



Informatica®

10.1.1

# Guía de seguridad

© Copyright Informatica LLC 2013, 2018

Este software y la documentación se proporcionan exclusivamente en virtud de un acuerdo de licencia independiente que contiene restricciones de uso y divulgación. Ninguna parte de este documento puede ser reproducida o transmitida de cualquier forma o manera (electrónica, fotocopia, grabación o mediante otros métodos) sin el consentimiento previo de Informatica LLC.

Informatica, el logotipo de Informatica, Informatica Cloud, PowerCenter y PowerExchange son marcas comerciales o marcas comerciales registradas de Informatica LLC en los Estados Unidos y en muchas otras jurisdicciones de todo el mundo. La lista actual de marcas comerciales de Informatica está disponible en Internet en <https://www.informatica.com/trademarks.html>. Otros nombres de productos y empresas pueden ser nombres o marcas comerciales de sus respectivos titulares.

Hay fragmentos de este software y/o documentación que están sujetas a copyright perteneciente a terceros, incluido, entre otros: Copyright DataDirect Technologies. Todos los derechos reservados. Copyright © Sun Microsystems. Todos los derechos reservados. Copyright © RSA Security Inc. Todos los derechos reservados. Copyright © Ordinal Technology Corp. Todos los derechos reservados. Copyright © Aandacht c.v. Todos los derechos reservados. Copyright Genivia, Inc. Todos los derechos reservados. Copyright Isomorphic Software. Todos los derechos reservados. Copyright © Meta Integration Technology, Inc. Todos los derechos reservados. Copyright © Intalio. Todos los derechos reservados. Copyright © Oracle. Todos los derechos reservados. Copyright © Adobe Systems Incorporated. Todos los derechos reservados. Copyright © DataArt, Inc. Todos los derechos reservados. Copyright © ComponentSource. Todos los derechos reservados. Copyright © Microsoft Corporation. Todos los derechos reservados. Copyright © Rogue Wave Software, Inc. Todos los derechos reservados. Copyright © Teradata Corporation. Todos los derechos reservados. Copyright © Yahoo! Inc. Todos los derechos reservados. Copyright © Glyph & Cog, LLC. Todos los derechos reservados. Copyright © Thinkmap, Inc. Todos los derechos reservados. Copyright © Clearpace Software Limited. Todos los derechos reservados. Copyright © Information Builders, Inc. Todos los derechos reservados. Copyright © OSS Nokalva, Inc. Todos los derechos reservados. Copyright Edifecs, Inc. Todos los derechos reservados. Copyright Cleo Communications, Inc. Todos los derechos reservados. Copyright © International Organization for Standardization 1986. Todos los derechos reservados. Copyright © ej-technologies GmbH. Todos los derechos reservados. Copyright © Jaspersoft Corporation. Todos los derechos reservados. Copyright © International Business Machines Corporation. Todos los derechos reservados. Copyright © yWorks GmbH. Todos los derechos reservados. Copyright © Lucent Technologies. Todos los derechos reservados. Copyright © University of Toronto. Todos los derechos reservados. Copyright © Daniel Veillard. Todos los derechos reservados. Copyright © Unicode, Inc. Copyright IBM Corp. Todos los derechos reservados. Copyright © MicroQuill Software Publishing, Inc. Todos los derechos reservados. Copyright © PassMark Software Pty Ltd. Todos los derechos reservados. Copyright © LogiXML, Inc. Todos los derechos reservados. Copyright © 2003-2010 Lorenzi Davide. Todos los derechos reservados. Copyright © Red Hat, Inc. Todos los derechos reservados. Copyright © The Board of Trustees of the Leland Stanford Junior University. Todos los derechos reservados. Copyright © EMC Corporation. Todos los derechos reservados. Copyright © Flexera Software. Todos los derechos reservados. Copyright © Jinfonet Software. Todos los derechos reservados. Copyright © Apple Inc. Todos los derechos reservados. Copyright © Telerik Inc. Todos los derechos reservados. Copyright © BEA Systems. Todos los derechos reservados. Copyright © PDFlib GmbH. Todos los derechos reservados. Copyright © Orientation in Objects GmbH. Todos los derechos reservados. Copyright © Tanuki Software, Ltd. Todos los derechos reservados. Copyright © Ricebridge. Todos los derechos reservados. Copyright © Sencha, Inc. Todos los derechos reservados. Copyright © Scalable Systems, Inc. Todos los derechos reservados. Copyright © jQWidgets. Todos los derechos reservados. Copyright © Tableau Software, Inc. Todos los derechos reservados. Copyright © MaxMind, Inc. Todos los derechos reservados. Copyright © TMate Software s.r.o. Todos los derechos reservados. Copyright © MapR Technologies Inc. Todos los derechos reservados. Copyright © Amazon Corporate LLC. Todos los derechos reservados. Copyright © Highsoft. Todos los derechos reservados. Copyright © Python Software Foundation. Todos los derechos reservados. Copyright © BeOpen.com. Todos los derechos reservados. Copyright © CNRI. Todos los derechos reservados.

Este producto incluye software desarrollado por la Apache Software Foundation (<http://www.apache.org/>) y/u otro software protegido por varias versiones de la licencia Apache License ("Licencia"). Puede obtener una copia de estas licencias en <http://www.apache.org/licenses/>. A menos que las leyes aplicables lo requieran o se haya acordado por escrito, el software distribuido bajo estas licencias se distribuye "TAL CUAL", SIN GARANTÍAS NI CONDICIONES DE NINGÚN TIPO, ya sea expresas o implícitas. Consulte las licencias del idioma específico para conocer los permisos y las limitaciones que rigen según las licencias.

Este producto incluye software desarrollado por Mozilla (<http://www.mozilla.org/>), copyright del software de The JBoss Group, LLC, todos los derechos reservados; copyright del software © 1999-2006 de Bruno Lowagie y Paulo Soares y otro software protegido con licencia por el acuerdo GNU Lesser General Public License Agreement, que se puede encontrar en la dirección <http://www.gnu.org/licenses/lgpl.html>. Los materiales se facilitan gratuitamente por parte de Informatica, "tal cual", sin garantía de ningún tipo, ya sea expresa o implícita, incluidas, entre otras, las garantías implícitas de adecuación para un propósito determinado y de validez para el comercio.

El producto incluye software ACE(TM) y TAO(TM) con copyright de Douglas C. Schmidt y su grupo de investigación de la Washington University, University of California, Irvine y Vanderbilt University, Copyright (©) 1993-2006, todos los derechos reservados.

Este producto incluye software desarrollado por el OpenSSL Project para uso en el OpenSSL Toolkit (copyright The OpenSSL Project. Todos los derechos reservados) y la redistribución de este software está sujeta a los términos especificados en <http://www.openssl.org> y <http://www.openssl.org/source/license.html>.

Este producto incluye software Curl con Copyright 1996-2013, Daniel Stenberg, <[daniel@haxx.se](mailto:daniel@haxx.se)>. Todos los derechos reservados. Los permisos y las limitaciones relativos a este software están sujetos a los términos disponibles en la dirección <http://curl.haxx.se/docs/copyright.html>. La autorización para utilizar, copiar, modificar y distribuir este software para cualquier propósito con o sin tasas se concede por el presente, siempre que el aviso de copyright anterior y este aviso de permiso aparezcan en todas las copias.

El producto incluye copyright de software 2001-2005 (©) MetaStuff, Ltd. Todos los derechos reservados. Los permisos y las limitaciones relativos a este software están sujetos a los términos disponibles en la dirección <http://www.dom4j.org/license.html>.

El producto incluye copyright de software © 2004-2007, The Dojo Foundation. Todos los derechos reservados. Los permisos y las limitaciones relativos a este software están sujetos a los términos disponibles en la dirección <http://dojotoolkit.org/license>.

Este producto incluye software ICU con copyright de International Business Machines Corporation y otros. Todos los derechos reservados. Los permisos y las limitaciones relativos a este software están sujetos a los términos disponibles en la dirección <http://source.icu-project.org/repos/icu/icu/trunk/license.html>.

Este producto incluye copyright de software © 1996-2006 Per Bothner. Todos los derechos reservados. Su derecho a utilizar estos materiales está establecido en la licencia que puede encontrarse en la dirección <http://www.gnu.org/software/kawa/Software-License.html>.

Este producto incluye software OSSP UUID con Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Los permisos y las limitaciones relativas a este software están sujetos a los términos disponibles en la dirección <http://www.opensource.org/licenses/mit-license.php>.

Este producto incluye software desarrollado por Boost (<http://www.boost.org/>) o protegido por la licencia de software de Boost. Los permisos y las limitaciones relativos a este software están sujetos a los términos disponibles en la dirección [http://www.boost.org/LICENSE\\_1\\_0.txt](http://www.boost.org/LICENSE_1_0.txt).

Este producto incluye copyright de software © 1997-2007 University of Cambridge. Los permisos y las limitaciones relativos a este software están sujetos a los términos disponibles en la dirección <http://www.pcre.org/license.txt>.

Este producto incluye copyright de software © 2007 The Eclipse Foundation. Todos los derechos reservados. Los permisos y las limitaciones relativos a este software están sujetos a los términos especificados en <http://www.eclipse.org/org/documents/epl-v10.php> y <http://www.eclipse.org/org/documents/edl-v10.php>.

Este producto incluye software protegido por licencia según los términos que aparecen en <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/>

hsqllicense.html, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, [http://www.gzip.org/zlib/zlib\\_license.html](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>, <http://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/licence.html>, <http://www.jgraph.com/jgraphdownload.html>, <http://www.jcraft.com/jsch/LICENSE.txt>, [http://jotm.objectweb.org/bsd\\_license.html](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/licence.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://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>, <https://github.com/documentcloud/underscore-contrib/blob/master/LICENSE> y <https://github.com/apache/hbase/blob/master/LICENSE.txt>.

Este producto incluye software desarrollado por la Academic Free License (<http://www.opensource.org/licenses/afl-3.0.php>), la Common Development and Distribution License (<http://www.opensource.org/licenses/cddl1.php>), la Common Public License (<http://www.opensource.org/licenses/cpl1.0.php>), la Sun Binary Code License Agreement Supplemental License Terms, la BSD License (<http://www.opensource.org/licenses/bsd-license.php>), la nueva BSD License (<http://opensource.org/licenses/BSD-3-Clause>), la MIT License (<http://www.opensource.org/licenses/mit-license.php>), la Artistic License (<http://www.opensource.org/licenses/artistic-license-1.0>) y la Initial Developer's Public License Version 1.0 (<http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/>).

Este producto incluye copyright de software © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. Todos los derechos reservados. Los permisos y las limitaciones relativos a este software están sujetos a los términos disponibles en la dirección <http://xstream.codehaus.org/license.html>. Este producto incluye software desarrollado por Indiana University Extreme! Lab. Para obtener más información, visite <http://www.extreme.indiana.edu/>.

Este producto incluye software Copyright © 2013 Frank Balluffi y Markus Moeller. Todos los derechos reservados. Los permisos y las limitaciones relativas a este software están sujetos a los términos de la licencia MIT.

Consulte las patentes en <https://www.informatica.com/legal/patents.html>.

**EXENCIÓN DE RESPONSABILIDAD:** Informatica LLC proporciona esta documentación "tal cual" sin garantía de ningún tipo, ya sea expresa o implícita, incluidas, entre otras, las garantías implícitas de no incumplimiento, de adecuación para un propósito determinado y de validez para el comercio. Informatica LLC no garantiza que este software o esta documentación estén libres de errores. La información proporcionada en este software o en esta documentación puede contener imprecisiones técnicas o errores tipográficos. La información de este software y esta documentación está sujeta a cambios en cualquier momento sin previo aviso.

#### AVISOS

Este producto de Informatica (el "Software") incluye ciertos controladores (los "Controladores DataDirect") de DataDirect Technologies, una empresa operativa de Progress Software Corporation ("DataDirect") que están sujetos a los términos y condiciones siguientes:

1. LOS CONTROLADORES DATADIRECT SE PROPORCIONAN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, YA SEA EXPRESA O IMPLÍCITA, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE NO INCUMPLIMIENTO, DE ADECUACIÓN PARA UN PROPÓSITO DETERMINADO Y DE VALIDEZ PARA EL COMERCIO.
2. EN NINGÚN CASO DATADIRECT NI SUS PROVEEDORES DE TERCEROS SERÁN RESPONSABLES ANTE EL USUARIO FINAL POR NINGÚN DAÑO DIRECTO, INDIRECTO, FORTUITO, ESPECIAL, CONSECUENTE, NI DE NINGÚN OTRO TIPO, RESULTANTE DEL USO DE LOS CONTROLADORES ODBC, INDEPENDIENTEMENTE DE SI SE HA AVISADO O NO DE LOS POSIBLES DAÑOS POR ADELANTADO. ESTAS LIMITACIONES SE APLICAN A TODAS LAS DEMANDAS JUDICIALES, INCLUIDAS, ENTRE OTRAS, AQUELLAS POR INCUMPLIMIENTO DE CONTRATO, INCUMPLIMIENTO DE LA GARANTÍA, NEGLIGENCIA, RESPONSABILIDAD ESTRUCTIVA, TERGIVERSACIÓN Y OTROS AGRAVIOS.

La información contenida en esta documentación está sujeta a cambios sin previo aviso. Si encuentra algún problema en esta documentación, infórmenos por escrito a Informatica LLC 2100 Seaport Blvd. Redwood City, CA 94063.

INFORMATICA LLC PROPORCIONA LA INFORMACIÓN DE ESTE DOCUMENTO "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, EXPRESA O IMPLÍCITA, INCLUIDAS LAS GARANTÍAS DE COMERCIALIZACIÓN, ADAPTACIÓN A UN FIN PARTICULAR Y CUALQUIER GARANTÍA O CONDICIÓN DE NO INCUMPLIMIENTO.

Fecha de publicación: 2018-06-09

# Tabla de contenido

<b>Prefacio .....</b>	<b>11</b>
Documentación de Informatica .....	11
Informatica Network. ....	11
Base de conocimiento de Informatica. ....	11
Documentación de Informatica .....	11
Matrices de disponibilidad de productos de Informatica. ....	12
Informatica Velocity. ....	12
Catálogo de soluciones de Informatica. ....	12
Servicio internacional de atención al cliente de Informatica. ....	12
 <b>Capítulo 1: Introducción a la seguridad de Informatica.....</b>	<b>13</b>
Resumen de seguridad de Informatica. ....	13
Seguridad de infraestructura. ....	14
Autenticación. ....	14
Comunicación de dominio segura. ....	15
Almacenamiento de datos seguro. ....	16
Seguridad operativa. ....	16
Repositorio de configuración del dominio. ....	16
Dominio de seguridad. ....	17
 <b>Capítulo 2: Autenticación de usuario.....</b>	<b>18</b>
Resumen de la autenticación de usuario. ....	18
Autenticación de usuario nativa. ....	19
Autenticación de usuario de LDAP. ....	19
Autenticación kerberos. ....	20
Inicio de sesión único basado en SAML para aplicaciones web de Informatica. ....	20
 <b>Capítulo 3: Dominios de seguridad de LDAP.....</b>	<b>22</b>
Resumen de los dominios de seguridad de LDAP. ....	22
Configuración de un dominio de seguridad de LDAP. ....	23
Paso 1. Configurar la conexión al servidor de LDAP. ....	23
Paso 2. Configurar un dominio de seguridad. ....	25
Paso 3. Programe las horas de sincronización. ....	27
Uso de grupos anidados en el servicio de directorio de LDAP. ....	28
Uso de un certificado SSL autofirmado. ....	28
Eliminación de un dominio de seguridad LDAP. ....	29
 <b>Capítulo 4: Configuración de la autenticación Kerberos.....</b>	<b>30</b>
Configuración de la autenticación Kerberos Resumen. ....	30
Paso 1. Crear un dominio de usuario de LDAP con usuarios de Microsoft Active Directory. ....	31

