Workflow Manager. - Excluir pastas e objetos globais.* - Designar pastas para compartilhamento.* - Editar nome e descrição de pastas.* <p>*O proprietário da pasta de repositório do PowerCenter ou o proprietário do objeto global também pode concluir essas tarefas.</p>

Serviço	Tarefas
Domínio	<ul style="list-style-type: none"> - Configure as propriedades do domínio. - Conceda permissão no domínio. - Gerencie e limpe os eventos de log. - Receba alertas de domínio. - Exiba os eventos de log de atividade do usuário.

Serviço	Tarefas
Domínio	<ul style="list-style-type: none"> - Configure as propriedades do domínio. - Conceda permissão no domínio. - Gerencie e limpe os eventos de log. - Receba alertas de domínio.

Serviço	Tarefas
	- Exiba os eventos de log de atividade do usuário.

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 Administrador, 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 logon 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, 186](#)
- [Permissões do Objeto de Domínio, 189](#)
- [Permissões de Conexão, 194](#)
- [Permissões de aplicativos e objetos de aplicativo, 196](#)
- [Permissões de Serviço de Dados SQL, 198](#)
- [Permissões do serviço da Web, 202](#)

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:

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.

Tipo de objeto	Ferramenta	Descrição
Objetos de conexão	Ferramenta Administrator Developer tool	É possível atribuir permissões em conexões definidas na ferramenta Administrator ou na Developer tool. Essas ferramentas compartilham as permissões de conexão.
Objetos de domínio	Ferramenta Administrator	Você pode atribuir permissões nos seguintes objetos de domínio: domínio, pastas, nós e serviços de aplicativo.
Projetos do repositório do Modelo	Developer tool	Você pode atribuir permissões em projetos definidos na Developer tool.

Você pode usar a ferramenta Administrator para configurar permissões em um objeto de domínio. Você pode atribuir permissões nos seguintes objetos de domínio:

- domínio
- nó
- serviços de aplicativo

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 .

Permissões que os usuários herdam. Quando os usuários têm permissão em um domínio, eles herdam a permissão em todos os objetos no domínio. 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.

Permissões que os usuários herdam. Quando os usuários têm permissão em um domínio, eles herdam a permissão em todos os objetos no domínio. 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.

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 Administrador 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 Administrador acessem todos os objetos da pasta na ferramenta Administrador. 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 Administrador 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 Administrador 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 Administrador exibam e editem as propriedades da licença. Sem permissão, um usuário não pode usar a licença ao criar um serviço de aplicativo.
Serviço de Aplicativo	Permite que os usuários da ferramenta Administrador 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.

Tipo de Objeto de Domínio	Descrição de Permissão
Domínio	Permite que os usuários da ferramenta Administrador acessem todos os objetos no domínio. Quando os usuários têm permissão em um domínio, eles herdam a permissão em todos os objetos no domínio.
Nó	Permite que os usuários da ferramenta Administrador exibam e editem as propriedades do nó.

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.
Licença	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades da licença.

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.
Nó	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades do nó.
Serviço de Aplicativo	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades de serviço de aplicativo.
Licença	Permite que os usuários da ferramenta Administrator exibam e editem as propriedades da licença.

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. No cabeçalho do Informatica Administrator, clique em **Gerenciar > Permissões**.

A caixa de diálogo **Gerenciar Permissões** é exibida.

2. Clique na guia **Grupos** ou **Usuários**.
3. Digite uma string para procurar usuários e grupos e clique no botão **Filtro**.
4. Selecione um usuário ou grupo.
5. Selecione um objeto de domínio 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.

6. Clique em **Fechar**.
7. Ou clique em **Editar Permissões** para editar permissões diretas.

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.

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. No cabeçalho do Informatica Administrator, clique em **Gerenciar > Permissões**.

A caixa de diálogo **Gerenciar permissões** é exibida.

2. Clique na guia **Grupos** ou **Usuários**.
3. Digite uma cadeia de caracteres para procurar usuários e grupos e clique no botão **Filtrar**.
4. Selecione um usuário ou grupo.
5. Selecione um objeto de domínio e clique no botão **Editar Permissões Diretas**.

A caixa de diálogo **Editar Permissões** é exibida.

6. Para atribuir a permissão no objeto, selecione **Permitir**.
7. Para revogar a permissão no objeto, selecione **Revogar**.

Você pode ver se a permissão é atribuída diretamente ou herdada clicando em **Exibir Detalhes de Permissão**.

8. Clique em **OK**.
9. Clique em **Fechar**.

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 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** e clique em **Conceder Permissão**.

A caixa de diálogo **Atribuir Usuários/Grupos ao Perfil do Sistema Operacional** exibe todos os usuários ou grupos que não têm permissão no perfil do sistema operacional.

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 **Próximo**.
6. Selecione **Permitir** e clique em **Concluir**.

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.

Você pode configurar permissões em uma conexão 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.
- Serviço de Integração de Dados. Impõe permissões de execução quando um usuário tenta visualizar dados ou executar um mapeamento 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

Ação	Tipos de Permissão
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. Acesse os dados físicos da fonte de dados subjacente definida pela conexão. Os usuários podem visualizar dados, executar um mapeamento, executar um mapeamento em uma tarefa de Mapeamento de fluxo de trabalho ou executar um perfil que usa 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. 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 **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.

7. Clique em **Fechar**.
8. 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 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 Administrador 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,

you attributed a selection permission to a user in a SQL data service. The user inherits the permission to select in all virtual tables in the SQL data service.