Paso 2. Migrar privilegios y permisos de usuarios nativos a un dominio de seguridad de LDAP. . . .	31
Comprobar las cuentas de usuario para autenticación Kerberos. . . . .	32
Crear el archivo de migración de usuario. . . . .	32
Ejecutar el comando infacmd isp migrateUsers. . . . .	33
Solución de problemas del comando migrateUsers. . . . .	34
Comprobar privilegios y permisos de las cuentas de usuario . . . . .	34
Paso 3. Configurar el archivo de configuración de Kerberos. . . . .	35
Paso 4. Generar el formato de nombre principal y de tabla de claves. . . . .	37
Requisitos de principal de servicio a nivel de nodo. . . . .	37
Requisitos de principal de servicio a nivel de proceso. . . . .	38
Ejecutar Informatica Kerberos SPN Format Generator en Windows. . . . .	38
Ejecutar Informatica Kerberos SPN Format Generator en UNIX. . . . .	40
Paso 5. Revisar el archivo de texto de formato de SPN y de tabla de claves. . . . .	41
Paso 6. Crear los archivos de nombres principales de servicio y de tabla de claves. . . . .	43
Solucionar problemas de los nombres principales de servicio y los archivos de tabla de claves. . . . .	44
Paso 7. Configurar la autenticación Kerberos del dominio. . . . .	46
Paso 8. Actualizar los nodos del dominio. . . . .	48
Paso 9. Actualizar los equipos cliente. . . . .	49
Paso 10. Iniciar el dominio de Informatica. . . . .	49
Después de configurar la autenticación Kerberos. . . . .	50
Bibliotecas personalizadas de Kerberos. . . . .	50
Utilizar las bibliotecas personalizadas de Kerberos. . . . .	51
Volver a utilizar las bibliotecas de Kerberos predeterminadas. . . . .	52
<b>Capítulo 5: Seguridad del dominio.....</b>	<b>53</b>
Resumen de la seguridad del dominio. . . . .	53
Comunicación segura dentro del dominio. . . . .	54
Comunicación segura de los servicios y el Administrador de servicios. . . . .	54
Base de datos segura del repositorio de configuración del dominio. . . . .	61
Base de datos segura del repositorio de PowerCenter. . . . .	63
Base de datos segura del repositorio de modelos. . . . .	64
Comunicación segura para flujos de trabajo y sesiones. . . . .	65
Conexiones seguras a un servicio de aplicación web. . . . .	65
Requisitos de las conexiones seguras con servicios de aplicación web. . . . .	66
Habilitar conexiones seguras con la Herramienta del administrador. . . . .	66
Servicios de aplicación web de Informatica. . . . .	67
Conjuntos de cifrado para el dominio de Informatica. . . . .	69
Configurar el dominio de Informatica para utilizar cifrado avanzado. . . . .	69
Creación de las listas de conjuntos de cifrado. . . . .	70
Configuración del dominio de Informatica con una nueva lista efectiva de conjuntos de cifrado. . . . .	70
Orígenes y destinos seguros. . . . .	71

Orígenes y destinos del servicio de integración de datos. . . . .	72
Orígenes y destinos de PowerCenter. . . . .	73
Almacenamiento de datos seguro. . . . .	73
Directorio seguro en UNIX. . . . .	73
Cambiar la clave de cifrado desde la línea de comandos. . . . .	74
Servicios de aplicación y puertos. . . . .	77

## **Capítulo 6: Inicio de sesión único para aplicaciones web de Informatica. .... 80**

Resumen del inicio de sesión único basado en SAML. . . . .	80
Proceso de autenticación del inicio de sesión único basado en SAML. . . . .	80
Experiencia de usuario de las aplicaciones web. . . . .	81
Configuración del inicio de sesión único basado en SAML. . . . .	81
Antes de habilitar el inicio de sesión único. . . . .	82
Paso 1. Crear un dominio de seguridad para las cuentas de usuario de las aplicaciones web. . . . .	82
Paso 2. Exportar el certificado de AD FS. . . . .	86
Paso 3. Importar el certificado al truststore de Informatica. . . . .	88
Paso 4. Configurar los servicios de federación de Active Directory. . . . .	89
Paso 5. Añadir las URL de la aplicación web de Informatica a AD FS. . . . .	96
Paso 6. Habilitar el inicio de sesión único basado en SAML. . . . .	98

## **Capítulo 7: Administración de seguridad en Informatica Administrator. .... 101**

Introducción al uso de Informatica Administrator. . . . .	101
Seguridad del usuario. . . . .	102
Cifrado. . . . .	103
Autenticación. . . . .	103
Autorización. . . . .	104
Ficha Seguridad. . . . .	105
Uso de la sección Buscar. . . . .	105
Uso del navegador de seguridad. . . . .	105
Grupos. . . . .	106
Usuarios. . . . .	107
Funciones. . . . .	107
Gestión de contraseñas. . . . .	108
Modificación de la contraseña. . . . .	108
Administración de seguridad de dominios. . . . .	108
Administración de seguridad del usuario. . . . .	109

## **Capítulo 8: Usuarios y grupos. .... 110**

Resumen de usuarios y gruposUsuarios y grupos . . . . .	110
Grupos predeterminados. . . . .	111
Grupo Administrador. . . . .	111
Grupo Todos. . . . .	112
Grupo Operador. . . . .	112

Descripción de cuentas de usuario. . . . .	112
Administrador predeterminado. . . . .	113
Administrador del dominio. . . . .	113
Administrador de la aplicación cliente. . . . .	113
Usuario. . . . .	114
Administración de usuarios. . . . .	115
Cómo crear usuarios nativos Cómo crear usuariosCómo crear usuarios. . . . .	115
Cómo editar las propiedades generales de usuarios nativos. . . . .	116
Asignar usuarios nativos a grupos nativos. . . . .	116
Asignar usuarios de LDAP a grupos nativos. . . . .	117
Cómo habilitar y deshabilitar cuentas de usuario. . . . .	117
Cómo eliminar usuarios nativos. . . . .	117
Usuarios de LDAP. . . . .	118
Cómo desbloquear una cuenta de usuario. . . . .	118
Cómo aumentar la memoria del sistema para un gran número de usuarios. . . . .	119
Visualización de la actividad del usuario. . . . .	120
Administración de grupos. . . . .	123
Cómo añadir un grupo nativo. . . . .	123
Edición de las propiedades de un grupo nativo. . . . .	124
Movimiento de un grupo nativo a otro. . . . .	124
Cómo eliminar un grupo nativo. . . . .	125
Grupos de LDAP. . . . .	125
Administración de perfiles de sistema operativo. . . . .	125
Propiedades de perfil de sistema operativo para el servicio de integración de PowerCenter . . . . .	125
Propiedades de perfil de sistema operativo para el servicio de integración de datos. . . . .	127
Cómo crear un perfil del sistema operativo. . . . .	129
Editar un perfil de sistema operativo. . . . .	131
Asigne un perfil del sistema operativo predeterminado a un usuario o grupo. . . . .	131
Eliminar un perfil de sistema operativo . . . . .	132
Trabajar con perfiles del sistema operativo en un dominio seguro. . . . .	132
Cómo trabajar con perfiles del sistema operativo en un dominio con autenticación Kerberos. . . . .	132
Bloqueo de cuenta. . . . .	133
Cómo configurar el bloqueo de cuenta. . . . .	134
Reglas y directrices para el bloqueo de cuenta. . . . .	134
<b>Capítulo 9: Privilegios y funciones. . . . .</b>	<b>135</b>
Introducción a los privilegios y funciones. . . . .	135
Privilegios. . . . .	135
Funciones. . . . .	137
Privilegios del dominio. . . . .	138
Grupo de privilegios Administración de seguridad. . . . .	139
Grupo de privilegios Administración de dominios. . . . .	140
Grupo de privilegios Supervisión. . . . .	145

Grupo de privilegios Herramientas. . . . .	146
Grupo de privilegios Administración en la nube. . . . .	146
Privilegios del servicio del analista. . . . .	146
Privilegios del servicio de administración de contenido. . . . .	148
Privilegios del servicio de integración de datos.. . . .	148
Privilegios del servicio de Metadata Manager. . . . .	149
Grupo de privilegios Catálogo. . . . .	149
Grupo de privilegios Carga. . . . .	151
Grupo de privilegios Modelo. . . . .	152
Grupo de privilegios Seguridad. . . . .	152
Privilegios del Servicio de repositorio de modelos. . . . .	152
Privilegios del servicio de repositorio de PowerCenter. . . . .	154
Grupo de privilegios Herramientas. . . . .	155
Grupo de privilegios Carpetas. . . . .	156
Grupo de privilegios Objetos de diseño. . . . .	158
Grupo de privilegios Orígenes y destinos. . . . .	160
Grupo de privilegios Objetos de tiempo de ejecución. . . . .	162
Grupo de privilegios Objetos globales. . . . .	166
Privilegios del Servicio de escucha PowerExchange. . . . .	169
Privilegios del Servicio de registrador PowerExchange. . . . .	169
Privilegios del servicio de programador. . . . .	170
Privilegios del servicio de Test Data Manager. . . . .	171
Grupo de privilegios Administración. . . . .	172
Grupo de privilegios Conexiones. . . . .	173
Grupo de privilegios Dominios de datos. . . . .	173
Grupo de privilegios Enmascaramiento de datos. . . . .	174
Grupo de privilegios Subconjunto de datos. . . . .	175
Grupo de privilegios Directivas. . . . .	176
Grupo de privilegios Proyectos. . . . .	177
Grupo de privilegios Reglas. . . . .	179
Grupo de privilegios Generación de datos. . . . .	180
Cómo administrar funciones. . . . .	180
Funciones definidas por el sistema. . . . .	181
Funciones personalizadas. . . . .	184
Cómo asignar privilegios y funciones a usuarios y grupos. . . . .	185
Privilegios heredados. . . . .	186
Asignación de privilegios y funciones a un usuario o grupo mediante navegación. . . . .	186
Visualización de usuarios con privilegios para un servicio. . . . .	187
Solucionar problemas de privilegios y funciones. . . . .	187
<b>Capítulo 10: Permisos.....</b>	<b>190</b>
Resumen de permisos. . . . .	190
Tipos de permisos. . . . .	191



Filtros de búsqueda para el trabajo con permisos. . . . .	192
Permisos del objeto de dominio. . . . .	193
Permisos por objeto de dominio. . . . .	194
Permisos por usuario o grupo. . . . .	195
Permisos de perfil de sistema operativo. . . . .	196
Permisos de conexión. . . . .	198
Tipos de permisos de conexión. . . . .	198
Permisos de conexión predeterminados. . . . .	199
Cómo asignar permisos sobre una conexión. . . . .	199
Visualización de detalles de permiso en una conexión. . . . .	199
Edición de permisos en una conexión. . . . .	200
Permisos de aplicación y de objeto de aplicación. . . . .	200
Tipos de permisos de aplicación y de objeto de aplicación. . . . .	200
Asignar permisos en una aplicación u objeto de aplicación. . . . .	201
Visualizar los detalles del permiso sobre una aplicación u objeto de aplicación. . . . .	201
Editar permisos sobre una aplicación u objeto de aplicación. . . . .	202
Denegar permisos sobre una aplicación u objeto de aplicación. . . . .	202
Permisos del servicio de datos SQL. . . . .	202
Tipos de permiso del servicio de datos SQL. . . . .	203
Asignación de permisos en un servicio de datos SQL. . . . .	203
Visualización de detalles de permisos en un servicio de datos SQL. . . . .	204
Edición de permisos en un servicio de datos SQL. . . . .	204
Denegación de permisos en un servicio de datos SQL. . . . .	205
Seguridad de nivel de columna. . . . .	205
Permisos del servicio web. . . . .	207
Tipos de permiso para los servicios web. . . . .	207
Asignación de permisos en un servicio web. . . . .	208
Visualización de detalles de permiso en un servicio web. . . . .	208
Edición de permisos en un servicio web. . . . .	209
<b>Capítulo 11: Informes de auditoría. . . . .</b>	<b>210</b>
Resumen de informes de auditoría. . . . .	210
Información personal del usuario. . . . .	211
Asociación de grupos de usuarios. . . . .	211
Privilegios. . . . .	213
Asociación de funciones. . . . .	213
Permiso del objeto de dominio. . . . .	214
Seleccionar usuarios para un informe de auditoría. . . . .	214
Seleccionar grupos para un informe de auditoría. . . . .	215
Seleccionar funciones para un informe de auditoría. . . . .	215
<b>Apéndice A: Permisos y privilegios de la línea de comandos. . . . .</b>	<b>217</b>
Comandos de infacmd as. . . . .	217

Comandos infacmd dis. . . . .	218
comandos infacmd es. . . . .	220
Comandos infacmd ipc. . . . .	220
Comandos infacmd isp. . . . .	220
Comandos infacmd mrs. . . . .	232
Comandos infacmd ms. . . . .	235
Comandos infacmd oie. . . . .	235
Comandos infacmd ps. . . . .	235
Comandos infacmd pwx. . . . .	236
Comandos infacmd rms. . . . .	237
Comandos infacmd rtm. . . . .	238
Comandos infacmd sch. . . . .	238
Comandos infacmd sql. . . . .	239
Comandos infacmd wfs. . . . .	240
Comandos pmcmd. . . . .	240
Comandos pmrep. . . . .	243
<b>Apéndice B: Funciones personalizadas. . . . .</b>	<b>249</b>
Función personalizada del Servicio del analista. . . . .	249
Funciones personalizadas del Servicio de Metadata Manager. . . . .	250
Función personalizada del operador. . . . .	252
Funciones personalizadas del Servicio de repositorio de PowerCenter. . . . .	253
Funciones personalizadas de Test Data Manager. . . . .	254
<b>Apéndice C: Lista predeterminada de conjuntos de cifrado. . . . .</b>	<b>260</b>
<b>Índice. . . . .</b>	<b>262</b>

# Prefacio

La Guía de seguridad de Informatica contiene información sobre la seguridad en el dominio de Informatica. Contiene la información que necesita para administrar la seguridad del dominio de Informatica y los clientes de Informatica que se conectan al dominio. Este libro da por hecho que conoce el dominio de Informatica e Informatica Administrator. También se da por sentado que está familiarizado con los servidores y procesos de autenticación para su red.

## Documentación de Informatica

### Informatica Network

Informatica Network incluye el servicio internacional de atención al cliente de Informatica, la base de conocimiento de Informatica y otros recursos de producto. Para acceder a Informatica Network, visite <https://network.informatica.com>.

Un miembro puede:

- Acceder a todos sus recursos de Informatica en un solo lugar.
- Busque recursos de producto, como documentación, preguntas frecuentes y mejores prácticas en la base de conocimiento.
- Vea la información de disponibilidad del producto.
- Revisar los casos de asistencia.
- Buscar su red de grupos de usuarios de Informatica locales y colaborar con sus iguales.

### Base de conocimiento de Informatica

Utilice la base de conocimiento de Informatica para buscar recursos de producto como documentación, artículos de procedimientos, mejores prácticas y PAM en la red de Informatica.

Para acceder a la base de conocimiento, visite <https://kb.informatica.com>. Si tiene preguntas, comentarios o ideas relacionadas con la base de conocimiento de Informatica, póngase en contacto con el equipo de la base de conocimiento de Informatica en [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).

### Documentación de Informatica

Para obtener la documentación más reciente del producto, consulte la base de conocimiento de Informatica en [https://kb.informatica.com/\\_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx](https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx).

Si tiene preguntas, comentarios o ideas relacionadas con esta documentación, póngase en contacto con el equipo de documentación de Informatica enviando un correo electrónico a [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

## Matrices de disponibilidad de productos de Informatica

Las matrices de disponibilidad de producto (PAM, Product Availability Matrixes) indican las versiones de sistemas operativos, bases de datos y otros tipos de orígenes de datos y destinos admitidos por una versión de un producto. Si es miembro de la red de Informatica, puede acceder a las PAM en <https://network.informatica.com/community/informatica-network/product-availability-matrices>.

## Informatica Velocity

Informatica Velocity es un conjunto de sugerencias y mejores prácticas desarrollado por los servicios profesionales de Informatica. Desarrollado a partir de la experiencia real de cientos de proyectos de administración de datos, Informatica Velocity representa el conocimiento conjunto de nuestros asesores, los cuales han trabajado con organizaciones de todo el mundo para planificar, desarrollar, implementar y mantener con éxito soluciones de administración de datos.

Si es miembro de la red de Informatica, puede acceder a los recursos de Informatica Velocity en <http://velocity.informatica.com>.

Si tiene alguna pregunta, comentario o idea acerca de Informatica Velocity, póngase en contacto con los servicios Profesionales de Informatica en [ips@informatica.com](mailto:ips@informatica.com).

## Catálogo de soluciones de Informatica

El Catálogo de soluciones de Informatica es un foro donde puede buscar soluciones que aumenten, amplíen o mejoren sus implementaciones de Informatica. Al aprovechar cualquiera de los cientos de soluciones de los desarrolladores y los socios de Informatica, puede mejorar la productividad y acelerar el tiempo de implementación en los proyectos. Puede acceder al Catálogo de soluciones de Informatica en <https://marketplace.informatica.com>.

## Servicio internacional de atención al cliente de Informatica

Puede ponerse en contacto con un centro de atención global por teléfono o a través del soporte en línea en la red de Informatica.

Para encontrar el número de teléfono local del servicio internacional de atención al cliente de Informatica, visite el sitio web de Informatica en el siguiente vínculo:

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

Si es miembro de la red de Informatica, puede utilizar el soporte en línea en <http://network.informatica.com>.

# CAPÍTULO 1

## Introducción a la seguridad de Informatica

Este capítulo incluye los siguientes temas:

- [Resumen de seguridad de Informatica, 13](#)
- [Seguridad de infraestructura, 14](#)
- [Seguridad operativa, 16](#)
- [Repositorio de configuración del dominio, 16](#)
- [Dominio de seguridad, 17](#)

## Resumen de seguridad de Informatica

Es posible asegurar el dominio de Informatica para protegerlo de amenazas tanto internas como externas a la red en la que se ejecuta el dominio.

La seguridad del dominio de Informatica incluye los siguientes tipos de seguridad:

### **Seguridad de infraestructura**

La seguridad de infraestructura protege el dominio de Informatica frente al acceso no autorizado o la modificación de servicios y recursos del dominio de Informatica. La seguridad de la infraestructura incluye los siguientes aspectos:

- La protección de los datos que se transmiten y se almacenan dentro del dominio de Informatica
- La autenticación de los usuarios y los servicios que se conectan al dominio de Informatica
- La seguridad de las conexiones para componentes externos, incluidas las aplicaciones cliente y las bases de datos relacionales para repositorios, orígenes y destinos.