You can deny permissions for users and groups on some service objects in the SQL data service. When you deny permissions, you configure exceptions for the permissions that users and groups already have. For example, you cannot attribute permissions for a column in a virtual table, but you can deny that a user execute a SQL SELECT instruction that includes the column.

Types of SQL Data Service Permissions

You can attribute the following permissions to users and groups:

- **Permission to grant.** Users can grant and revoke permissions on service objects in the SQL data service using the Administrator tool or using the *infacmd* command-line program.
- **Permission to execute.** Users can execute virtual procedures stored in the SQL data service using a client tool such as JDBC or ODBC.
- **Permission to select.** Users can execute SQL SELECT instructions on virtual tables in the SQL data service using a client tool such as JDBC or ODBC.

Some permissions are not applicable to all service objects in the SQL data service.

The following table describes the permissions for each service object in the SQL data service:

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.	-

Attributing Permissions in a SQL Data Service

When you attribute permissions to a service object in the SQL data service, you define the access level of a user or group to the object.

1. In the **Manage** guide, select the **Services and Me** display.
2. In the **Navigator**, select a Data Integration Service.
3. In the content panel, select the **Applications** display.
4. Select the service object.
5. In the details panel, select the **Group Permissions** or **User Permissions** display.
6. Click the **Attribute Permission** button.

The **Attribute Permissions** dialog box displays all users or groups that do not have permission to the service object.

7. Enter filter conditions to search for users and groups and click the **Filter** button.
8. Select a user or group and click **Next**.
9. Select **Allow** for each type of permission that you want to attribute.

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.

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, 206](#)
- [Informações Pessoais do Usuário, 207](#)
- [Associação de Grupo de Usuários, 207](#)
- [Privilégios, 208](#)
- [Associação de Funções, 209](#)
- [Permissões em Objetos de Domínio, 209](#)
- [Selecionando Usuários para um Relatório de Auditoria, 210](#)
- [Selecionando Grupos para um Relatório de Auditoria, 211](#)
- [Selecionando Funções para um Relatório de Auditoria, 211](#)

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*, 213](#)
- [Comandos *infacmd dis*, 214](#)
- [Comandos *infacmd es*, 216](#)
- [Comandos *infacmd ipc*, 216](#)
- [Comandos *infacmd isp*, 216](#)
- [Comandos *infacmd mrs*, 228](#)
- [Comandos *infacmd ms*, 230](#)
- [Comandos *infacmd oie*, 231](#)
- [Comandos *infacmd ps*, 231](#)
- [Comandos *infacmd pwx*, 232](#)
- [Comandos *infacmd rms*, 233](#)
- [Comandos *infacmd rtm*, 234](#)
- [Comandos *infacmd sch*, 234](#)
- [Comandos *infacmd sql*, 235](#)
- [Comandos *infacmd wfs*, 236](#)
- [Comandos *pmcmd*, 236](#)
- [Comandos *pmrep*, 239](#)

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 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 <i>infacmd dis</i>	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	-	-	-
ListApplications	-	-	-

Comando infacmd dis	Grupo de Privilégios	Nome do Privilégio	Permissão para...
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 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.

Os usuários devem ser atribuído a função Administrador para o domínio para executar os comandos a seguir:

- AddDomainLink
- AssignGroupPermission (no domínio)
- AssignGroupPermission (nos perfis do sistema operacional)
- AddServiceLevel
- AssignUserPermission (no domínio)
- AssignUserPermission (nos perfis do sistema operacional)
- CreateConnection
- CreateOSProfile
- PurgeLog
- RemoveDomainLink

- RemoveOSProfile
- RemoveServiceLevel
- SwitchToGatewayNode
- SwitchToWorkerNode
- UpdateDomainOptions
- UpdateGatewayInfo
- UpdateServiceLevel
- UpdateSMTPOptions

A função Administrador para o domínio deve ser atribuída aos usuários para a execução do comando UpdateGatewayInfo.

A tabela a seguir relaciona os privilégios e permissões necessários para os comandos *infacmd isp*:

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
GetNodeName	-	-	Nó
UpdateGatewayInfo	-	-	-

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
AddAlertUser (para sua conta de usuário)	-	-	-
AddAlertUser (para outros usuários)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
AddConnectionPermissions	-	-	Conceder na conexão
AddDomainLink	-	-	-
AddDomainNode	Administração de Domínio	Gerenciar Nós e Grades	Domínio e nó
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)	-	-	-

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
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	-	-	-
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.
AssignUserToGroup	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
AssignedToLicense	Administração de Domínio	Gerenciar Serviços	Objeto de licença e serviço de aplicativo
AssignISTOMMSservice	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
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.
AssignRSToWSHubService	Administração de Domínio	Gerenciar Serviços	Serviço do Repositório do PowerCenter e Hub de Serviços da Web
ConvertLogFile	-	-	Domínio ou serviço de aplicativo
CreateFolder	Administração de Domínio	Gerenciar Pastas do Domínio	Pasta pai ou do domínio
CreateConnection	-	-	-
CreateGrid	Administração de Domínio	Gerenciar Nós e Grades	Pasta pai ou de domínio e nós atribuídos à grade
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

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
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

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
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 usuários, grupos e funções)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ExportDomainObjects (para conexões)	Administração de Domínio	Gerenciar conexões	Leitura em conexões

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
ExportUsersAndGroups	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
generateHadoopConnectionFromHiveConection	-	-	-
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 usuários, grupos e funções)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ImportDomainObjects (para conexões)	Administração de Domínio	Gerenciar conexões	Gravar em conexões
ImportUsersAndGroups	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ListAlertUsers	-	-	Domínio
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
ListConnectionOptions	-	-	Leitura na conexão
ListConnections	-	-	-
ListConnectionPermissions	-	-	-
ListConnectionPermissions por grupo	-	-	-
ListConnectionPermissions por usuário	-	-	-
ListDomainLinks	-	-	Domínio
ListDomainOptions	-	-	Domínio
ListFolders	-	-	Pastas
ListGridNodes	-	-	-
ListGroupsForUser	-	-	Domínio
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.
ListLDAPConnectivity	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
ListLicenses	-	-	Objetos de licença
listMonitoringOptions	Monitoramento	Configuração de Monitoramento	Domínio
ListNodeOptions	-	-	Nó
ListNodes	-	-	-
ListNodeResources	-	-	Nó
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domínio
ListRolePrivileges	-	-	-
ListSecurityDomains	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
ListServiceLevels	-	-	Domínio
ListServiceNodes	-	-	Serviço de aplicativo
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListSMTPOptions	-	-	Domínio
ListUserPermissions	-	-	-
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	-	-	-
purgeMonitoringData	Monitoramento	Configuração de Monitoramento	Domínio
RemoveAlertUser (para conta de usuário)	-	-	-
RemoveAlertUser (para outros usuários)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
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

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
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
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	-

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
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 sua conta de usuário)	-	-	-
ResetPassword (para outros usuários)	Administração de Segurança	Gerenciar Usuários, Grupos e Funções	-
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
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
UnassignLicense	Administração de Domínio	Gerenciar Serviços	Objeto de licença e serviço de aplicativo
UnAssignRoleFromGroup	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
UnAssignRoleFromUser	Administração de Segurança	Conceder privilégios e funções	Domínio, Serviço do Metadata Manager, Serviço de Repositório do Modelo ou Serviço de Repositório do PowerCenter.
UnassignRSWHubService	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
updateMonitoringOptions	Monitoramento	Configuração de Monitoramento	Domínio
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

Comando infacmd isp	Grupo de Privilégios	Nome do Privilégio	Permissão Ativada
UpdateSAPBWService	Administração de Domínio	Gerenciar Serviços	Serviço SAP BW
UpdateServiceLevel	-	-	-
UpdateServiceProcess	Administração de Domínio	Gerenciar Serviços	Serviço de Integração do PowerCenter Cada nó adicionado ao Serviço de Integração do PowerCenter
UpdateSMTPOptions	-	-	-
UpdateWSHubService	Administração de Domínio	Gerenciar Serviços	Hub de Serviços da Web

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 infacmd mrs	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

Comando infacmd mrs	Grupo de Privilégios	Nome do Privilégio	Permissão para...
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
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

Comando <i>infacmd mrs</i>	Grupo de Privilégios	Nome do Privilégio	Permissão para...
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 <i>infacmd ms</i>	Grupo de Privilégios	Nome do Privilégio	Permissão para...
GetRequestLog	-	-	-
ListMappings	-	-	-
ListMappingParams	-	-	-
RunMapping	-	-	Executar objetos de conexão usados pelo mapeamento.

Comandos *infacmd oie*

Para executar comandos *infacmd oie*, o usuário deve ter uma das permissões de objeto de repositório do modelo listadas.

A tabela a seguir lista as permissões necessárias para comandos *infacmd oie*:

Comando <i>infacmd oie</i>	Grupo de Privilégio	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

Comando infacmd ps	Grupo de Privilégio	Nome do Privilégio	Permissão para...
List	-	-	Leitura do projeto
Purge	-	-	Ler e gravar no projeto

Comando infacmd ps	Grupo de Privilégio	Nome do Privilégio	Permissão para...
CreateWH	-	-	-
DropWH	-	-	-

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 infacmd pwx	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	-
DisplayMemoryLogger	Comandos de Informações	displaymemory	-

Comando infacmd pwx	Grupo de Privilégio	Nome do Privilégio	Permissão para...
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`
- `getrunningessionsdetails`
- `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
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- 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 privilégio	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
CheckIn (para seus próprios check-outs)	Origens e Destinos	Criar, Editar e Excluir	Ler e Gravar na pasta

Comando pmrep	Grupo de privilégio	Nome do privilégio	Permissão
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	-
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
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

Comando pmrep	Grupo de privilégio	Nome do privilégio	Permissão
DeployFolder	Pastas	Copiar no repositório original Criar no repositório de destino	Ler na pasta
ExecuteQuery	-	-	Ler e executar na consulta
Sair	-	-	-
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
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

Comando pmrep	Grupo de privilégio	Nome do privilégio	Permissão
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
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

Comando pmrep	Grupo de privilégio	Nome do privilégio	Permissão
UndoCheckout (para check-outs de outros)	Objetos de Tempo de Execução	Gerenciar Versões	Ler e Gravar na pasta
Cancelarregistro	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, 244](#)
- [Funções Personalizadas do Serviço do Metadata Manager, 245](#)
- [Função Personalizada do Operador, 247](#)
- [Funções Personalizadas do Serviço do Repositório do PowerCenter, 248](#)
- [Regras personalizadas do Test Data Manager, 249](#)