### **Seguridad operativa**

La seguridad operativa controla el acceso a los datos y los servicios en el dominio de Informatica. La seguridad operativa incluye los siguientes aspectos:

- La configuración de restricciones al acceso del usuario a datos y metadatos basadas en la función del usuario en la organización
- La configuración de restricciones a la capacidad del usuario para realizar operaciones dentro del dominio de Informatica basadas en la función del usuario en la organización

Informatica almacena la información de configuración del dominio y la lista de usuarios autorizados a acceder al dominio en el repositorio de configuración del dominio. El repositorio de configuración del

dominio también contiene los grupos, las funciones, los privilegios y los permisos que se asignan a cada usuario en el dominio de Informatica.

Informatica organiza la lista de usuarios en función de los dominios de seguridad. Un dominio de seguridad contiene un conjunto de cuentas de usuario. Un dominio puede tener varios dominios de seguridad.

## Seguridad de infraestructura

La seguridad de infraestructura incluye la autenticación de usuario y servicio, la comunicación segura en el dominio y el almacenamiento de datos seguro.

### Autenticación

El administrador de servicios autentica los servicios que se ejecutan en el dominio y los usuarios que inician sesión en las herramientas cliente de Informatica.

Puede configurar el dominio de Informatica para utilizar los siguientes tipos de autenticación:

#### **Autenticación nativa**

La autenticación nativa es un modo de autenticación disponible solo para las cuentas de usuario del dominio de Informatica. Cuando el dominio de Informatica utiliza la autenticación nativa, el administrador de servicios almacena las credenciales y los privilegios de usuario en el repositorio de configuración del dominio y realiza toda la autenticación de usuarios en el dominio de Informatica.

Si el dominio de Informatica utiliza la autenticación nativa de manera predeterminada, el dominio tiene un dominio de seguridad nativo y todas las cuentas de usuario pertenecen al dominio de seguridad nativo.

Informatica utiliza el nombre de usuario y las contraseñas para autenticar a los usuarios y servicios en el dominio de Informatica.

#### **Autenticación de protocolo ligero de acceso a directorios (LDAP)**

LDAP es un protocolo de software para acceder a los usuarios y los recursos de una red. Si el dominio de Informatica utiliza la autenticación de LDAP, las cuentas de usuario y las credenciales se almacenan en el servicio de directorio de LDAP. Los privilegios y los permisos del usuario se almacenan en el repositorio de configuración del dominio. Debe sincronizar periódicamente las cuentas de usuario del repositorio de configuración del dominio con las cuentas de usuario del servicio de directorio de LDAP.

Informatica utiliza el nombre de usuario y las contraseñas para autenticar a los usuarios y servicios de Informatica en el dominio de Informatica.

#### **Autenticación Kerberos**

Kerberos es un protocolo de autenticación de red que utiliza vales para autenticar a los usuarios y los servicios de una red. Cuando el dominio de Informatica utiliza la autenticación Kerberos, las cuentas de usuario y las credenciales se almacenan en la base de datos principal de Kerberos, que puede ser un servicio de directorio de LDAP. Los privilegios y los permisos del usuario se almacenan en el repositorio de configuración del dominio. Debe sincronizar periódicamente las cuentas de usuario del repositorio de configuración del dominio con las cuentas de usuario de la base de datos principal de Kerberos.

Informatica utiliza vales de Kerberos para autenticar a los usuarios y servicios de Informatica en el dominio de Informatica.

### Inicio de sesión único basado en SAML

El lenguaje de marcado de aserción de seguridad (SAML) es un formato de datos basado en XML para el intercambio de información de autenticación y autorización entre un proveedor de servicios y un proveedor de identidad. Puede configurar el inicio de sesión único basado en SAML para las aplicaciones web de la Herramienta del administrador, la Herramienta del analista y la Herramienta de supervisión.

En un dominio de Informatica, la aplicación web de Informatica es el proveedor de servicios y los servicios de federación de Microsoft Active Directory (AD FS) son el proveedor de identidad. Las cuentas y las credenciales de los usuarios de las aplicaciones web de Informatica se almacenan en Microsoft Active Directory. Se importan las cuentas de Active Directory a un dominio de seguridad dentro del dominio de Informatica. Periódicamente, debe sincronizar las cuentas de usuario en el dominio de seguridad con las cuentas de usuario en el servicio de directorio de Active Directory.

Tenga en cuenta que no puede habilitar el inicio de sesión único basado en SAML en un dominio de Informatica configurado para utilizar la autenticación Kerberos.

## Comunicación de dominio segura

El dominio de Informatica tiene varias opciones para asegurar los datos y metadatos que se transmiten entre el administrador de servicios y los servicios del dominio y las aplicaciones cliente. Informatica utiliza los protocolos TCP/IP y HTTP para comunicarse entre los componentes del dominio y utiliza certificados SSL para asegurar la comunicación entre los servicios y el administrador de servicios del dominio.

El protocolo SSL o TLS utiliza criptografía de claves públicas para cifrar y descifrar el tráfico de red. La clave pública utilizada para cifrar y descifrar el tráfico se almacena en un certificado SSL que puede ser autofirmado o firmado. Un certificado autofirmado está firmado por el creador del certificado. Dado que la identidad del firmante no se comprueba, un certificado autofirmado es menos seguro que un certificado firmado. Un certificado firmado es un certificado SSL que contiene la identidad de la persona que solicita el certificado verificada por una autoridad de certificación (CA). Informatica recomienda usar certificados firmados por una CA para un mayor nivel de seguridad.

Un almacén de claves contiene claves privadas y certificados. Se utiliza para proporcionar una credencial. Un truststore contiene el certificado de servidores SSL o TLS de confianza. Se utiliza para comprobar una credencial.

Para proteger conexiones en el dominio, Informatica requiere almacenes de claves y truststores con formato PEM y JKS. Puede utilizar los siguientes programas para crear los archivos necesarios:

#### **keytool**

Utilice keytool para crear un certificado SSL o una solicitud de firma de certificado (CSR), así como almacenes de claves y truststores con formato JKS.

Si desea más información sobre keytool, consulte la documentación en el siguiente sitio web:

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

#### **OpenSSL**

Puede utilizar OpenSSL para crear un certificado SSL o CSR, así como para convertir un almacén de claves en formato JKS a PEM.

Si desea más información sobre OpenSSL, consulte la documentación en el siguiente sitio web:

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

El tipo de conexión que se protege determina los archivos necesarios.

## Almacenamiento de datos seguro

Informatica cifra los datos confidenciales, como las contraseñas y los parámetros de conexión segura, antes de almacenar los datos en el repositorio de configuración del dominio. Informatica también guarda los archivos confidenciales, como los archivos de configuración, en un directorio seguro.

## Seguridad operativa

Puede asignar privilegios, funciones y permisos a usuarios o grupos de usuarios para administrar el nivel de acceso que los usuarios y grupos pueden tener y el ámbito de las acciones que los usuarios y grupos pueden realizar en el dominio.

Puede utilizar los siguientes métodos para administrar el acceso del usuario y grupo en el dominio:

### Privilegios

Los privilegios determinan las acciones que los usuarios pueden realizar en las herramientas cliente de Informatica. Puede asignar un conjunto de privilegios a un usuario para restringir el acceso a los servicios disponibles en el dominio. También puede asignar privilegios a un grupo para permitir que todos los usuarios del grupo tengan el mismo acceso a los servicios.

### Funciones

Una función es un conjunto de privilegios que se pueden asignar a usuarios o grupos. Puede utilizar funciones para administrar con mayor facilidad las asignaciones de privilegios a los usuarios. Puede crear una función con privilegios limitados y asignarla a los usuarios y grupos que tengan restringido el acceso a los servicios del dominio. O puede crear funciones con privilegios relacionados para asignarlos a los usuarios y grupos que necesiten el mismo nivel de acceso.

### Permisos

Los permisos definen el nivel de acceso que los usuarios tienen a un objeto. Un usuario que tenga el privilegio para poder realizar una determinada acción puede necesitar permiso para realizar la acción en un objeto concreto. Por ejemplo, para administrar un servicio de aplicaciones, un usuario debe tener el privilegio para administrar servicios y el permiso en el servicio de aplicación específico.

### El grupo Administrador predeterminado

El dominio de Informatica tiene un grupo Administrador definido por el sistema que incluye todos los privilegios y permisos de un servicio. Cualquier cuenta de usuario que añada al grupo Administrador tiene privilegios y permisos en todos los servicios y objetos del dominio. Al instalar los servicios de Informatica, el programa de instalación crea una cuenta de usuario que pertenece al grupo Administrador. Es posible usar la cuenta Administrador predeterminada para iniciar sesión en la herramienta Administrador de manera provisional.

## Repositorio de configuración del dominio

El repositorio de configuración del dominio contiene información sobre la configuración del dominio y los privilegios y permisos del usuario.

Si el dominio de Informatica utiliza la autenticación de usuario nativa, el repositorio de configuración del dominio también contendrá las credenciales de usuario. Si el dominio utiliza la autenticación de LDAP o



Kerberos, el repositorio de configuración del dominio no contendrá las credenciales de usuario. Todas las credenciales de usuario de LDAP y Kerberos se almacenan fuera del dominio de Informatica, en el servicio de directorio de LDAP o en la base de datos principal de Kerberos.

Al crear el dominio de Informatica durante la instalación, el programa de instalación crea un repositorio de configuración del dominio en una base de datos relacional. Debe especificar la base de datos en la que se va a crear el repositorio de configuración del dominio. Puede crear el repositorio en una base de datos protegida con el protocolo SSL.

## Dominio de seguridad

Un dominio de seguridad es un conjunto de cuentas de usuario y grupos del dominio de Informatica.

El dominio de Informatica puede tener los siguientes tipos de dominios de seguridad:

### **Dominio de seguridad nativo**

El dominio de seguridad nativo contiene los usuarios y grupos creados y administrados en la herramienta Administrator. Informatica almacena todas las credenciales de cuentas de usuario en el dominio de seguridad nativo, en el repositorio de configuración del dominio. De forma predeterminada, el dominio de seguridad nativo se crea durante la instalación. Tras la instalación, no puede crear más dominios de seguridad nativos ni eliminar el dominio de seguridad nativo.

Si el dominio de Informatica utiliza la autenticación Kerberos, el dominio utiliza el dominio de seguridad nativo.

### **Dominio de seguridad de LDAP**

Un dominio de seguridad de LDAP contiene usuarios y grupos importados desde un servicio de directorio de LDAP. Si el dominio de Informatica utiliza la autenticación de LDAP o Kerberos, se puede crear un dominio de seguridad de LDAP y añadir usuarios y grupos que se importen desde el servicio de directorio de LDAP.

Al instalar los servicios de Informatica y crear un dominio que utilice la autenticación nativa o de LDAP, el programa de instalación crea el dominio de seguridad nativo, pero no crea un dominio de seguridad de LDAP. Puede crear dominios de seguridad de LDAP tras la instalación.

Al instalar los servicios de Informatica y crear un dominio que utilice la autenticación Kerberos, el programa de instalación crea los siguientes dominios de seguridad de LDAP:

- Dominio de seguridad interno. El programa de instalación crea un dominio de seguridad de LDAP con el nombre `_infalInternalNamespace`. El dominio de seguridad `_infalInternalNamespace` contiene la cuenta de usuario Administrador predeterminada que creó durante la instalación. Tras la instalación, no puede añadir usuarios al dominio de seguridad `_infalInternalNamespace` ni eliminar el dominio de seguridad.
- Dominio de seguridad del dominio de usuario. El programa de instalación crea un dominio de seguridad de LDAP vacío con el mismo nombre que el del dominio Kerberos que especificó durante la instalación. Tras la instalación, se pueden importar usuarios desde la base de datos principal de Kerberos en el dominio de seguridad del dominio de usuario. No puede eliminar el dominio de seguridad del dominio de usuario.  
Cuando ejecute los programas de la línea de comandos en un dominio que utiliza la autenticación Kerberos. El valor predeterminado de la opción del dominio de seguridad es el del dominio de usuario creado durante la instalación.

Los dominios de seguridad de LDAP se pueden crear y administrar del mismo modo, tanto si el dominio de Informatica utiliza la autenticación de LDAP como la autenticación Kerberos.

## CAPÍTULO 2

# Autenticación de usuario

Este capítulo incluye los siguientes temas:

- [Resumen de la autenticación de usuario, 18](#)
- [Autenticación de usuario nativa, 19](#)
- [Autenticación de usuario de LDAP, 19](#)
- [Autenticación kerberos, 20](#)
- [Inicio de sesión único basado en SAML para aplicaciones web de Informatica, 20](#)

## Resumen de la autenticación de usuario

La autenticación de usuario en el dominio de Informatica depende del tipo de autenticación que configure al instalar los servicios de Informatica.

El dominio de Informatica puede utilizar los siguientes tipos de autenticación para autenticar a los usuarios del dominio de Informatica:

- Autenticación de usuario nativa
- Autenticación de usuario de LDAP
- Autenticación de red de Kerberos
- Inicio de sesión único basado en el lenguaje de marcado de aserción de seguridad (SAML)

Las cuentas de usuario nativas se almacenan en el dominio de Informatica y solo se pueden utilizar dentro de este.

LDAP, Kerberos y las cuentas de usuario se almacenan en un servicio de directorio de LDAP y se comparten con las aplicaciones de la empresa.

El inicio de sesión único basado en SAML autentica a los usuarios confrontando sus credenciales con las de las cuentas almacenadas en Microsoft Active Directory. Las cuentas se importan de Active Directory a un dominio de seguridad dentro del dominio de Informatica.

Puede seleccionar el tipo de autenticación que se va a utilizar en el dominio de Informatica durante la instalación. Si habilita la autenticación Kerberos durante la instalación, debe configurar el dominio de Informatica para trabajar con el centro de distribución de claves (KDC) Kerberos. Debe crear los nombres principales del servicio (SPN) que necesita el dominio de Informatica en la base de datos principal de Kerberos. La base de datos principal de Kerberos puede ser un servicio de directorio de LDAP. También debe crear archivos de tabla de claves para los SPN y almacenarlos en el directorio de Informatica según requiera el dominio de Informatica.

Si no habilita la autenticación Kerberos durante la instalación, el programa de instalación configura el dominio de Informatica para que utilice la autenticación nativa. Tras la instalación, puede configurar una conexión a un servidor de LDAP y configurar el dominio de Informatica para que utilice la autenticación de LDAP, además de la autenticación nativa.

La autenticación nativa y la autenticación de LDAP se pueden utilizar a la vez en el dominio de Informatica. El Administrador de servicios autentica a los usuarios en función de su dominio de seguridad. Si un usuario pertenece al dominio de seguridad nativo, el Administrador de servicios autentica al usuario en el repositorio de configuración del dominio. Si el usuario pertenece a un dominio de seguridad de LDAP, el Administrador de servicios pasa el nombre de usuario y la contraseña al servidor de LDAP autenticarlos.

No es posible usar la autenticación nativa con la autenticación Kerberos. Si el dominio de Informatica utiliza autenticación Kerberos, todas las cuentas de usuario deben estar en dominios de seguridad de LDAP. El servidor de Kerberos autentica una cuenta de usuario cuando el usuario inicia sesión en la red. Las aplicaciones cliente de Informatica utilizan las credenciales del inicio de sesión de red para autenticar a los usuarios en el dominio de Informatica. Las funciones y los grupos nativos siguen siendo compatibles.

Puede habilitar el inicio de sesión único basado en SAML para las aplicaciones web de Informatica durante o después de la instalación. Sin embargo, debe completar todas las tareas de configuración requeridas antes de habilitar el inicio de sesión único basado en SAML. No puede habilitar el inicio de sesión único basado en SAML en un dominio de Informatica configurado para utilizar la autenticación Kerberos.

## Autenticación de usuario nativa

Si el dominio de Informatica utiliza la autenticación nativa, el administrador de servicios almacena toda la información de cuentas de usuario y realiza la autenticación de todos los usuarios en el dominio de Informatica. Cuando un usuario inicia sesión, el administrador de servicios utiliza el dominio de seguridad nativo para autenticar el nombre de usuario y la contraseña.

Si no configura el dominio de Informatica para que utilice la autenticación de red de Kerberos, el dominio de Informatica contiene un dominio de seguridad nativo de forma predeterminada. Éste se crea en el momento de la instalación y no se puede eliminar. Un dominio de Informatica sólo puede contar con un dominio de seguridad nativo. Las cuentas de usuario del dominio de seguridad nativo se crean y se mantienen en la herramienta Administrator. El administrador de servicios almacena los detalles de las cuentas de usuario, incluidos los privilegios y las credenciales de usuario, en el repositorio de configuración del dominio.

## Autenticación de usuario de LDAP

Puede configurar el dominio de Informatica para que los usuarios de un servicio de directorio de LDAP puedan iniciar sesión en las aplicaciones cliente de Informatica. El dominio de Informatica puede utilizar la autenticación de usuario de LDAP, además de la autenticación de usuario nativa.