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">- Compartilhar Atalhos- Exibir Linhagem- Exibir Catálogos Relacionados- Exibir Relatórios- Exibir Resultados do Perfil- Exibir Catálogo- Exibir Relacionamentos- Gerenciar Relacionamentos- Exibir Comentários- Publicar Comentários- Excluir Comentários- Exibir Links- Gerenciar Links- Exibir Glossário- Gerenciar Objetos
Carregar	<ul style="list-style-type: none">- Exibir Recurso- Carregar Recurso- Gerenciar Agendamento- Limpar Metadados- Gerenciar Recurso
Modelo	<ul style="list-style-type: none">- Exibir Modelo- Gerenciar Modelo- Exportar/Importar Modelos
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">- Exibir Linhagem- Exibir Catálogos Relacionados- Exibir Catálogo- Exibir Relacionamentos- Exibir Comentários- Exibir Links
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">- Exibir Linhagem- Exibir Catálogos Relacionados- Exibir Relatórios- Exibir Resultados do Perfil- Exibir Catálogo- Exibir Relacionamentos- Exibir Comentários- Publicar Comentários- Excluir Comentários- Exibir Links- Gerenciar Links- Exibir Glossário
Carregar	<ul style="list-style-type: none">- Exibir Recurso- Carregar Recurso
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">- Exibição: Exibir Trabalhos e Outros Usuários- Exibição: Exibir Estatísticas- Exibição: Exibir Relatórios- Monitoramento de Acesso: Acesso com a Ferramenta Analyst- Monitoramento de Acesso: Acesso com a Developer Tool- Monitoramento de Acesso: Acesso com a Ferramenta Administrator- Executar Ações nas Tarefas <p>Nota: 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">- Gerenciar Trabalhos Agendados: Criar Agendamento- Gerenciar Trabalhos Agendados: Excluir Agendamento- Gerenciar Trabalhos Agendados: Editar Agendamento- Gerenciar Trabalhos Agendados: Exibir Agendamentos
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">- Acessar o Designer- Acessar o Workflow Manager- Acessar o Workflow Monitor
Objetos de Design	<ul style="list-style-type: none">- Criar, Editar e Excluir- Gerenciar Versões
Origens e Destinos	<ul style="list-style-type: none">- Criar, Editar e Excluir- Gerenciar Versões
Objetos de Tempo de Execução	<ul style="list-style-type: none">- Criar, Editar e Excluir- Executar- Gerenciar Versões- Monitorar

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">- Executar- Gerenciar Execução- Monitorar

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">- Copiar- Criar- Gerenciar Versões
Objetos Globais	<ul style="list-style-type: none">- Gerenciar Grupos de Implantação- Executar Grupos de Implantação- Criar Rótulos- Criar Consultas

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">- Exibir Conexões- Gerenciar Conexões- Gerenciar Preferências

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">- Exibir Diretivas- Gerenciar Diretivas
Domínios de Dados	<ul style="list-style-type: none">- Exibir Domínios de Dados- Gerenciar Domínios de Dados

Grupo de Privilégios	Nome do Privilégio
Regras	<ul style="list-style-type: none"> - Exibir Regras de Mascaramento - Gerenciar Regras de Mascaramento - Exibir Regras de Geração - Gerenciar Regras de Geração
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"> - Exibir Projeto - Executar Projeto - Monitorar Projeto - Auditar projeto
Administração	<ul style="list-style-type: none"> - Exibir Conexões - Gerenciar Conexões
Conjuntos de Dados	<ul style="list-style-type: none"> - Exibir Conjunto de Dados - Exibir Dados no Conjunto de Dados.

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
Regras	<ul style="list-style-type: none"> - Exibir Regras de Mascaramento - Exibir Regras de Geração - Gerenciar Regras de Geração
Domínios de Dados	Exibir Domínios de Dados
Projetos	<ul style="list-style-type: none"> - Exibir Projeto - Descobrir Projeto - Executar Projeto - Monitorar Projeto - Auditar projeto - Importar Metadados
Mascaramento de dados	<ul style="list-style-type: none"> - Exibir Mascaramento de Dados - Gerenciar Mascaramento de Dados
Subconjunto de Dados	<ul style="list-style-type: none"> - Exibir Subconjunto de Dados - Gerenciar Subconjunto de Dados

Grupo de Privilégios	Nome do Privilégio
Geração de Dados	<ul style="list-style-type: none"> - Exibir Geração de Dados - Gerenciar Geração de Dados
Administração	<ul style="list-style-type: none"> - Exibir Conexões - Gerenciar Conexões
Conjuntos de Dados	<ul style="list-style-type: none"> - Exibir Conjunto de Dados - Exibir Dados no Conjunto de Dados

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
Regras	<ul style="list-style-type: none"> - Exibir Regras de Mascaramento - Exibir Regras de Geração - Gerenciar Regras de Geração
Domínios de Dados	Exibir Domínios de Dados
Projetos	<ul style="list-style-type: none"> - Exibir Projeto - Gerenciar Projeto - Descobrir Projeto - Executar Projeto - Monitorar Projeto - Auditar projeto - Importar Metadados
Mascaramento de dados	<ul style="list-style-type: none"> - Exibir Mascaramento de Dados - Gerenciar Mascaramento de Dados
Subconjunto de Dados	<ul style="list-style-type: none"> - Exibir Subconjunto de Dados - Gerenciar Subconjunto de Dados
Geração de Dados	<ul style="list-style-type: none"> - Exibir Geração de Dados - Gerenciar Geração de Dados
Administração	<ul style="list-style-type: none"> - Exibir Conexões - Gerenciar Conexões
Conjuntos de Dados	<ul style="list-style-type: none"> - Exibir Conjunto de Dados - Exibir Dados no Conjunto de Dados - Gerenciar Conjunto de Dados - Gerenciar Dados no Conjunto de Dados - Redefinir Conjunto de Dados

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
Regras	<ul style="list-style-type: none">- Exibir Regras de Mascaramento- Exibir Regras de Geração
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
Regras	<ul style="list-style-type: none">- Exibir Regras de Mascaramento- Gerenciar Regras de Mascaramento- Exibir Regras de Geração- Gerenciar Regras de Geração
Domínios de Dados	<ul style="list-style-type: none">- Exibir Domínios de Dados- Gerenciar Domínios de Dados
Projetos	<ul style="list-style-type: none">- Exibir Projeto- Gerenciar Projeto- Descobrir Projeto- Executar Projeto- Monitorar Projeto- Auditar projeto- Importar Metadados
Mascaramento de dados	<ul style="list-style-type: none">- Exibir Mascaramento de Dados- Gerenciar Mascaramento de Dados
Subconjunto de Dados	<ul style="list-style-type: none">- Exibir Subconjunto de Dados- Gerenciar Subconjunto de Dados
Geração de Dados	<ul style="list-style-type: none">- Exibir Geração de Dados- Gerenciar Geração de Dados

Grupo de Privilégios	Nome do Privilégio
Administração	<ul style="list-style-type: none"> - Exibir Conexões - Gerenciar Conexões
Conjuntos de Dados	<ul style="list-style-type: none"> - Exibir Conjunto de Dados - Exibir Dados no Conjunto de Dados - Gerenciar Conjunto de Dados - Gerenciar Dados no Conjunto de Dados - Redefinir Conjunto de Dados

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"> - Exibir Projeto - Monitorar Projeto
Conjuntos de Dados	<ul style="list-style-type: none"> - Exibir Conjunto de Dados - Gerenciar Conjunto de Dados - Redefinir Conjunto de Dados - Exibir Dados no Conjunto de Dados - Gerenciar Dados no Conjunto de Dados

APÊNDICE C

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

ÍNDICE

A

- Active Directory Federation Services
 - configurando para logon único [89](#)
- Administrador
 - função [178](#)
- administrador de domínio
 - descrição [113](#)
- administrador padrão
 - descrição [112](#)
 - modificando [112](#)
 - senhas, alterando [112](#)
- administradores
 - cliente de aplicativo [113](#)
 - domínio [113](#)
 - padrão [112](#)
- alterando
 - senha da conta de usuário [108](#)
- aplicativo
 - permissões [196](#)
- arquivo de truststore cacerts [28](#)
- arquivos de migração do usuário
 - migrateUsers [32](#)
- as
 - permissões por comando [213](#)
 - privilegios por comando [213](#)
- autenticação
 - Kerberos [20](#)
 - LDAP [19](#), [23](#), [103](#)
 - nativa [19](#), [103](#)
 - Service Manager [103](#)
- autenticação Kerberos
 - descrição [20](#)
 - usando bibliotecas personalizadas [50](#)
- autenticação LDAP
 - certificado SSL autoassinado [28](#)
 - configurando [23](#)
 - descrição [19](#), [103](#)
 - grupos aninhados [28](#)
 - serviços de diretório [23](#)
 - tempos de sincronização [27](#)
- autenticação nativa
 - descrição [19](#), [103](#)
- autorização
 - Gerenciador de Serviços [104](#)
 - Serviço de Integração de Dados [104](#)
 - Serviço de Repositório do Modelo [104](#)
 - Serviço do Metadata Manager [104](#)
 - Serviço do Repositório do PowerCenter [104](#)
 - serviços de aplicativo [104](#)

C

- Carregar grupo de privilégio
 - descrição [149](#)

- certificado SSL
 - Autenticação de usuário LDAP [23](#)
 - autenticação LDAP [28](#)
- Cliente do PowerCenter
 - administrador [113](#)
- conexões
 - permissões [194](#)
 - permissões padrão [195](#)
 - tipos de permissão [194](#)
- configuração de cliente
 - domínio seguro [60](#)
- consultas de objeto
 - privilegios para o PowerCenter [164](#)
- contas
 - alterando a senha [108](#)
- contas de usuário
 - alterando a senha [108](#)
 - ativando [117](#)
 - criadas durante a instalação [112](#)
 - padrão [112](#)
 - visão geral [112](#)
- convertUserActivityLog
 - logs de atividade do usuário [119](#)
- Criar Tabelas de Referência
 - privilegio [146](#)

D

- Data Integration Service
 - privilegios [147](#)
- descrição do grupo
 - caracteres inválidos [122](#)
- descrição do usuário
 - caracteres inválidos [115](#)
- destinos
 - privilegios [158](#)
- dis
 - permissões por comando [214](#)
 - privilegios por comando [214](#)
- domínio
 - administrador [113](#)
 - Função Administrador [178](#)
 - privilegios [136](#)
 - privilegios de administração [138](#)
 - privilegios de administração de segurança [137](#)
 - segurança do usuário [109](#)
 - sincronização de usuário [104](#)
 - usuários com privilegios [183](#)
- domínio de segurança LDAP
 - descrição [19](#), [20](#)
- domínio de segurança nativo
 - descrição [19](#)
- domínio Informatica
 - permissões [109](#)
 - privilegios [109](#)