Para habilitar el dominio de Informatica para utilizar la autenticación de usuario de LDAP, debe configurar una conexión con un servidor de LDAP y especificar, desde el servicio de directorio de LDAP, especificar los usuarios y grupos que pueden tener acceso al dominio de Informatica. Puede utilizar la herramienta Administrador para configurar la conexión con el servidor de LDAP.

Al sincronizar los dominios de seguridad de LDAP con el servicio de directorio de LDAP, el administrador de servicios importa la lista de las cuentas de usuario de LDAP con acceso al dominio de Informatica a los dominios de seguridad de LDAP. Al asignar privilegios y permisos a los usuarios de los dominios de

seguridad de LDAP, el administrador de servicios almacena la información en el repositorio de configuración del dominio. El administrador de servicios no almacena las credenciales de usuario en el repositorio de configuración del dominio.

Cuando un usuario inicia sesión, el administrador de servicios pasa el nombre de usuario y la contraseña al servidor de LDAP para autenticarlos.

**Nota:** El administrador de servicios requiere que los usuarios de LDAP inicien sesión en una aplicación cliente con una contraseña, incluso si un servicio de directorio de LDAP puede permitir una contraseña en blanco en el modo de inicio de sesión anónimo.

## Autenticación kerberos

Puede configurar el dominio de Informatica para que utilice autenticación de red Kerberos para autenticar usuarios y servicios en una red.

La autenticación Kerberos es un protocolo de red que utiliza tickets para autenticar el acceso a los servicios y a los nodos de una red. Kerberos utiliza un Centro de distribución de claves (KDC) para validar las identidades de usuarios y servicios y para conceder tickets a las cuentas de usuarios y servicios autenticadas. En el protocolo de Kerberos, los usuarios y los servicios se conocen como principales. El KDC tiene una base de datos de principales y sus claves secretas asociadas que se utilizan como prueba de identidad. Kerberos puede utilizar un servicio de directorio de LDAP como una base de datos principal.

Para utilizar la autenticación Kerberos, debe instalar y ejecutar el dominio de Informatica en una red que utilice la autenticación de red de Kerberos. Informatica se puede ejecutar en una red que utilice la autenticación Kerberos y el servicio de Microsoft Active Directory como la base de datos principal.

Informatica no admite la autenticación Kerberos con varios dominios. El host del servidor, los equipos cliente y el servidor de autenticación Kerberos deben estar en el mismo dominio.

El dominio de Informatica requiere archivos de tabla de claves para autenticar nodos y servicios en el dominio sin transmitir contraseñas a través de la red. Los archivos de tabla de claves contienen los nombres principales de servicio (SPN) y claves cifradas asociadas. Cree los archivos de tabla de claves antes de crear nodos y servicios en el dominio de Informatica.

## Inicio de sesión único basado en SAML para aplicaciones web de Informatica

Puede configurar un dominio de Informatica para permitir a los usuarios utilizar el inicio de sesión único (SSO) basado en SAML para iniciar sesión en las aplicaciones web de la Herramienta del administrador, la Herramienta del analista y la Herramienta de supervisión.

El lenguaje de marcado de aserción de seguridad (SAML) es un formato de datos basado en XML para el intercambio de información de autenticación y autorización entre un proveedor de servicios y un proveedor de identidad. En un dominio de Informatica, la aplicación web de Informatica es el proveedor de servicios. Los servicios de federación de Microsoft Active Directory (AD FS) 2.0. son el proveedor de identidad, que autentican a los usuarios de aplicaciones web con el almacén de identidades de Active Directory de la organización.

Para permitir que el dominio de Informatica utilice el inicio de sesión único basado en SAML, debe crear un dominio de seguridad de LDAP para las cuentas de usuario de la aplicación web de Informatica y, a continuación, importar los usuarios al dominio desde Active Directory. Puede utilizar la Herramienta de administrador para configurar la conexión al servidor de Active Directory y, a continuación, importar los usuarios al dominio de seguridad.

Cuando un usuario inicia sesión en una aplicación web de Informatica, la aplicación envía una solicitud de autenticación SAML para AD FS. AD FS autentica las credenciales del usuario comparándolas con la información de la cuenta del usuario en Active Directory y, a continuación, devuelve a la aplicación web un token de aserción de SAML que contiene información relacionada con la seguridad sobre el usuario.

Se configura AD FS para emitir tokens de SAML que se utilizan para autenticar a los usuarios de las aplicaciones web de Informatica. También debe exportar el certificado de firma de la aserción del proveedor de identidad de AD FS y, a continuación, importarlo al archivo de truststore predeterminado de Informatica en cada nodo de puerta de enlace del dominio.

## CAPÍTULO 3

# Dominios de seguridad de LDAP

Este capítulo incluye los siguientes temas:

- [Resumen de los dominios de seguridad de LDAP, 22](#)
- [Configuración de un dominio de seguridad de LDAP, 23](#)
- [Eliminación de un dominio de seguridad LDAP, 29](#)

## Resumen de los dominios de seguridad de LDAP

Un dominio de seguridad de LDAP contiene un conjunto de usuarios y grupos importados desde un servicio de directorio de LDAP. Debe crear un dominio de seguridad de LDAP si se utiliza la autenticación de usuario de LDAP o la autenticación de red Kerberos.

Configure los dominios de seguridad de LDAP para almacenar la lista de usuarios de un servicio de directorio LDAP para el que desee permitir el acceso al dominio y las aplicaciones cliente de Informatica. El dominio de seguridad de LDAP no almacena las credenciales de la cuenta de usuario. Cuando un usuario inicia sesión en un cliente de Informatica, el administrador de servicios verifica que la cuenta de usuario esté en un dominio de seguridad. Si la cuenta de usuario pertenece a un dominio de seguridad de LDAP, el administrador de servicios autentica el usuario con el servicio de directorio de LDAP.

Si instala los servicios de Informatica y no habilita la autenticación Kerberos, el programa de instalación de Informatica crea el dominio de seguridad nativo de forma predeterminada. Tras la instalación, se pueden añadir usuarios y grupos al dominio de seguridad nativo. Si en un servicio de directorio de LDAP hay usuarios a los que desea dar acceso a aplicaciones cliente de Informatica, puede configurar dominios de seguridad de LDAP además del dominio de seguridad nativo. Configure una conexión con el servidor de LDAP e importe los usuarios y grupos a los dominios de seguridad de LDAP.

Al instalar los servicios de Informatica y habilitar la autenticación Kerberos, el programa de instalación de Informatica crea un dominio de seguridad de LDAP con el nombre del dominio Kerberos que se especifique durante la instalación. Tras la instalación, puede configurar una conexión con el servidor de LDAP e importar los usuarios y grupos desde el servicio de directorio de LDAP al dominio de seguridad de LDAP. Si utiliza la autenticación Kerberos, no se puede usar el dominio de seguridad nativo.

# Configuración de un dominio de seguridad de LDAP

Puede crear un dominio de seguridad de LDAP para las cuentas de usuario que importe desde un servicio de directorio de LDAP. Para organizar diferentes grupos de usuarios, puede crear varios dominios de seguridad de LDAP.

La creación y administración de los usuarios y grupos de LDAP se realiza en el servicio de directorio de LDAP. Configure una conexión con el servidor de LDAP y utilice filtros de búsqueda para especificar los usuarios y grupos que pueden acceder al dominio de Informatica. A continuación, importe las cuentas de usuario en los dominios de seguridad de LDAP. Si el servidor de LDAP utiliza un protocolo SSL, también debe especificar la ubicación del certificado de SSL.

Los usuarios se pueden importar desde los siguientes servicios de directorio de LDAP:

- IBM Tivoli Directory Server
- Microsoft Active Directory

**Nota:** Si utiliza la autenticación Kerberos, solo puede importar usuarios de Microsoft Active Directory.

- Novell eDirectory
- OpenLDAP
- Sun Java System Directory Server

Después de importar usuarios en un dominio de seguridad de LDAP, se pueden asignar funciones, privilegios y permisos a los usuarios. Puede asignar cuentas de usuario de LDAP a grupos nativos para organizarlas según sus funciones en el dominio de Informatica.

No se puede utilizar la Herramienta del administrador para crear, editar o eliminar usuarios ni grupos en un dominio de seguridad de LDAP. Los cambios en los usuarios y grupos de LDAP se deben realizar en el servicio de directorio de LDAP y, a continuación, sincronizar el dominio de seguridad de LDAP con el servicio de directorio de LDAP.

Utilice el cuadro de diálogo Configuración de LDAP para establecer la conexión con el servicio de directorio de LDAP y crear el dominio de seguridad de LDAP. También puede utilizar el cuadro de diálogo Configuración de LDAP para configurar un programa de sincronización.

Para configurar el dominio de seguridad de LDAP, realice los pasos siguientes:

1. Configure la conexión al servidor de directorio de LDAP.
2. Configure un dominio de seguridad.
3. Programe las horas de sincronización.

## Paso 1. Configurar la conexión al servidor de LDAP

Configure la conexión al servidor de LDAP que contiene el servicio de directorio desde el que desea importar las cuentas de usuario para el dominio de Informatica.

Al configurar la conexión al servidor de LDAP, indique que el administrador de servicios debe omitir la distinción entre mayúsculas y minúsculas en los atributos del nombre distintivo de las cuentas de usuario de LDAP cuando se asignan usuarios a grupos en el dominio de Informatica. Si el administrador de servicios no omite la distinción entre mayúsculas y minúsculas, es posible que no asigne todos los usuarios que pertenecen a un grupo.

Si el servidor de LDAP utiliza SSL, debe importar el certificado al archivo de truststore `cacerts` en cada nodo de puerta de enlace del dominio de Informatica. Consulte ["Uso de un certificado SSL autofirmado" en la página 28](#) para obtener información detallada.

Para configurar una conexión al servicio de directorio de LDAP, realice las tareas siguientes:

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Haga clic en el menú **Acciones** y seleccione **Configuración de LDAP**.
3. En el cuadro de diálogo **Configuración de LDAP**, haga clic en la ficha **Conectividad de LDAP**.
4. Configure las propiedades de conexión del servidor de LDAP.

Es posible que tenga que ponerse en contacto con el administrador de LDAP para obtener información relativa al servidor de LDAP.

La siguiente tabla describe las propiedades de configuración del servidor de LDAP:

Propiedad	Descripción
Nombre del servidor	Nombre de host o dirección IP del equipo que hospeda el servicio de directorio de LDAP.
puerto	El puerto de escucha del servidor de LDAP. Es el número de puerto para comunicarse con el servicio de directorio de LDAP. Por lo general, el número de puerto del servidor de LDAP es 389. Si el servidor de LDAP utiliza SSL, el número de puerto del servidor de LDAP es 636. El número máximo de puerto es 65535.
Servicio de directorio de LDAP	Tipo de servicio de directorio LDAP. Seleccione uno de los siguientes servicios de directorio: <b>Nota:</b> Si utiliza la autenticación Kerberos, debe seleccionar Microsoft Active Directory.
Nombre	Nombre distintivo (DN) para el usuario principal. El nombre de usuario suele estar formado por un nombre común (CN), un nombre de organización (O) y un país (C). El nombre de usuario principal es un usuario administrativo que tiene acceso al directorio. Especifique un usuario que tenga permiso para leer otras entradas de usuario en el servicio de directorio de LDAP. Deje esta propiedad en blanco si el usuario que inicia la sesión es anónimo. Si desea más información, consulte la documentación del servicio de directorio de LDAP.
Contraseña	La contraseña del usuario principal. Deje esta propiedad en blanco si el usuario que inicia la sesión es anónimo. No disponible si utiliza la autenticación Kerberos.
Usar certificado SSL	Indica que el servidor de LDAP utiliza el protocolo de capa de conexión segura (SSL).
Confiar en certificado LDAP	Determina si el administrador de servicios puede confiar en el certificado SSL del servidor de LDAP. Si selecciona esta propiedad, el administrador de servicios se conecta con el servidor de LDAP sin verificar el certificado SSL. Si no la selecciona, el administrador de servicios comprueba que el certificado SSL esté firmado por una entidad certificadora antes de conectarse con el servidor de LDAP.  Para habilitar el administrador de servicios para que reconozca un certificado autofirmado como válido, especifique el archivo truststore y la contraseña que se debe usar.
No distingue entre mayúsculas y minúsculas	Indica que el Administrador de servicios no debe distinguir entre mayúsculas y minúsculas para los atributos de nombre distinguido al asignar usuarios a grupos. Habilite esta opción.



Propiedad	Descripción
Atributo de pertenencia a grupos	Nombre del atributo que contiene información de pertenencia a grupos para un usuario. Es el atributo del objeto de grupo de LDAP que contiene los DN de los usuarios y grupos que son miembros de un grupo. Por ejemplo, <i>member</i> o <i>memberof</i> .
Tamaño máximo	Número máximo de cuentas de usuario que se importan a un dominio de seguridad. Por ejemplo, si el valor se ha definido en 100, puede importar un máximo de 100 cuentas de usuario en el dominio de seguridad.  Si el número de usuarios para importar excede el valor de esta propiedad, el administrador de servicios genera un mensaje de error y no importa ningún usuario. Defina esta propiedad en un valor más alto si tiene muchos usuarios para importar. El valor predeterminado es 1000.

- Haga clic en Probar conexión para verificar que la conexión al servidor de LDAP sea válida.

## Paso 2. Configurar un dominio de seguridad

Debe crear un dominio de seguridad para cada conjunto de cuentas de usuario y grupos que desee importar desde el servidor de directorio de LDAP. Defina bases de búsqueda y filtros para definir el conjunto de cuentas de usuario y grupos que se deben incluir en un dominio de seguridad. El administrador de servicios usa los filtros y las bases de búsqueda de usuarios para importar las cuentas de usuario y los filtros y las bases de búsqueda de grupos para importar grupos. El administrador de servicios importa los grupos y la lista de usuarios que pertenecen a los grupos en cuestión. Importa los grupos incluidos en el filtro de grupos y las cuentas de usuario incluidas en el filtro de usuarios.

Los nombres de los usuarios y los grupos que se deben importar desde el servicio de directorio de LDAP deben seguir las mismas reglas que los nombres de los usuarios y grupos nativos. El administrador de servicios no importa usuarios o grupos de LDAP si los nombres no siguen estas reglas.

**Nota:** A diferencia de lo que ocurre con los nombres de usuarios nativos, los nombres de usuarios LDAP distinguen entre mayúsculas y minúsculas.

Cuando configure el servicio de directorio de LDAP, puede usar diferentes atributos para el ID único (UID, por sus siglas en inglés). El administrador de servicios requiere un determinado UID para identificar a los usuarios en cada servicio de directorio de LDAP. Antes de configurar el dominio de seguridad, compruebe que el servicio de directorio de LDAP use el UID requerido.

En la siguiente tabla se enumera el UID necesario para cada servicio de directorio de LDAP:

Servicio de directorio de LDAP	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Novell eDirectory	uid
OpenLDAP	uid
Sun Java System Directory Server	uid

El administrador de servicios no importa el atributo de LDAP que indica que una cuenta de usuario está habilitada o deshabilitada. Debe habilitar o deshabilitar una cuenta de usuario de LDAP en Administrator

Tool. El estado de la cuenta de usuario en el servicio de directorio de LDAP influye en la autenticación del usuario en las aplicaciones cliente. Una cuenta de usuario, por ejemplo, puede estar habilitada en el dominio de Informática pero deshabilitada en el servicio de directorio de LDAP. Si el servicio de directorio de LDAP permite a las cuentas de usuario deshabilitadas iniciar sesión, el usuario puede iniciar sesión en las aplicaciones cliente. Si el servicio de directorio de LDAP no permite a las cuentas de usuario deshabilitadas iniciar sesión, el usuario no puede iniciar sesión en las aplicaciones cliente.

**Nota:** Si modifica las propiedades de conexión de LDAP para que se conecte a un servidor de LDAP diferente, el administrador de servicio no elimina los dominios de seguridad existentes. Debe asegurarse de que los dominios de seguridad de LDAP sean correctos para el nuevo servidor de LDAP. Modifique los filtros de usuario y grupo de los dominios de seguridad o cree otros dominios de seguridad de modo que el administrador de servicios importe correctamente los usuarios y grupos que desee utilizar en el dominio de Informática.

Para configurar un dominio de seguridad de LDAP, realice los pasos siguientes:

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Haga clic en el menú **Acciones** y seleccione **Configuración de LDAP**.
3. En el cuadro de diálogo **Configuración de LDAP**, haga clic en la ficha **Dominios de seguridad**.
4. Haga clic en **Añadir**.
5. Use la sintaxis de consulta de LDAP para crear filtros que permitan especificar los usuarios y grupos que se deben incluir en el dominio de seguridad que está creando.

Es posible que tenga que ponerse en contacto con el administrador de LDAP para obtener la información relativa a los usuarios y grupos disponibles en el servicio de directorio de LDAP.