- domínio Informatica ()
 - segurança do usuário [109](#)
 - usuários, gerenciando [114](#)
- domínio seguro
 - configuração de cliente [60](#)
- domínios de segurança
 - configurando LDAP [25](#)
 - exclusão de LDAP [29](#)
 - LDAP [19](#), [20](#), [22](#)
 - nativa [19](#)
- domínios de segurança LDAP
 - descrição [22](#)
- Domínios de segurança LDAP
 - configurando [25](#)
 - excluindo [29](#)

E

- Editar Metadados de Tabela de Referência
 - privilegio [146](#)
- es
 - permissões por comando [216](#)
 - privilegios por comando [216](#)
- esquema virtual
 - permissões [198](#)
 - permissões herdadas [198](#)

F

- filtros
 - getUserActivityLog [120](#)
- filtros de pesquisa
 - permissões [188](#)
- fluxo de trabalho
 - permissões [196](#)
 - permissões herdadas [196](#)
- funções
 - Administrador [178](#)
 - atribuindo [181](#)
 - descrição [136](#)
 - gerenciando [177](#)
 - personalizadas [180](#)
 - solução de problemas [183](#)
 - visão geral [107](#)
- funções definidas pelo sistema
 - Administrador [178](#)
 - atribuindo aos usuários e grupos [181](#)
 - descrição [177](#)
- funções personalizadas
 - atribuindo aos usuários e grupos [181](#)
 - criando [180](#)
 - descrição [177](#), [180](#)
 - editando [181](#)
 - excluindo [181](#)
 - Operador [247](#)
 - privilegios, atribuindo [181](#)
 - Serviço Analyst [244](#)
 - Serviço do Metadata Manager [245](#)
 - Serviço do Repositório do PowerCenter [248](#)

G

- Gerenciador de Serviços
 - autorização [104](#)
 - sign-on único [103](#)

- getUserActivityLog
 - filtros [120](#)
 - logs de atividade do usuário [119](#)
- grades
 - permissões [189](#)
- Grupo de privilégio Administração de segurança
 - descrição [137](#)
- Grupo de privilégio da Administração de Nuvem
 - domínio [145](#)
- Grupo de privilégio de administração do domínio
 - descrição [138](#)
- Grupo de privilégio de Objetos em tempo de Execução
 - descrição [160](#)
- Grupo de privilégio de Objetos Globais
 - descrição [164](#)
- Grupo de privilégio Ferramentas
 - domínio [144](#)
 - Serviço do Repositório do PowerCenter [153](#)
- Grupo de privilégio Modelo
 - descrição [150](#)
- Grupo de privilégio Monitoramento
 - domínio [143](#)
- Grupo de privilégio Objetos de Design
 - descrição [155](#)
- Grupo de privilégio Origens e Destinos
 - descrição [158](#)
- Grupo de privilégio Pastas
 - descrição [154](#)
- Grupo de privilégio Procurar
 - descrição [148](#)
- Grupo de privilégio Segurança
 - descrição [150](#)
- Grupo Todos
 - descrição [112](#)
- grupos
 - caracteres inválidos [122](#)
 - definir Todos como padrão [112](#)
 - funções, atribuindo [181](#)
 - gerenciando [122](#)
 - grupo pai [122](#)
 - nome inválido [122](#)
 - privilegios, atribuindo [181](#)
 - sincronização [104](#)
 - visão geral [106](#)
- grupos aninhados
 - autenticação LDAP [28](#)
 - serviço de diretório LDAP [28](#)
- grupos de implantação
 - privilegios para o PowerCenter [164](#)
- grupos de privilégio
 - Administração do Informatica Cloud [145](#)
- Grupos de privilégio
 - descrição [135](#)
- grupos de privilegios
 - Administração de domínio [138](#)
 - Administração de segurança [137](#)
 - Carregar [149](#)
 - Ferramentas [144](#), [153](#)
 - Modelo [150](#)
 - Monitoramento [143](#)
 - Objetos de Design [155](#)
 - Objetos de Tempo de Execução [160](#)
 - Objetos Globais [164](#)
 - Origens e Destinos [158](#)
 - Pastas [154](#)
 - Procurar [148](#)
 - Segurança [150](#)

- Grupos LDAP
 - gerenciando [122](#)
 - importando [23](#)
- grupos nativos
 - adicionando [122](#)
 - editando [123](#)
 - excluindo [124](#)
 - gerenciando [122](#)
 - movendo para outro grupo [124](#)
 - usuários, atribuindo [116](#)
- grupos pai
 - descrição [122](#)

I

- IBM Tivoli Directory Server
 - autenticação LDAP [23](#)
- infacmd isp
 - migrateUsers [33](#)
- Informatica Administrator
 - guias, exibindo [101](#)
 - Navegador [105](#)
 - Página de segurança [105](#)
 - pesquisando [105](#)
 - visão geral [101](#)
- Informatica Analyst
 - administrador [113](#)
- Informatica Developer
 - administrador [113](#)
- ipc
 - permissões por comando [216](#)
 - privilegios por comando [216](#)
- isp
 - permissões por comando [216](#)
 - privilegios por comando [216](#)

L

- licenças
 - permissões [189](#)
- logon único
 - configurando [81](#)
 - visão geral [80](#)
- logs de atividade do usuário
 - convertUserActivityLog [119](#)
 - formatos de saída [119](#)
 - getUserActivityLog [119](#)