La siguiente tabla describe las propiedades de filtro que se pueden definir para un dominio de seguridad:

Propiedad	Descripción
Dominio de seguridad	Nombre del dominio de seguridad de LDAP. La distinción entre mayúsculas y minúsculas no se aplica a este nombre, el cual debe ser único dentro del dominio. No puede exceder 128 caracteres ni incluir los siguientes caracteres especiales: , + / < > @ ; \ % ? El nombre puede contener un carácter de espacio ASCII, menos en el primer y último carácter. Los otros caracteres de espacio no están permitidos.
Base de búsqueda de usuarios	El nombre distinguido (DN) de la entrada que sirve de punto de inicio para buscar nombres de usuario en el servicio de directorio de LDAP. La búsqueda encuentra un objeto en el directorio de acuerdo con la ruta del nombre distinguido del objeto. Por ejemplo, en Microsoft Active Directory, el nombre distinguido de un objeto de usuario puede ser cn=UserName,ou=OrganizationalUnit,dc=DomainName, donde la serie de nombres distinguidos relativos que denota dc=DomainName identifica el dominio DNS del objeto.
Filtro de usuarios	Una cadena de consulta de LDAP que especifica los criterios para buscar usuarios en el servicio de directorio. El filtro puede especificar tipos de atributo, valores de aserción y criterios coincidentes. Por ejemplo: (objectClass=*) busca todos los objetos. (&(objectClass=user)(!(cn=susan))) busca todos los objetos de usuario excepto "susan". Si desea más información sobre los filtros de búsqueda, consulte la documentación del servicio de directorio de LDAP.

Propiedad	Descripción
Base de búsqueda de grupos	El nombre distinguido (DN) de la entrada que sirve de punto de inicio para buscar nombres de grupo en el servicio de directorio de LDAP.
Filtro de grupos	Una cadena de consulta de LDAP que especifica los criterios para buscar grupos en el servicio de directorio.

6. Haga clic en **Vista previa** para ver un subconjunto de la lista de usuarios y grupos que se hallan dentro de los parámetros del filtro.  
Si la vista previa no muestra el conjunto correcto de usuarios y grupos, modifique los filtros de usuario y grupo y busque en las bases para obtener los usuarios y grupos correctos.
7. Para añadir otro dominio de seguridad de LDAP, repita los pasos del [4](#) al [6](#).
8. Para sincronizar inmediatamente los usuarios y grupos de los dominios de seguridad con los del servicio de directorio de LDAP, haga clic en **Sincronizar ahora**.  
El administrador de servicios sincroniza los usuarios de todos los dominios de seguridad de LDAP con los usuarios del servicio de directorio de LDAP. El tiempo que tarda el proceso de sincronización en completarse depende del número de usuarios y grupos que se deben importar.
9. Haga clic en **Aceptar** para guardar los dominios de seguridad.

### Paso 3. Programe las horas de sincronización

Mediante la configuración de un programa, el administrador de servicios puede sincronizar periódicamente la lista de usuarios y grupos del dominio de seguridad de LDAP con la lista de usuarios y grupos del servicio de directorio de LDAP.

**Importante:** Antes de iniciar el proceso de sincronización, compruebe que el archivo `/etc/hosts` contiene una entrada para el nombre de host del servidor de LDAP. Si el Administrador de servicios no puede resolver el nombre de host del servidor de LDAP, la sincronización de usuarios podría generar un error.

Durante la sincronización, el administrador de servicios importa los usuarios y grupos desde el servicio de directorio de LDAP. El administrador de servicios elimina cualquier usuario o grupo desde el dominio de seguridad de LDAP que ya no esté incluido en los filtros de búsqueda utilizados para la importación.

De forma predeterminada, el administrador de servicios no tiene una hora programada para la sincronización con el servicio de directorio de LDAP. Para asegurarse de que la lista de usuarios y grupos de los dominios de seguridad de LDAP sea precisa, puede programar las horas del día a las que quiera que el administrador de servicios sincronice los dominios de seguridad de LDAP. El administrador de servicios sincroniza los dominios de seguridad de LDAP con el servicio de directorio de LDAP todos los días a las horas que establezca.

**Nota:** Durante la sincronización, el administrador de servicios bloquea la cuenta de usuario que sincroniza. Cuando la cuenta de usuario está bloqueada, el administrador de servicios no puede autenticar la cuenta de usuario. Por ello, es posible que los usuarios no puedan iniciar sesión en las aplicaciones cliente. Posiblemente, los usuarios que estén conectados a los clientes de aplicación cuando comience la sincronización no puedan realizar tareas. La duración de la sincronización varía en función del número de usuarios y grupos objeto del proceso. Para evitar interrupciones, se recomienda sincronizar los dominios de seguridad en períodos de baja actividad de los usuarios. Para sincronizar más de 100 usuarios o grupos, habilite la paginación en el servicio de directorio de LDAP antes de ejecutar la sincronización. Si no habilita la paginación en el servicio de directorio de LDAP, la sincronización puede fallar.

Para programar la sincronización de los dominios de seguridad de LDAP con el servicio de directorio de LDAP, realice los pasos siguientes:

1. En la herramienta Administrator, haga clic en la ficha **Seguridad**.
2. Haga clic en el menú **Acciones** y seleccione **Configuración de LDAP**.
3. En el cuadro de diálogo **Configuración de LDAP**, haga clic en la ficha **Programar**.
4. Haga clic en el botón **Añadir (+)** para añadir una hora.

El programa de sincronización utiliza un formato de 24 horas.

Puede añadir tantas horas de sincronización como necesite. Si la lista de usuarios y grupos del servicio de directorio de LDAP cambia con frecuencia, sería conveniente programar el administrador de servicios para que realice la sincronización en distintos puntos del día.

5. Para sincronizar inmediatamente los usuarios y grupos de los dominios de seguridad con los del servicio de directorio de LDAP, haga clic en **Sincronizar ahora**.
6. Haga clic en **Aceptar** para guardar el programa de sincronización.

**Nota:** Si reinicia el dominio de Informatica antes de que el administrador de servicios se sincronice con el servicio de directorio de LDAP, se perderán las horas de sincronización que ha añadido.

## Uso de grupos anidados en el servicio de directorio de LDAP

Un dominio de seguridad de LDAP puede contener grupos de LDAP anidados. El administrador de servicios puede importar grupos anidados que se hayan creado de la siguiente forma:

- Cree los grupos que se hallen bajo las mismas unidades organizativas (UO).
- Defina la relación entre los grupos.

Desea crear, por ejemplo, una agrupación anidada en la que el GrupoB pertenezca al GrupoA y el GrupoD, al GrupoC.

1. Cree el GrupoA, el GrupoB, el GrupoC y el GrupoD dentro de la misma unidad organizativa.
2. Edite el GrupoA y añada el GrupoB como un miembro.
3. Edite el GrupoC y añada el GrupoD como un miembro.

No puede importar grupos de LDAP anidados a un dominio de seguridad de LDAP que se haya creado de diferente forma.

## Uso de un certificado SSL autofirmado

Puede conectarse con un servidor de LDAP que utilice un certificado SSL firmado por una entidad emisora de certificados (CA). Como valor predeterminado, el administrador de servicios no se conecta con un servidor de LDAP que use un certificado autofirmado.

Para conectarse a un servidor de LDAP que utiliza un certificado SSL, utilice la herramienta de administración de claves y certificados Java keytool para importar el certificado al archivo de truststore `cacerts` en cada nodo de puerta de enlace del dominio. El archivo de truststore `cacerts` se encuentra en el directorio siguiente de cada nodo:

```
<directorio de instalación de Informatica>\java\jre\lib\security
```

La utilidad keytool se encuentra en el directorio siguiente de cada nodo:

```
<directorio de instalación de Informatica>\java\jre\bin
```

Reinicie el nodo después de importar el certificado.

# Eliminación de un dominio de seguridad LDAP

Para impedir que los usuarios de un dominio de seguridad LDAP accedan a las aplicaciones cliente de forma permanente, puede eliminar el dominio de seguridad LDAP. Cuando elimine un dominio de seguridad LDAP, el administrador de servicios eliminará todos los grupos y cuentas de usuario del dominio de seguridad LDAP de la base de datos de configuración del dominio.

1. En el cuadro de diálogo Configuración de LDAP, haga clic en la ficha **Dominios de seguridad**.  
El cuadro de diálogo de configuración de LDAP mostrará la lista de dominios de seguridad.
2. Para asegurarse de que elimina el dominio de seguridad correcto, haga clic en el nombre del dominio de seguridad para ver el filtro utilizado para importar los usuarios y grupos y compruebe que sea el dominio de seguridad que desee eliminar.
3. Haga clic en el botón **Eliminar** junto a un dominio de seguridad para eliminarlo.
4. Haga clic en **Aceptar** para confirmar que desea eliminar el dominio de seguridad.

## CAPÍTULO 4

# Configuración de la autenticación Kerberos

Este capítulo incluye los siguientes temas:

- [Configuración de la autenticación Kerberos Resumen, 30](#)
- [Paso 1. Crear un dominio de usuario de LDAP con usuarios de Microsoft Active Directory, 31](#)
- [Paso 2. Migrar privilegios y permisos de usuarios nativos a un dominio de seguridad de LDAP, 31](#)
- [Paso 3. Configurar el archivo de configuración de Kerberos, 35](#)
- [Paso 4. Generar el formato de nombre principal y de tabla de claves, 37](#)
- [Paso 5. Revisar el archivo de texto de formato de SPN y de tabla de claves, 41](#)
- [Paso 6. Crear los archivos de nombres principales de servicio y de tabla de claves, 43](#)
- [Paso 7. Configurar la autenticación Kerberos del dominio, 46](#)
- [Paso 8. Actualizar los nodos del dominio, 48](#)
- [Paso 9. Actualizar los equipos cliente, 49](#)
- [Paso 10. Iniciar el dominio de Informatica, 49](#)
- [Después de configurar la autenticación Kerberos, 50](#)
- [Bibliotecas personalizadas de Kerberos, 50](#)

## Configuración de la autenticación Kerberos Resumen

Cuando cree el dominio de Informatica durante la instalación, puede seleccionar la opción para habilitar la autenticación Kerberos. Si no habilita la autenticación Kerberos durante la instalación, puede utilizar los programas de la línea de comandos de Informatica para configurar el dominio para utilizar la autenticación Kerberos.

Para configurar la autenticación Kerberos del dominio de Informatica en la línea de comandos, realice los siguientes pasos:

1. Cree un dominio de usuario de LDAP con usuarios de Microsoft Active Directory.
2. Migre usuarios nativos a un dominio de seguridad de LDAP.
3. Configure los ajustes de Kerberos y copie el archivo de configuración en el directorio de Informatica.
4. Genere el SPN y el archivo de tabla de claves con el formato requerido por el dominio de Informatica.
5. Revise el archivo de texto con el formato del SPN y el archivo de tabla de claves.

6. Cree los SPN y los archivos de tabla de claves.
7. Configure la autenticación Kerberos del dominio de Informatica.
8. Actualice los nodos del dominio de Informatica.
9. Actualice los equipos cliente.
10. Inicie el dominio de Informatica y ejecute la Herramienta del administrador.

Después de configurar la autenticación Kerberos y los dominios de seguridad de LDAP, compruebe que las cuentas de usuario tienen los privilegios y los permisos correctos. Compruebe que los servicios del dominio rinden como se esperaba y que los usuarios pueden iniciar sesión con inicio de sesión único.

**Nota:** Los pasos que se indican se basan en el supuesto de que ha instalado los servicios de Informatica sin habilitar la autenticación Kerberos. Si ha habilitado la autenticación Kerberos durante la instalación, siga los pasos de las guías de instalación de Informatica.

## Paso 1. Crear un dominio de usuario de LDAP con usuarios de Microsoft Active Directory

Antes de configurar el dominio de Informatica para utilizar la autenticación Kerberos, compruebe que todas las cuentas de usuario se encuentren en dominios de seguridad de LDAP dentro del dominio de Informatica. Las cuentas de usuario se deben importar a un dominio de seguridad de LDAP desde Microsoft Active Directory.

Si el dominio de Informatica tiene cuentas de usuario en un dominio de seguridad de LDAP que no utiliza Microsoft Active Directory, migre los usuarios a Microsoft Active Directory. Para obtener más información sobre la migración de cuentas de usuario a Microsoft Active Directory, consulte la documentación de su implementación de LDAP.

Si el dominio tiene cuentas de usuario en el dominio de seguridad nativo, migre los usuarios a Microsoft Active Directory. Configure un dominio de seguridad de LDAP y configure la conexión al servicio de Microsoft Active Directory. A continuación, configure filtros para los usuarios y grupos y sincronice las cuentas de usuario en Microsoft Active Directory con las cuentas de usuario en el dominio de seguridad de LDAP.

Para obtener más información sobre la configuración de un dominio de LDAP y la sincronización de las cuentas de usuario, consulte [“Configuración de un dominio de seguridad de LDAP” en la página 23](#)

## Paso 2. Migrar privilegios y permisos de usuarios nativos a un dominio de seguridad de LDAP

Si el dominio de Informatica tiene cuentas de usuario en el dominio de seguridad nativo, migre todos los grupos de usuarios, las funciones, los privilegios y los permisos para las cuentas a las correspondientes cuentas de usuario en un dominio de seguridad de LDAP. Tras configurar el dominio de Informatica para utilizar autenticación Kerberos, no podrá modificar las cuentas de usuario en el dominio de seguridad nativo.

Si el dominio tiene cuentas de usuario en el dominio de seguridad nativo, las correspondientes cuentas de usuario de Active Directory en el dominio de seguridad de LDAP deben tener los mismos grupos, funciones, privilegios y permisos. Migre los grupos, las funciones, los privilegios y los permisos de los usuarios nativos

a los usuarios del dominio de seguridad de LDAP. A continuación, compruebe que la migración de los grupos, las funciones, los privilegios y los permisos se ha realizado correctamente.

Si el dominio no contiene cuentas de usuario en el dominio de seguridad nativo, continúe con ["Paso 3. Configurar el archivo de configuración de Kerberos" en la página 35.](#)

Para migrar los grupos, las funciones, los privilegios y los permisos de usuarios nativos a los usuarios del dominio de seguridad de LDAP, realice los siguientes pasos:

1. Compruebe las cuentas de usuario para la autenticación Kerberos.
2. Cree el archivo de migración de usuario.
3. Ejecute el comando `infacmd isp migrateusers`.
4. Compruebe los grupos, las funciones, los privilegios y los permisos de las cuentas de usuario.

**Nota:** Para evitar que ocurran problemas durante la migración de las funciones, los privilegios y los permisos de los grupos de usuarios, absténgase de ejecutar flujos de trabajo o de modificar los grupos de usuarios, las funciones, los privilegios o los permisos durante el proceso de migración.

## Comprobar las cuentas de usuario para autenticación Kerberos

Consulte la lista de cuentas de usuario nativas y determine las cuentas que desea migrar a un dominio de seguridad de LDAP para autenticación Kerberos.

Para enumerar las cuentas de usuario del dominio de Informática, ejecute el siguiente comando:

```
infacmd isp ListAllUsers
```

Cada cuenta de usuario nativa que desee migrar al dominio de seguridad de LDAP debe contar con una cuenta correspondiente en el servicio Microsoft Active Directory que se utiliza para la autenticación Kerberos.

Si las cuentas no existen en el servicio de Microsoft Active Directory, añada las cuentas de usuario al servicio de directorios. Para obtener más información sobre cómo añadir las cuentas de usuario al servicio de Microsoft Active Directory, consulte la documentación de Microsoft Active Directory.

**Nota:** El nombre de usuario de las cuentas de usuario del dominio de seguridad de LDAP tiene una longitud máxima de 20 caracteres. Al añadir las cuentas de usuario al servicio de Microsoft Active Directory, asegúrese de que la longitud del nombre de usuario no exceda los 20 caracteres.

## Crear el archivo de migración de usuario

El comando `infacmd isp migrateUsers` utiliza un archivo de migración de usuario para determinar los grupos, las funciones, los privilegios y los permisos que se asignarán a los usuarios de LDAP. El archivo de migración de usuario es un archivo de texto sin formato que contiene la lista de usuarios nativos y de usuarios de LDAP correspondientes que deben tener los mismos grupos, funciones, privilegios y permisos.

Al crear el archivo de migración de usuario, debe especificar el dominio de seguridad de la cuenta de usuario. Una barra diagonal (/) separa el dominio de seguridad del nombre de usuario. Una coma (,) separa el usuario nativo del usuario de LDAP correspondiente. Los dominios de seguridad distinguen mayúsculas de minúsculas. En cambio, los nombres de usuario no distinguen mayúsculas de minúsculas.

Utilice el siguiente formato para enumerar las entradas en el archivo de migración de usuario:

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



Puede migrar los grupos, las funciones, los privilegios y los permisos de los usuarios nativos a los usuarios de diferentes dominios de seguridad de LDAP. Por ejemplo, si el archivo de migración de usuario contiene la siguiente lista de usuarios:

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

El comando `migrateUser` asigna a User1 y User2 de LDAPSecurityDomain los mismos grupos, funciones, privilegios y permisos de User1 y User2 en el dominio de seguridad nativo. El comando asigna a User3 de newLDAPSecDomain los mismos grupos, funciones, privilegios y permisos de User3 en el dominio de seguridad nativo.

El comando `migrateUsers` omite las entradas con nombres de usuario de origen o de destino duplicados.

## Ejecutar el comando `infacmd isp migrateUsers`

Para migrar los grupos, las funciones, los privilegios y los permisos de los usuarios del dominio de seguridad nativo a los usuarios del dominio de seguridad de LDAP, ejecute el comando `infacmd migrateUsers` y especifique el archivo de migración de usuarios que se debe utilizar.