M

- mapeamento
 - permissões [196](#)
 - permissões herdadas [196](#)
- memória do sistema
 - aumentando [118](#)
- Metadata Manager
 - administrador [113](#)
- Microsoft Active Directory
 - autenticação LDAP [23](#)
- migrateUsers
 - arquivos de migração do usuário [32](#)
 - infacmd isp [33](#)
- mrs
 - permissões por comando [228](#)
 - privilegios por comando [228](#)

- ms
 - permissões por comando [230](#)
 - privilegios por comando [230](#)

N

- Navegador
 - Página de segurança [105](#)
- nome inválido
 - conta de usuário [115](#)
 - grupos [122](#)
- nós
 - permissões [189](#)
- Novell eDirectory
 - autenticação LDAP [23](#)

O

- objetos de conexão
 - privilegios para o PowerCenter [164](#)
- objetos de design
 - descrição [155](#)
 - privilegios [155](#)
- objetos de domínio
 - permissões [189](#)
- objetos em tempo de execução
 - descrição [160](#)
 - privilegios [160](#)
- objetos globais
 - privilegios para o PowerCenter [164](#)
- oie
 - permissões por comando [231](#)
 - privilegios por comando [231](#)
- OpenLDAP
 - autenticação LDAP [23](#)
- operação do serviço da Web
 - permissões [202](#)
- Operador}
 - funções personalizadas [247](#)
- origens
 - privilegios [158](#)

P

- pacotes de criptografia
 - avancado [69](#)
 - configurando [69](#)
 - Java Cryptography Extension (JCE) [69](#)
- Página de segurança
 - Informatica Administrator [105](#)
 - Navegador [105](#)
- pastas
 - permissões [189](#)
 - privilegios [154](#)
- perfil do sistema operacional
 - criando [128](#)
 - editando [125](#)
 - excluindo [131](#)
 - gerenciando [124](#)
 - padrão [130](#)
 - propriedades, Serviço de Integração de Dados [125](#), [126](#)
 - propriedades, Serviço de Integração do PowerCenter [125](#)
- perfis do sistema operacional
 - permissões [189](#), [192](#)

- permissão direta
 - descrição [187](#)
- permissão efetiva
 - descrição [187](#)
- permissão herdada
 - descrição [187](#)
- permissões
 - aplicativo [196](#)
 - comandos de sql [235](#)
 - comandos dis [214](#)
 - comandos do ipc [216](#)
 - comandos do isp [216](#)
 - comandos mrs [228](#)
 - comandos MS [230](#)
 - comandos oie [231](#)
 - comandos pmcmd [236](#)
 - comandos pmrep [239](#)
 - comandos ps [231](#)
 - comandos pwx [232](#)
 - Comandos rms [233](#)
 - comandos rtm [234](#)
 - comandos wfs [236](#)
 - como comandos [213](#)
 - conexões [194](#)
 - descrição [186](#)
 - diretas [187](#)
 - efetivas [187](#)
 - esquema virtual [198](#)
 - filtros de pesquisa [188](#)
 - fluxo de trabalho [196](#)
 - grades [189](#)
 - herdado [187](#)
 - licenças [189](#)
 - mapeamento [196](#)
 - nós [189](#)
 - objetos de domínio [189](#)
 - operação do serviço da Web [202](#)
 - pastas [189](#)
 - perfis do sistema operacional [189](#), [192](#)
 - procedimento armazenado virtual [198](#)
 - serviço da Web [202](#)
 - serviço de dados SQL [198](#)
 - serviços de aplicativo [189](#)
 - tabela virtual [198](#)
 - tipos [187](#)
 - trabalhando com privilégios [186](#)
- Permissões
 - Comandos es [216](#)
 - Comandos sch [234](#)
- permissões de domínio
 - diretas [187](#)
 - efetivas [187](#)
 - herdado [187](#)
- pmcmd
 - permissões por comando [236](#)
 - privilégios por comando [236](#)
- pmrep
 - permissões por comando [239](#)
 - privilégios por comando [239](#)
- privilégios
 - administração de domínio [138](#)
 - administração de segurança [137](#)
 - Administração do Informatica Cloud [145](#)
 - atribuindo [181](#)
 - comandos de sql [235](#)
 - comandos dis [214](#)
 - comandos do ipc [216](#)
 - comandos do isp [216](#)

- privilégios ()
 - Comandos es [216](#)
 - comandos mrs [228](#)
 - comandos MS [230](#)
 - comandos oie [231](#)
 - comandos pmcmd [236](#)
 - comandos pmrep [239](#)
 - comandos ps [231](#)
 - comandos pwx [232](#)
 - Comandos rms [233](#)
 - comandos rtm [234](#)
 - Comandos sch [234](#)
 - comandos wfs [236](#)
 - como comandos [213](#)
 - Data Integration Service [147](#)
 - descrição [134](#)
 - destinos [158](#)
 - domínio [136](#)
 - ferramentas de domínio [144](#)
 - Ferramentas do serviço de repositório do PowerCenter [153](#)
 - herdado [182](#)
 - monitoramento [143](#)
 - objetos de design [155](#)
 - objetos em tempo de execução [160](#)
 - Objetos globais do PowerCenter [164](#)
 - origens [158](#)
 - pastas [154](#)
 - programas de linha de comando [213](#)
 - Serviço Analyst [145](#)
 - Serviço de Agendador [168](#)
 - Serviço de Repositório do Modelo [151](#)
 - Serviço de Repositório do PowerCenter [152](#)
 - Serviço do Agente de Log do PowerExchange [167](#)
 - Serviço do Gerenciamento de Conteúdo [146](#)
 - Serviço do Metadata Manager [147](#)
 - Serviço do Ouvinte do PowerExchange [167](#)
 - solução de problemas [183](#)
 - trabalhando com permissões [186](#)
- Privilégios do Serviço do Metadata Manager
 - Carregar grupo de privilégio [149](#)
 - Grupo de privilégio Modelo [150](#)
 - Grupo de privilégio Procurar [148](#)
 - Grupo de privilégio Segurança [150](#)
- privilégios herdados
 - descrição [182](#)
- procedimento armazenado virtual
 - permissões [198](#)
 - permissões herdadas [198](#)
- programas de linha de comando
 - privilégios [213](#)
- ps
 - permissões por comando [231](#)
 - privilégios por comando [231](#)
- pwx
 - permissões por comando [232](#)
 - privilégios por comando [232](#)