Antes de que ejecute el comando `infacmd isp migrateUsers`, asegúrese de que todas las instancias de los siguientes servicios se están ejecutando en el dominio:

- Servicio del analista
- Servicio de administración de contenido
- Servicio de repositorio de modelos
- Servicio de Metadata Manager
- Servicio de repositorio de PowerCenter®

Asegúrese de que el servicio de repositorio de PowerCenter se está ejecutando en modo normal.

Para migrar los grupos, las funciones, los privilegios y los permisos de los usuarios, ejecute el siguiente comando:

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

Por ejemplo, el siguiente comando migra los grupos, las funciones, los privilegios y los permisos de usuarios con base en el archivo de migración de usuarios `um_s.txt`:

```
infacmd isp migrateUsers -dn UMT_Domain -un Administrator -pd Administrator -umf C:\UMT
\um_s.txt
```

El comando sobrescribe los permisos del objeto de conexión que se han asignado al usuario de LDAP con los permisos del objeto de conexión del usuario nativo. El comando fusiona los grupos, las funciones, los privilegios y los permisos del objeto de dominio de los usuarios nativos y los usuarios de LDAP correspondientes.

El comando `migrateUsers` crea un archivo de registro detallado llamado `infacmd_uml_<date>_<time>.txt` en el directorio en el que se ejecuta el comando.

Para obtener más información sobre el comando, consulte *Referencia de comando de Informatica*.

## Solución de problemas del comando migrateUsers

### ¿Cómo se puede mejorar el rendimiento de la migración?

Para mejorar el rendimiento de la migración, realice los pasos siguientes:

1. Cree varios archivos únicos de migración de usuario con una cantidad limitada de usuarios en cada archivo.
2. Ejecute varias instancias del comando migrateUsers al mismo tiempo.

Por ejemplo, para migrar los grupos, las funciones, los privilegios y los permisos de 150 usuarios, puede crear tres archivos de migración de usuario con 50 usuarios cada uno. A continuación, ejecute tres instancias del comando migrateUsers de manera simultánea. Especifique un único archivo de migración de usuarios para cada instancia del comando.

### El comando migrateUsers genera un error.

Si el comando migrateUsers genera un error, están disponibles las siguientes rutas de acceso de recuperación:

- Ejecute el comando migrateUsers de nuevo.
- Modifique el archivo de migración de usuarios. A continuación, ejecute el comando migrateUsers.

Cuando ejecute de nuevo el comando, especifique el mismo archivo de migración de usuarios. El comando sobrescribe los permisos del objeto de conexión que se han asignado al usuario de LDAP con los permisos del objeto de conexión del usuario nativo. El comando fusiona los grupos, las funciones, los privilegios y los permisos del objeto de dominio de los usuarios nativos y los usuarios de LDAP correspondientes.

Para modificar el archivo de migración de usuarios, realice los pasos siguientes:

1. Vea el archivo de registro detallado que se ha creado al ejecutar el comando migrateUsers.
2. Elimine los usuarios que el comando migró correctamente desde el archivo de migración de usuarios.
3. Ejecute el comando migrateUsers.

## Comprobar privilegios y permisos de las cuentas de usuario

Antes de habilitar la autenticación Kerberos, debe comprobar que los usuarios del dominio de seguridad de LDAP tengan los grupos, las funciones, los privilegios y los permisos correctos. Puede usar el comando infacmd para comprobar los grupos, las funciones, los privilegios y los permisos de las cuentas de usuario del dominio de seguridad de LDAP.

Compruebe que los siguientes objetos se han migrado correctamente:

### Usuarios y grupos

Para determinar los grupos a los que pertenecen las cuentas de usuario, obtenga una lista de los usuarios y los grupos asociados. Ejecute el siguiente comando:

```
infacmd aud getUserGroupAssociation
```

### Funciones

Para obtener la lista de funciones asociadas a los usuarios y grupos del dominio, ejecute el siguiente comando:

```
infacmd aud getUserGroupAssociationForRoles
```

### Privilegios

Para obtener una lista de los privilegios asignados a los usuarios y grupos del dominio, ejecute el siguiente comando:

```
infacmd aud getPrivilegeAssociation
```

### Permisos

Para obtener una lista de los permisos asignados a los usuarios y grupos del dominio, ejecute el siguiente comando:

```
infacmd aud getDomainObjectPermissions
```

### Permisos de carpetas y objetos globales

Si el dominio contiene un servicio de repositorio de PowerCenter, compruebe los permisos de las carpetas y los objetos de repositorio global de PowerCenter que se han asignado a las cuentas de usuario. El repositorio de PowerCenter puede tener los siguientes objetos:

- Carpetas
- Grupos de implementación
- Etiquetas
- Consultas
- Conexiones

Tras configurar el dominio para utilizar la autenticación Kerberos, no podrá modificar las cuentas de usuario nativas.

Una vez que confirme que los grupos, las funciones, los privilegios y los permisos de las cuentas de usuario nativas se han migrado a las cuentas de usuario de LDAP correctamente, puede eliminar las cuentas de usuario nativas. Utilice la herramienta del administrador para eliminar las cuentas de usuario. Para obtener más información, consulte [“Cómo eliminar usuarios nativos” en la página 117](#).

## Paso 3. Configurar el archivo de configuración de Kerberos

Kerberos almacena la información de configuración en un archivo llamado *krb5.conf*. Informatica necesita establecer determinadas propiedades en el archivo de configuración de Kerberos de manera que el dominio de Informatica pueda utilizar la autenticación Kerberos correctamente. Debe establecer las propiedades del archivo de configuración *krb5.conf* y, a continuación, copiar el archivo en el directorio de Informatica.

El archivo de configuración contiene la información sobre el servidor de Kerberos, incluidos el dominio de Kerberos y la dirección del KDC. Puede solicitar al administrador de Kerberos que establezca las propiedades del archivo de configuración y que envíe una copia del archivo.

1. Realice una copia de seguridad del archivo *krb5.conf* antes de realizar cambios.
2. Edite el archivo *krb5.conf*.
3. En la sección *libdefaults*, establezca o añada las propiedades que requiere Informatica.

La siguiente tabla muestra los valores que debe utilizar para establecer las propiedades de la sección libdefaults:

Parámetro	Valor
default_realm	Nombre de dominio del servicio del dominio de Informatica.
forwardable	Permite que un servicio delegue credenciales de usuario del cliente a otro servicio. Establezca este parámetro como True. El dominio de Informatica requiere que los servicios de aplicación autentiquen las credenciales de usuario del cliente con otros servicios.
default_tkt_enctypes	Tipo de cifrado de la clave de sesión en el vale de concesión de vales (TGT). Establezca este parámetro como <i>rc4-hmac</i> . Informatica solo es compatible con el tipo de cifrado <i>rc4-hmac</i> .
udp_preference_limit	Determina el protocolo que utiliza Kerberos cuando envía un mensaje al KDC. Establezca <code>udp_preference_limit = 1</code> para usar TCP siempre. El dominio de Informatica solo es compatible con el protocolo TCP. Si <code>udp_preference_limit</code> está establecido en cualquier otro valor, el dominio de Informatica puede cerrarse de forma inesperada.

- En la sección de *dominios*, incluya el número de puerto en la dirección del KDC separado por dos puntos. Por ejemplo, si la dirección del KDC es `kerberos.example.com` y el número de puerto es 88, establezca el parámetro *kdc* como se indica a continuación:
 

```
kdc = kerberos.example.com:88
```
- Guarde el archivo `krb5.conf`.
- Copie el archivo de configuración en el directorio de Informatica.
 

Debe copiar `krb5.conf` en el directorio siguiente: `<INFA_HOME>/services/shared/security`. Si el dominio tiene varios nodos, copie `krb5.conf` en el mismo directorio en todos los nodos del dominio.