R

- recurso de serviço da Web
 - permissões [202](#)
- relatórios de auditoria
 - descrição [206](#)
 - para grupos [211](#)
 - para usuários [210](#), [211](#)
- rms
 - permissões por comando [233](#)

- rms ()
 - privilegios por comando [233](#)
- rótulos
 - privilegios para o PowerCenter [164](#)
- rtm
 - permissões por comando [234](#)
 - privilegios por comando [234](#)

S

- sch
 - permissões por comando [234](#)
 - privilegios por comando [234](#)
- Seção Pesquisa
 - Informatica Administrator [105](#)
- Security Assertion Markup Language (SAML)
 - suporte para [80](#)
- segurança
 - funções [136](#)
 - permissões [109](#)
 - privilegios [109](#), [134](#), [137](#)
 - senhas [115](#)
- segurança de nível de coluna
 - restringindo colunas [201](#)
- Segurança do PowerCenter
 - gerenciando [105](#)
- segurança do usuário
 - descrição [102](#)
- senha
 - alterando para uma conta de usuário [108](#)
- senhas
 - alterando para administrador padrão [112](#)
 - requisitos [115](#)
 - usuários nativos [115](#)
- Service Manager
 - autenticação [103](#)
- Serviço Analyst
 - funções personalizadas [244](#)
 - privilegios [145](#)
- serviço da Web
 - permissões [202](#)
 - tipos de permissão [203](#)
- Serviço de Agendador
 - privilegios [168](#)
- serviço de dados SQL
 - permissões [198](#)
 - permissões herdadas [198](#)
 - tipos de permissão [199](#)
- serviço de diretório LDAP
 - conectando ao [23](#)
 - grupos aninhados [28](#)
- Serviço de Integração de Dados
 - autorização [104](#)
- Serviço de Repositório do Modelo
 - autorização [104](#)
 - privilegios [151](#)
 - sincronização de usuário [104](#)
 - usuários com privilegios [183](#)
- Serviço de Repositório do PowerCenter
 - privilegios [152](#)
 - usuários com privilegios [183](#)
- Serviço do Agente de Log do PowerExchange
 - privilegios [167](#)
- Serviço do Gerenciamento de Conteúdo
 - privilegios [146](#)
- Serviço do Metadata Manager
 - autorização [104](#)

- Serviço do Metadata Manager ()
 - funções personalizadas [245](#)
 - privilegios [147](#)
 - sincronização de usuário [104](#)
 - usuários com privilegios [183](#)
- Serviço do Ouvinte do PowerExchange
 - privilegios [167](#)
- Serviço do Repositório do PowerCenter
 - autorização [104](#)
 - Função Administrador [178](#)
 - funções personalizadas [248](#)
 - sincronização de usuário [104](#)
- serviços de aplicativo
 - autorização [104](#)
 - permissões [189](#)
 - sincronização de usuário [104](#)
- Servidor de Diretório Sun Java System
 - autenticação LDAP [23](#)
- sign-on único
 - descrição [103](#)
- sincronização
 - tempos para o serviço de diretório LDAP [27](#)
 - usuários [104](#)
 - Usuários LDAP [23](#)
- sql
 - permissões por comando [235](#)
 - privilegios por comando [235](#)

T

- tabela virtual
 - permissões [198](#)
 - permissões herdadas [198](#)
- Test Data Manager
 - administrador [113](#)

U

- UpdateColumnOptions
 - substituindo valores de colunas [201](#)
- usuários
 - atribuindo a grupos [116](#)
 - caracteres inválidos [115](#)
 - funções, atribuindo [181](#)
 - gerenciando [114](#)
 - grande número de [118](#)
 - memória do sistema [118](#)
 - nome inválido [115](#)
 - privilegios, atribuindo [181](#)
 - sincronização [104](#)
 - visão geral [106](#)
- Usuários LDAP
 - ativando [117](#)
 - atribuindo a grupos [116](#)
 - gerenciando [114](#)
 - importando [23](#)
- usuários nativos
 - adicionando [115](#)
 - ativando [117](#)
 - atribuindo a grupos [116](#)
 - editando [116](#)
 - excluindo [117](#)
 - gerenciando [114](#)
 - senhas [115](#)
- utilitário keytool [28](#)

V

variáveis de ambiente

INFA_TRUSTSTORE [60](#)

INFA_TRUSTSTORE_PASSWORD [60](#)

W

wfs

permissões por comando [236](#)

privilégios por comando [236](#)