El siguiente ejemplo muestra el contenido de un `krb5.conf` con las propiedades requeridas:

```
[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 obtener más información sobre el archivo de configuración de Kerberos, consulte la documentación de autenticación red Kerberos.

## Paso 4. Generar el formato de nombre principal y de tabla de claves

Si ejecuta el dominio de Informatica con autenticación Kerberos, debe asociar los nombres principales de servicio (SPN) y los archivos de tabla de claves de Kerberos a los nodos y procesos del dominio de Informatica. Informatica necesita archivos de tabla de claves para autenticar servicios en la red sin solicitar contraseñas.

Según los requisitos de seguridad del dominio, puede establecer el nivel principal de servicio en uno de los siguientes niveles:

### **Nivel de nodo**

Si el dominio se utiliza para pruebas o desarrollo y no requiere un alto nivel de seguridad, puede configurar el principal del servicio a nivel de nodo. Puede utilizar un SPN y un archivo de tabla de claves para el nodo y todos los procesos del servicio del nodo. También debe configurar otro SPN y un archivo de tabla de claves diferente para los procesos HTTP del nodo.

### **Nivel de proceso**

Si el dominio se utiliza para producción y requiere un alto nivel de seguridad, puede configurar el principal del servicio a nivel de proceso. Cree un SPN y un archivo de tabla de claves únicos para cada nodo y cada proceso del nodo. También debe configurar otro SPN y un archivo de tabla de claves diferente para los procesos HTTP del nodo.

El dominio de Informatica requiere que los nombres principales del servicio y del archivo de claves tengan un determinado formato. Para garantizar que tengan el formato correcto para los nombres de archivo del nombre de servicio principal y de claves, utilice Informatica Kerberos SPN Format Generator para generar una lista de los nombres de archivo de los nombres de servicio principal y de claves en el formato requerido por el dominio de Informatica.

## Requisitos de principal de servicio a nivel de nodo

Si el dominio de Informatica no requiere un alto nivel de seguridad, el nodo y los procesos del servicio pueden compartir los mismos SPN y archivos de tabla de claves. El dominio no requiere un SPN independiente para cada proceso de servicio en un nodo.

El dominio de Informatica requiere un SPN y un archivo de tabla de claves para los siguientes componentes a nivel de nodo:

### **Nombre distintivo (DN) principal del servicio de directorio de LDAP**

El nombre principal del usuario de enlace de DN que se utiliza para realizar búsquedas en el servicio de directorio LDAP. El nombre del archivo de claves debe ser `infa_ldapuser.keytab`.

### **Proceso de nodo**

El nombre principal del nodo de Informatica que inicia o acepta las llamadas de autenticación. El mismo nombre principal se utiliza para autenticar los servicios en el nodo. Cada nodo de puerta de enlace del dominio requiere un nombre principal independiente.

### **Procesos HTTP en el dominio**

El nombre principal de todos los servicios de aplicación web en el dominio de Informatica, incluido Informatica Administrator. El navegador utiliza este nombre principal para autenticar todos los procesos de HTTP en el dominio. El nombre del archivo de claves debe ser `webapp_http.keytab`.

## Requisitos de principal de servicio a nivel de proceso

Si el dominio de Informatica requiere un alto nivel de seguridad, cree otro SPN y un archivo de tabla de claves diferente para cada nodo y cada servicio del nodo.

El dominio de Informatica requiere un SPN y un archivo de tabla de claves para los siguientes componentes a nivel de proceso:

### Nombre distintivo (DN) principal del servicio de directorio de LDAP

El nombre principal del usuario de enlace de DN que se utiliza para realizar búsquedas en el servicio de directorio LDAP. El nombre del archivo de claves debe ser `infa_ldapuser.keytab`.

### Proceso de nodo

El nombre principal del nodo de Informatica que inicia o acepta las llamadas de autenticación.

### Servicio de Informatica Administrator

El nombre principal del servicio de Informatica Administrator que autentica el servicio con otros servicios del dominio de Informatica. El nombre del archivo de tabla de claves debe ser `_AdminConsole.keytab`.

### Procesos HTTP en el dominio

El nombre principal de todos los servicios de aplicación web en el dominio de Informatica, incluido Informatica Administrator. El navegador utiliza este nombre principal para autenticar todos los procesos de HTTP en el dominio. El nombre del archivo de claves debe ser `webapp_http.keytab`.

### Proceso de servicio

El nombre principal del servicio de aplicación que se ejecuta en un nodo en el dominio de Informatica. Cada servicio de aplicación necesita un nombre principal de servicio y un nombre de archivo de tabla de claves únicos.

## Ejecutar Informatica Kerberos SPN Format Generator en Windows

Puede ejecutar Informatica Kerberos SPN Format Generator para generar un archivo que muestre el formato correcto de los nombres SPN y de los archivos de tabla de claves requeridos en el dominio de Informatica.

1. En un equipo que aloje el nodo de Informatica, vaya al siguiente directorio de Informatica:  
`<DirectorioDeInformatica>/Tools/Kerberos`
2. Ejecute el archivo `SPNFormatGenerator.bat`.  
Se abre la página de **bienvenida** de Informatica Kerberos SPN Format Generator.
3. Haga clic en **Siguiente**.  
Aparecerá la página **Nivel principal de servicio**.
4. Seleccione el nivel en el que se establecerán los principales del servicio de Kerberos del dominio.

La siguiente tabla describe los niveles que puede seleccionar:

Nivel	Descripción
Nivel de proceso	Configura el dominio para usar un nombre principal de servicio (SPN) y un archivo de claves únicos para cada nodo y cada servicio de aplicación en un nodo. El número de SPN y de archivos de tabla de claves necesarios para cada nodo depende del número de procesos del servicio de aplicación que se ejecutan en el nodo. Utilice la opción de nivel de proceso para los dominios que requieran un alto nivel de seguridad, como los dominios de producción.
Nivel de nodo	Configura el dominio para compartir archivos de SPN y de claves en un nodo. Esta opción requiere un SPN y un archivo de tabla de claves para el nodo y todos los servicios de aplicación que se ejecutan en el nodo. También se necesita otro SPN y un archivo de tabla de claves para todos los procesos de HTTP en el nodo. Utilice la opción de nivel de nodo para los dominios que no requieren un alto nivel de seguridad, como los dominios de pruebas y desarrollo.

- Haga clic en **Siguiente**.

Aparecerá la página **Parámetros de autenticación: autenticación Kerberos**.

- Introduzca los parámetros de dominio y nodo para generar el formato de SPN.

La siguiente tabla describe los parámetros que debe especificar:

Solicitud	Descripción
Nombre del dominio	El nombre del dominio. El nombre no debe superar los 128 caracteres y debe ser ASCII de 7 bits. No puede contener espacios ni los siguientes caracteres: ` % * + ; " ? , < > \ /
Nombre del nodo	El nombre del nodo de Informática.
Nombre de host del nodo	El nombre de host totalmente cualificado o la dirección IP del equipo en el que desea crear el nodo. El nombre de host del nodo no puede contener el carácter de subrayado (_). <b>Nota:</b> No utilice <i>localhost</i> . El nombre de host debe identificar el equipo de forma explícita.
Nombre del dominio de servicio	Nombre del dominio de Kerberos de los servicios del dominio de Informática. El nombre del dominio debe escribirse en mayúsculas.

Si establece el principal de servicio a nivel de nodo, la utilidad mostrará el botón **+Nodo**. Si establece el principal de servicio a nivel de proceso, la utilidad mostrará los botones **+Nodo** y **+Servicio**.

- Para generar el formato de SPN para un nodo adicional, haga clic en **+Nodo** y especifique el nombre de nodo y el nombre de host.

Puede especificar varios nodos para un dominio.

- Para generar el formato de SPN para un servicio, haga clic en **+Servicio** y especifique el nombre de servicio en el campo **Servicio en el nodo**.

El campo **Servicio en el nodo** solo se muestra si establece el principal de servicio a nivel de proceso y hace clic en **+Servicio**. Puede especificar varios servicios para un nodo. Los servicios aparecerán de forma inmediata debajo del nodo en el que se ejecutan.

9. Para quitar un nodo de la lista, haga clic en **-Nodo**.  
Informatica SPN Format Generator eliminará el nodo. Si ha añadido servicios al nodo, los servicios se eliminarán junto con el nodo.
10. Para quitar un servicio de un nodo, borre el campo de nombre de servicio.
11. Haga clic en **Siguiente**.  
SPN Format Generator muestra la ruta de acceso y el nombre del archivo que contiene la lista con los nombres principales de servicio y los de los archivos de tabla de claves.
12. Haga clic en **Terminado** para salir de SPN Format Generator.  
SPN Format Generator genera un archivo de texto que contiene nombres de archivo de SPN y de claves en el formato requerido para el dominio de Informatica.

## Ejecutar Informatica Kerberos SPN Format Generator en UNIX

Puede ejecutar Informatica Kerberos SPN Format Generator para generar un archivo que muestre el formato correcto de los nombres SPN y de los archivos de tabla de claves requeridos en el dominio de Informatica.

1. En un equipo que aloje el nodo de Informatica, vaya al siguiente directorio de Informatica:  
<DirectorioDeInformatica>/Tools/Kerberos
2. En una línea de comandos de shell, ejecute el archivo SPNFormatGenerator.sh.
3. Pulse **Intro** para continuar.
4. En la sección **Nivel principal de servicio**, seleccione el nivel en el que se establecerán los principales de servicio de Kerberos del dominio.

La siguiente tabla describe los niveles que puede seleccionar:

Nivel	Descripción
1->Nivel de proceso	Configura el dominio para usar un nombre principal de servicio (SPN) y un archivo de claves únicos para cada nodo y cada servicio de aplicación en un nodo. El número de SPN y de archivos de tabla de claves necesarios para cada nodo depende del número de procesos del servicio de aplicación que se ejecutan en el nodo. Utilice la opción de nivel de proceso para los dominios que requieran un alto nivel de seguridad, como los dominios de producción.
2->Nivel de nodo	Configura el dominio para compartir archivos de SPN y de claves en un nodo. Esta opción requiere un SPN y un archivo de tabla de claves para el nodo y todos los servicios de aplicación que se ejecutan en el nodo. También se necesita otro SPN y un archivo de tabla de claves para todos los procesos de HTTP en el nodo. Utilice la opción de nivel de nodo para los dominios que no requieren un alto nivel de seguridad, como los dominios de pruebas y desarrollo.

5. Introduzca los parámetros de dominio y nodo necesarios para generar el formato de SPN.



La siguiente tabla describe los parámetros que debe especificar:

Solicitud	Descripción
Nombre del dominio	El nombre del dominio. El nombre no debe superar los 128 caracteres y debe ser ASCII de 7 bits. No puede contener espacios ni los siguientes caracteres: ` % * + ; " ? , < > \ /
Nombre del nodo	El nombre del nodo de Informatica.
Nombre de host del nodo	El nombre de host totalmente cualificado o la dirección IP del equipo en el que desea crear el nodo. El nombre de host del nodo no puede contener el carácter de subrayado (_). <b>Nota:</b> No utilice <i>localhost</i> . El nombre de host debe identificar el equipo de forma explícita.
Nombre del dominio de servicio	Nombre del dominio de Kerberos de los servicios del dominio de Informatica. El nombre del dominio debe escribirse en mayúsculas.

Si establece el principal de servicio a nivel de nodo, aparecerá el mensaje **¿Agregar nodo?**. Si establece el principal de servicio a nivel de proceso, aparecerá el mensaje **¿Agregar servicio?**.

- En el mensaje **¿Agregar nodo?**, introduzca 1 para generar el formato de SPN para un nodo adicional. A continuación, introduzca el nombre de nodo y el nombre de host del nodo.

Para generar los formatos de SPN para varios nodos, introduzca 1 en cada mensaje **¿Agregar nodo?** y especifique un nombre de nodo y un nombre de host del nodo.

- En el mensaje **¿Agregar servicio?**, introduzca 1 para generar el formato de SPN de un servicio que se ejecutará en el nodo anterior. A continuación, introduzca el nombre de servicio.

Para generar los formatos de SPN para varios servicios, introduzca 1 en cada mensaje **¿Agregar servicio?** y especifique un nombre de servicio.

- Introduzca 2 para cerrar los mensajes **¿Agregar nodo?** o **¿Agregar servicio?**.

SPN Format Generator muestra la ruta de acceso y el nombre del archivo que contiene la lista con los nombres principales de servicio y los de los archivos de tabla de claves.

- Pulse Intro para salir de SPN Format Generator.

SPN Format Generator genera un archivo de texto que contiene nombres de archivo de SPN y de claves en el formato requerido para el dominio de Informatica.

## Paso 5. Revisar el archivo de texto de formato de SPN y de tabla de claves

Kerberos SPN Format Generator genera un archivo de texto llamado SPNKeytabFormat.txt que muestra el formato requerido por el dominio de Informatica para los nombres principales de servicio y los nombres de archivos de tabla de claves. Los nombres de SPN y de archivo de tabla de claves que incluye la lista varían en función del nivel principal de servicio que seleccione.

Revise el archivo de texto y compruebe que no hay mensajes de error.

El archivo de texto contiene la siguiente información:

### Nombre de entidad

Identifica el nodo o el servicio asociado al proceso.

### SPN

El formato del SPN en la base de datos principal de Kerberos. El SPN distingue entre mayúsculas y minúsculas. Cada tipo de SPN tiene un formato diferente.

Un SPN puede tener uno de los siguientes formatos:

Tipo de tabla de claves	Formato de SPN
NODE_SPN	isp/<NombreDeNodo>/<NombreDeDominio>@<NOMBREREAL>
NODE_AC_SPN	_AdminConsole/<NombreDeNodo>/<NombreDeDominio>@<NOMBREREAL>
NODE_HTTP_SPN	HTTP/<NombreDeHostDeNodo>@<NOMBREREAL> <b>Nota:</b> Kerberos SPN Format Generator valida el nombre de host del nodo. Si el nombre de host del nodo no es válido, la utilidad no genera un SPN. En su lugar, se muestra el siguiente mensaje: No se puede resolver el nombre de host.
SERVICE_PROCESS_SPN	<NombreDeServicio>/<NombreDeNodo>/<NombreDeDominio>@<NOMBREREAL>

### Nombre de archivo de tabla de claves

El formato del nombre de archivo de tabla de claves que se creará para el SPN asociado en la base de datos principal de Kerberos. El nombre del archivo de tabla de claves distingue entre mayúsculas y minúsculas.

Los nombres de archivo de tabla de claves utilizan los siguientes formatos:

Tipo de tabla de claves	Nombre de archivo de tabla de claves
NODE_SPN	<NombreDeNodo>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<NombreDeServicio>.keytab

### Tipo de tabla de claves

El tipo de la tabla de claves. El tipo de tabla de claves puede ser uno de los siguientes tipos:

- NODE\_SPN. El archivo de tabla de claves de un proceso del nodo.
- NODE\_AC\_SPN. El archivo de tabla de claves del proceso de servicio de Informatica Administrator.
- NODE\_HTTP\_SPN. El archivo de tabla de claves de los procesos HTTP de un nodo.
- SERVICE\_PROCESS\_SPN. El archivo de tabla de claves de un proceso de servicio.

## Principales de servicio a nivel de nodo

El siguiente ejemplo muestra el contenido del archivo SPNKeytabFormat.txt generado para los principales de servicio a nivel del nodo:

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		

## Principales de servicio a nivel de proceso

El siguiente ejemplo muestra el contenido del archivo SPNKeytabFormat.txt generado para los principales de servicio a nivel de proceso:

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

# Paso 6. Crear los archivos de nombres principales de servicio y de tabla de claves

Después de generar la lista de nombres de SPN y de archivos de tabla de claves con el formato requerido por Informatica, envíe una solicitud al administrador de Kerberos para añadir los SPN a la base de datos principal de Kerberos y crear los archivos de tabla de claves.

Utilice las siguientes directrices cuando cree los archivos de SPN y de claves:

**El nombre principal de usuario (UPN) debe ser el mismo que el del SPN.**

Cuando cree una cuenta de usuario para el servicio principal, debe establecer el UPN con el mismo nombre que el SPN. Los servicios de aplicación del dominio de Informatica pueden actuar como un servicio o un cliente según la operación. Debe configurar el servicio principal para que se pueda identificar por el mismo UPN y SPN.

Una cuenta de usuario debe estar asociada a un solo SPN. No establezca varios SPN para una cuenta de usuario.

#### **Habilite la delegación en Microsoft Active Directory.**

Debe habilitar la delegación para todas las cuentas de usuario con principales de servicio utilizados en el dominio de Informatica. En el servicio Microsoft Active Directory, establezca la opción **Confiar en este usuario para la delegación a cualquier servicio (solo Kerberos)** en cada cuenta de usuario en la que establezca un SPN.

La autenticación delegada ocurre cuando se autentica un usuario en un servicio y este servicio usa las credenciales del usuario autenticado para conectarse a otro servicio. Debido a que los servicios del dominio de Informatica deben conectarse a otros servicios para completar operaciones, el dominio de Informatica requiere que la opción de delegación esté habilitada en Microsoft Active Directory.

Por ejemplo, cuando un cliente de PowerCenter se conecta al servicio de repositorio de PowerCenter, la cuenta de usuario del cliente se autentica con el nombre principal del servicio de repositorio de PowerCenter. Cuando el servicio de repositorio de PowerCenter se conecta al servicio de integración de PowerCenter, el nombre principal del servicio de repositorio de PowerCenter puede utilizar las credenciales del usuario para autenticar con el servicio de integración de PowerCenter. No es necesario que la cuenta de usuario cliente también se autentique con el servicio de integración de PowerCenter.

#### **Utilice la utilidad ktpass para crear los archivos de clave principal de servicio.**

Microsoft Active Directory suministra la utilidad ktpass para crear archivos de claves. Informatica es compatible con autenticación Kerberos solo en Microsoft Active Directory y tiene archivos de claves únicos certificados que se crean con ktpass.

Los archivos de tabla de claves de un nodo deben estar disponibles en el equipo que aloja el nodo. De forma predeterminada, los archivos de tabla de claves se almacenan en el siguiente directorio: <INFA\_HOME>/isp/config/keys.

Cuando reciba los archivos de tabla de claves del administrador de Kerberos, cópielos en el directorio especificado para los archivos de tabla de claves utilizados en el dominio de Informatica.

## **Solucionar problemas de los nombres principales de servicio y los archivos de tabla de claves**

Puede usar utilidades de Kerberos para comprobar que los nombres principales de servicio y los nombres de archivo de tabla de claves creados por el administrador de Kerberos coinciden con los nombres que se han solicitado. También puede usar las utilidades para determinar el estado del centro de distribución de claves de Kerberos (KDC).

Puede usar las utilidades de Kerberos, *comosetspn*, *kinit* y *klist*, para ver y comprobar los SPN y los archivos de tabla de claves. Para usar las utilidades, asegúrese de que la variable de entorno KRB5\_CONFIG contiene la ruta de acceso y el nombre de archivo del archivo de configuración de Kerberos.

**Nota:** Los siguientes ejemplos muestran formas de usar las utilidades de Kerberos para comprobar que los SPN y los archivos de tabla de claves son válidos. Puede que los ejemplos sean diferentes del modo en que el administrador de Kerberos usa las utilidades para crear los SPN y los archivos de tabla de claves necesarios para el dominio de Informatica. Para obtener más información sobre la ejecución de las utilidades de Kerberos, consulte la documentación de Kerberos.

Use las siguientes utilidades para comprobar los SPN y los archivos de tabla de claves:

## klist

Puede usar *klist* para enumerar los principales de Kerberos y las claves en un archivo de tabla de claves. Para enumerar las claves en el archivo de tabla de claves y la marca de tiempo de la entrada de tabla de claves, ejecute el siguiente comando:

```
klist -k -t <keytab_file>
```

El siguiente ejemplo de una salida muestra los principales en un archivo de tabla de claves:

```
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

Puede usar *kinit* para solicitar un ticket que otorga tickets para una cuenta de usuario para comprobar que el KDC funciona y puede conceder tickets. Para solicitar un ticket que otorga tickets para una cuenta de usuario, ejecute el siguiente comando:

```
kinit <user_account>
```

También puede usar *kinit* para solicitar un ticket que otorga tickets y comprobar que el archivo de tabla de claves se puede utilizar para establecer una conexión de Kerberos. Para solicitar un ticket que otorga tickets para un SPN, ejecute el siguiente comando:

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

El siguiente ejemplo de una salida muestra el ticket que otorga tickets creado en la memoria caché predeterminada para un archivo de tabla de claves y un SPN específicos:

```
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

Puede usar *setspn* para ver, modificar o eliminar el SPN de una cuenta de servicio de Active Directory. En el equipo que aloja el servicio de Active Directory, abra una ventana de la línea de comandos y ejecute el comando.

Para ver los SPN que están asociados a una cuenta de usuario, ejecute el siguiente comando:

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

El siguiente ejemplo de una salida muestra el SPN asociado a la cuenta de usuario *is96svc*:

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

Para ver las cuentas de usuario asociadas a un SPN, ejecute el siguiente comando:

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

El siguiente ejemplo de una salida muestra la cuenta de usuario asociada al 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 buscar SPN duplicados, ejecute el siguiente comando:

```
setspn -X
```

El siguiente ejemplo de una salida muestra varias cuentas de usuario asociadas a un 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:** La búsqueda de SPN duplicados puede tardar bastante y consumir una gran cantidad de memoria.

### **kdestroy**

Puede usar *kdestroy* para eliminar los tickets de autorización de Kerberos activos y la memoria caché de credenciales de usuario donde están alojados. Si ejecuta *kdestroy* sin parámetros, eliminará la memoria caché de credenciales predeterminada.

## Paso 7. Configurar la autenticación Kerberos del dominio

Ejecute *infasetup* para cambiar la autenticación del dominio de Informatica a la autenticación de red Kerberos.

**Nota:** Compruebe que todos los objetos del repositorio están protegidos antes de configurar el dominio para utilizar la autenticación Kerberos.

Cuando ejecuta el comando *infasetup* para cambiar la autenticación del dominio, el comando crea los siguientes dominios de seguridad de LDAP:

- Dominio de seguridad interno. El dominio de seguridad interno es un dominio de seguridad LDAP con el nombre *\_infaInternalNamespace*. El dominio de seguridad *\_infaInternalNamespace* contiene la cuenta de usuario administrador predeterminada que se creó al configurar la autenticación Kerberos. Una vez configurada la autenticación Kerberos, no podrá añadir usuarios al dominio de seguridad *\_infaInternalNamespace* o eliminar el dominio de seguridad.
- Dominio de seguridad del dominio de usuario. El dominio de seguridad del dominio de usuario es un dominio de seguridad LDAP vacío con el mismo nombre que el dominio de usuario de Kerberos. Una vez configurada la autenticación Kerberos, no podrá importar usuarios desde la base de datos principal de Kerberos al dominio de seguridad del dominio de usuario.

El comando *infasetup* también crea una cuenta de usuario administrador. Especifique el nombre de usuario del usuario administrador. Después de configurar la autenticación Kerberos, el dominio de seguridad *\_infaInternalNamespace* contiene la cuenta de usuario administrador.

Para configurar el dominio para utilizar autenticación Kerberos, ejecute el siguiente comando:

```
infasetup switchToKerberosMode
```

1. En el nodo de puerta de enlace, ejecute el comando *infasetup* para cambiar la autenticación del dominio. En el símbolo del sistema, vaya al directorio en el que se encuentran los programas de la línea de comandos de Informatica. De forma predeterminada, los programas de la línea de comandos están instalados en el siguiente directorio: *<InformaticaInstallationDir>/isp/bin*

2. Ejecute el comando `infasetup` con las opciones y los argumentos requeridos.

Especifique los siguientes comandos:

- Windows: `infasetup switchToKerberosMode`
- UNIX: `infasetup.sh switchToKerberosMode`

La siguiente tabla describe las opciones para el comando `switchToKerberosMode`:

Opción	Argumento	Descripción
-administratorName -ad	administrator_name	El nombre de usuario de la cuenta de administrador del dominio que se crea al configurar la autenticación Kerberos. La cuenta de usuario debe estar en la base de datos principal de Kerberos.  Después de configurar la autenticación Kerberos, este usuario se incluye en el dominio de seguridad <i>_infalInternalNamespace</i> .
-ServiceRealmName -srn	realm _name_of_node_spn	Nombre del dominio de Kerberos al que pertenecen los servicios del dominio de Informática. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas.  El nombre del dominio del servicio y el del dominio del usuario deben coincidir.
-UserRealmName -urn	realm _name_of_user_spn	Nombre del dominio de Kerberos al que pertenecen los usuarios del dominio de Informática. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas.  El nombre del dominio del servicio y el del dominio del usuario deben coincidir.
-SPNShareLevel -spnSL	PROCESS  NODE	El nivel principal de servicio del dominio. Establezca la propiedad en uno de los siguientes niveles: - Proceso. El dominio necesita un nombre principal de servicio (SPN) y un archivo de tabla de claves únicos para cada nodo y cada servicio en un nodo. El número de SPN y de archivos de tabla de claves necesarios para cada nodo depende del número de procesos del servicio que se ejecutan en el nodo. Utilice la opción de nivel de proceso si el dominio requiere un alto nivel de seguridad, como en el caso de un dominio de producción. - Nodo. El dominio utiliza un SPN y un archivo de tabla de claves para el nodo y todos los servicios que se ejecutan en el nodo. También se necesita otro SPN y un archivo de tabla de claves para todos los procesos de HTTP en el nodo. Utilice la opción de nivel de nodo si el dominio no requiere un alto nivel de seguridad, como en el caso de un dominio de pruebas o de desarrollo. El valor predeterminado es el proceso.

El comando `switchToKerberosMode` cambia el modo de autenticación para el dominio de autenticación de usuario nativa o autenticación de usuario de LDAP a autenticación de red de Kerberos.

## Paso 8. Actualizar los nodos del dominio

Ejecute el comando `infasetup` para actualizar todos los nodos del dominio con la información del servidor de autenticación Kerberos.

Actualice todos los nodos de puerta de enlace y de trabajo con la información del servidor de autenticación Kerberos excepto el nodo de puerta de enlace en el que se ejecuta el comando `switchToKerberosMode`.

Para actualizar la puerta de enlace y los nodos de trabajo, utilice los siguientes comandos:

### **infasetup UpdateGatewayNode**

Utilice el comando `UpdateGatewayNode` para establecer los parámetros de autenticación Kerberos en un nodo de puerta de enlace del dominio. Si el dominio tiene varios nodos de puerta de enlace, ejecute el comando `UpdateGatewayNode` en cada nodo de puerta de enlace.

### **infasetup UpdateWorkerNode**

Utilice el comando `UpdateWorkerNode` para establecer los parámetros de autenticación Kerberos en un nodo de trabajo del dominio. Si el dominio tiene varios nodos de trabajo, ejecute el comando `UpdateWorkerNode` en cada nodo de trabajo.

1. En un equipo que aloja un nodo de Informática, ejecute el comando `infasetup` para actualizar el nodo.

En el símbolo del sistema, vaya al directorio en el que se encuentran los programas de la línea de comandos de Informática. De forma predeterminada, los programas de la línea de comandos están instalados en el siguiente directorio: `<InformaticaInstallationDir>/isp/bin`

2. Ejecute `infasetup` con las opciones y argumentos requeridos.

Introduzca el siguiente comando:

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

La siguiente tabla describe las opciones para actualizar la información de autenticación Kerberos para un nodo:

Opción	Argumento	Descripción
-EnableKerberos -krb	enable_kerberos	Configura el dominio de Informática para utilizar la autenticación Kerberos.
-ServiceRealmName -srn	realm _name_of_node_spn	Nombre del dominio de Kerberos al que pertenecen los servicios del dominio de Informática. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas.  El nombre del dominio del servicio y el del dominio del usuario deben coincidir.
-UserRealmName -urn	realm _name_of_user_spn	Nombre del dominio de Kerberos al que pertenecen los usuarios del dominio de Informática. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas.  El nombre del dominio del servicio y el del dominio del usuario deben coincidir.



## Paso 9. Actualizar los equipos cliente

Copie el archivo de configuración de Kerberos y establezca la variable de entorno en los equipos que alojan los clientes de Informatica. También deberá configurar el navegador para que acceda a las aplicaciones web de Informatica.

Tras configurar el dominio de Informatica para ejecutar la autenticación Kerberos, realice las siguientes tareas en las herramientas de cliente de Informatica:

### **Copie el archivo de configuración de Kerberos a los equipos cliente.**

Copie el archivo de configuración en cada equipo que aloja un cliente de Informatica. Debe copiar el archivo `krb5.conf` en el siguiente directorio: <Directorio del cliente de Informatica>/shared/security

### **Configure las variables de entorno KRB5\_CONFIG utilizando el archivo de configuración de Kerberos.**

Utilice la variable de entorno KRB5\_CONFIG para almacenar la ruta de acceso y el nombre del archivo de configuración de Kerberos, `krb5.conf`. Debe establecer la variable de entorno KRB5\_CONFIG en cada equipo que hospede un cliente de Informatica.

### **Configure el navegador web.**

Si el dominio de Informatica se ejecuta en una red con autenticación Kerberos, deberá configurar el navegador para permitir el acceso a las aplicaciones web de Informatica. En Microsoft Internet Explorer y en Google Chrome, añada la URL de la aplicación web de Informatica a la lista de sitios de confianza. Si utiliza Chrome 41 o posterior, también debe definir las directivas `AuthServerWhitelist` y `AuthNegotiateDelegateWhitelist`.

### **En UNIX, cree un archivo de memoria caché de credenciales para inicios de sesión únicos**

Para ejecutar los programas de la línea de comandos de Informatica en UNIX con inicio de sesión único, debe generar un archivo de memoria caché de credenciales para autenticar la cuenta de usuario que ejecuta los comandos en la red de Kerberos. Utilice la utilidad `kinit` de MIT Kerberos para generar el archivo de memoria caché de credenciales. El archivo de memoria caché de credenciales permite que un usuario ejecute los comandos sin las opciones de nombre de usuario y contraseña.

Si utiliza un archivo de memoria caché de credenciales, debe establecer la ruta predeterminada y el nombre de archivo de la memoria caché de credenciales en la variable de entorno KRB5CCNAME.

Para obtener más información sobre la ejecución de los programas de la línea de comandos de Informatica en UNIX con inicio de sesión único, consulte *Referencia de comando de Informatica*.

## Paso 10. Iniciar el dominio de Informatica

Tras configurar el dominio de Informatica para utilizar la autenticación Kerberos, inicie el dominio y la herramienta Administrator.

1. En Windows, puede iniciar el servicio de Informatica desde el Panel de control o el menú Inicio.

Para iniciar Informatica desde el menú Inicio de Windows, haga clic en **Programas > Informatica [versión] > Servidor**. Haga clic con el botón derecho en **Iniciar servicios de Informatica** y seleccione **Ejecutar como administrador**.

En UNIX, ejecute el siguiente comando para iniciar el daemon de Informatica:

```
infaservice.sh startup
```

De forma predeterminada, `infaservice.sh` se instala en el siguiente directorio: <INFA\_HOME>/tomcat/bin

2. Inicie Informatica Administrator.

Utilice la siguiente URL para iniciar la herramienta del administrador: `http://<nombre de host completo>:<puerto http>`. Si ha configurado la herramienta del administrador para utilizar una conexión segura, utilice el protocolo HTTPS: `https://<nombre de host completo>:<puerto http>`

Al iniciar la herramienta Administrator, deberá añadir la URL a la lista de sitios de confianza del navegador.

3. Seleccione el dominio de seguridad para su cuenta de usuario.

Si utiliza la autenticación Kerberos, la red utiliza el inicio de sesión único. No necesita iniciar sesión en la herramienta Administrator con un nombre de usuario y una contraseña.

## Después de configurar la autenticación Kerberos

Si el nivel principal de servicio del dominio está a nivel de proceso, el dominio requerirá un SPN y un archivo de tabla de claves para cada servicio que cree en el dominio. Antes de habilitar un servicio, compruebe que hay un SPN y un archivo de tabla de claves disponible para el servicio. Kerberos no puede autenticar el servicio de aplicación si no tiene un archivo de tabla de claves en el directorio de Informatica.

Si no hay ningún SPN ni archivos de tabla de claves disponibles para los servicios de aplicación que va a crear en el dominio, debe crear el SPN y el archivo de tabla de claves antes de habilitar el servicio. Puede utilizar Informatica Kerberos SPN Format Generator para generar el formato del SPN y del nombre de archivo de tabla de claves del servicio. Para ahorrar tiempo, piense en los nombres de los servicios que quiera crear y los nodos en los que se ejecutarán. A continuación, ejecute la utilidad para generar a la vez el formato del SPN y del nombre de archivo de tabla de claves de todos los servicios.

Para obtener más información sobre Informatica Kerberos SPN Format Generator, consulte [“Paso 4. Generar el formato de nombre principal y de tabla de claves” en la página 37.](#)

Envíe una solicitud al administrador de Kerberos para añadir los SPN a la base de datos principal y crear el archivo de tabla de claves correspondiente.

Cuando reciba los archivos de tabla de claves del administrador de Kerberos, copie los archivos en el directorio especificado para el archivo de tabla de claves. De forma predeterminada, los archivos de tabla de claves se almacenan en el siguiente directorio: `<INFA_HOME>/isp/config/keys`

Si el nivel principal de servicio del dominio está a nivel de nodo, puede crear y habilitar los servicios de aplicación sin crear SPN ni archivos de tabla de claves adicionales.

## Bibliotecas personalizadas de Kerberos

Puede configurar clientes de base de datos personalizados o nativos dentro del dominio de Informatica a fin de utilizar bibliotecas personalizadas de Kerberos en lugar de las bibliotecas predeterminadas de Kerberos que utiliza Informatica.

Puede que desee utilizar las bibliotecas personalizadas de Kerberos en las situaciones siguientes:

### **Utilizar bibliotecas personalizadas de Kerberos en un dominio de Informatica que no está configurado para utilizar Kerberos.**

En esta situación, dispone de un cliente de base de datos que conecta a bases de datos de origen o destino que se utilizan para las asignaciones. Las bases de datos están configuradas para utilizar las bibliotecas personalizadas de Kerberos para la autenticación. Sin embargo, el dominio de Informatica no está configurado para utilizar la autenticación Kerberos.

Para permitir que el cliente de base de datos se conecte a las bases de datos mediante Informatica, puede hacer que las bibliotecas personalizadas estén disponibles para el cliente de base de datos. Sin embargo, los procesos del dominio de Informatica no utilizan las bibliotecas personalizadas de Kerberos para la autenticación.

### **Utilizar las bibliotecas personalizadas de Kerberos en un dominio de Informatica protegido con Kerberos.**

En esta situación, el cliente de base de datos conecta a bases de datos de origen o destino que están configuradas para utilizar bibliotecas personalizadas de Kerberos. Sin embargo, el dominio de Informatica está configurado para utilizar las bibliotecas de Kerberos predeterminadas de Informatica para la autenticación.

Para permitir que el cliente de base de datos se conecte a las bases de datos mediante Informatica, puede configurar el dominio de Informatica para que cargue las bibliotecas personalizadas de Kerberos en lugar de las bibliotecas de Kerberos predeterminadas de Informatica. Todos los procesos y subprocesos del dominio de Informatica utilizan las bibliotecas personalizadas de Kerberos.

Si es necesario, puede eliminar los vínculos a las bibliotecas personalizadas de Kerberos y actualizar los nodos del dominio para volver a usar las bibliotecas de Kerberos predeterminadas de Informatica.

## **Utilizar las bibliotecas personalizadas de Kerberos**

Utilice el comando `infasetup updateMitKerberosLinkage` para configurar los servicios de aplicación y los clientes de la base de datos en un dominio de Informatica para utilizar bibliotecas personalizadas de Kerberos.

Debe especificar el directorio que contiene las bibliotecas de Kerberos que desea utilizar. Puede copiar las bibliotecas a cada nodo o en una ubicación compartida a la que puedan acceder todos los nodos del dominio.

Si el dominio de Informatica utiliza la autenticación Kerberos, asegúrese de que las bibliotecas personalizadas de Kerberos que desea utilizar tienen el mismo número de versión que las bibliotecas de Kerberos que Informatica utiliza de forma predeterminada.

1. Coloque las bibliotecas personalizadas de Kerberos en una ubicación a la que puedan acceder todos los nodos del dominio.
2. Cierre el dominio.
3. Ejecute el comando `infasetup updateMitKerberosLinkage` en cada nodo del dominio.

La tabla siguiente describe las opciones y los argumentos del comando `infasetup updateMitKerberosLinkage`:

Opción	Argumento	Descripción
-useKerberos -krb	true false	<p>Obligatorio. Establezca este valor en true si el dominio de Informatica utiliza la autenticación Kerberos. Si el valor se establece en true, los procesos de Informatica llaman a Kerberos con las bibliotecas de Kerberos predeterminadas o con las bibliotecas en el directorio especificado con la opción -mkd.</p> <p>Establezca este valor en false si el dominio de Informatica no utiliza la autenticación Kerberos. Si el valor se establece en false, el dominio de Informatica no carga las bibliotecas de Kerberos. Los clientes de la base de datos llaman a Kerberos con las bibliotecas personalizadas especificadas en el directorio especificado con la opción -mkd.</p>
-mitKerberosDirectory -mkd	kerberos_library_directory_node_spn	<p>Opcional. El directorio que contiene las bibliotecas personalizadas de Kerberos. El directorio debe contener los archivos de biblioteca. No puede utilizar vínculos simbólicos.</p> <p>Si la opción -krb es true, asegúrese de que las bibliotecas de Kerberos personalizadas que desea utilizar tengan el mismo número de versión que las bibliotecas de Kerberos que Informatica utiliza de forma predeterminada.</p> <p>Si hay varias versiones de la misma biblioteca, todas las versiones deben tener el mismo tamaño y la misma suma de comprobación. Por ejemplo, si el directorio contiene dos versiones de libkrb5, como libkr5.so.3 y libkrb5.so, ambas bibliotecas deben tener el mismo tamaño de archivo y el mismo valor de suma de comprobación.</p> <p>Si el directorio especificado está vacío, el comando elimina todas las bibliotecas de Kerberos personalizadas del dominio de Informatica.</p> <p>Si la opción -krb se establece en true, pero no se especifica un directorio de biblioteca, Informatica utiliza las bibliotecas predeterminadas de Kerberos.</p>

- Reinicie el dominio después de ejecutar el comando en todos los nodos.

## Volver a utilizar las bibliotecas de Kerberos predeterminadas

Ejecute el comando `infasetup restoreMitKerberosLinkage` en los nodos de un dominio de Informatica para restaurar los vínculos a las bibliotecas de Kerberos predeterminadas que utiliza Informatica. El comando elimina los vínculos a las bibliotecas personalizadas de Kerberos que existen dentro del dominio de Informatica.

- Cierre el dominio.
- Ejecute el comando `restoreMitKerberosLinkage` en cada nodo del dominio.  
El comando no utiliza ninguna opción ni argumentos.
- Reinicie el dominio después de ejecutar el comando en todos los nodos.

## CAPÍTULO 5

# Seguridad del dominio

Este capítulo incluye los siguientes temas:

- [Resumen de la seguridad del dominio, 53](#)
- [Comunicación segura dentro del dominio, 54](#)
- [Conexiones seguras a un servicio de aplicación web, 65](#)
- [Conjuntos de cifrado para el dominio de Informatica, 69](#)
- [Orígenes y destinos seguros, 71](#)
- [Almacenamiento de datos seguro, 73](#)
- [Servicios de aplicación y puertos, 77](#)

## Resumen de la seguridad del dominio

Puede habilitar opciones en el dominio de Informatica para configurar una comunicación segura entre los componentes del dominio y entre el dominio y los componentes del cliente.

Puede habilitar diferentes opciones para asegurar componentes específicos del dominio. No tiene que asegurar todos los componentes del dominio. Por ejemplo, puede asegurar la comunicación entre los servicios del dominio, pero no asegurar la conexión entre el servicio de repositorio de modelos y la base de datos del repositorio.

Informatica utiliza los protocolos TCP/IP y HTTP para comunicarse entre sus componentes en el dominio. El dominio utiliza certificados SSL para asegurar la comunicación entre componentes.

Al instalar los servicios de Informatica, puede habilitar una comunicación segura para los servicios del dominio y para la herramienta Administrator. Tras la instalación, puede configurar una comunicación segura en el dominio mediante la Herramienta del administrador o desde la línea de comandos.

Durante la instalación, el programa de instalación genera una clave de cifrado para cifrar datos confidenciales, como las contraseñas, que se almacenan en el dominio. Puede proporcionar la palabra clave que utilizará el programa de instalación para generar la clave de cifrado. Tras la instalación, puede cambiar la clave de cifrado para datos confidenciales. Debe actualizar el contenido de los repositorios para actualizar los datos cifrados.

Puede habilitar la comunicación segura en las siguientes áreas:

### **Dominio**

En el dominio, puede seleccionar opciones para habilitar la comunicación segura para los componentes siguientes:

- Entre el administrador de servicios, los servicios del dominio y las herramientas cliente de Informatica
- Entre el dominio y el repositorio de configuración del dominio
- Entre los servicios de repositorio y las bases de datos del repositorio
- Entre el servicio de integración de PowerCenter y los procesos DTM

### **Servicios de aplicación web**

Puede proteger la conexión entre un servicio de aplicación web, como el servicio del analista, y el navegador.

### **Orígenes y destinos**

Puede habilitar una comunicación segura entre el servicio de integración de datos y el servicio de integración de PowerCenter y las bases de datos de origen y destino.

### **Almacenamiento de datos**

Informatica cifra datos confidenciales, como las contraseñas, cuando almacena datos en el dominio. Informatica genera una clave de cifrado en función de una palabra clave que se proporciona durante la instalación. Informatica utiliza la clave de cifrado para cifrar y descifrar datos confidenciales que estén almacenados en el dominio.

## Comunicación segura dentro del dominio

Puede utilizar la opción Comunicación segura para asegurar la conexión entre servicios y entre servicios y los administradores de servicios del dominio. Además, puede habilitar la seguridad para los flujos de trabajo y utilizar las bases de datos seguras para los repositorios que cree en el dominio.

Después de proteger el dominio, configure las aplicaciones del cliente de Informatica para trabajar con un dominio de seguro.

## Comunicación segura de los servicios y el Administrador de servicios

Puede configurar la comunicación segura del dominio durante la instalación. Tras la instalación, puede configurar la comunicación segura para el dominio en la Herramienta del administrador o desde la línea de comandos.

Informatica proporciona un certificado SSL que se puede utilizar para asegurar el dominio. Sin embargo, debe proporcionar un certificado SSL personalizado para los dominios que requieran un mayor nivel de seguridad, como un dominio en un entorno de producción. Especifique los archivos de almacén de claves y truststore que contienen los certificados SSL que desee utilizar.

**Nota:** Informatica proporciona certificados SSL con fines de evaluación. Si no proporciona un certificado SSL, Informatica utiliza la misma clave privada predeterminada para todas las instalaciones de Informatica. La seguridad de su dominio podría estar en peligro. Proporcione un certificado SSL para garantizar un nivel de seguridad alto para el dominio. El certificado que proporcione puede estar autofirmado o lo puede firmar una entidad de certificación (CA).

Al configurar la comunicación segura para el dominio, se aseguran las conexiones entre los siguientes componentes:

- El Administrador de servicios y todos los servicios que se ejecutan en el dominio
- El Servicio de integración de datos y el Servicio de repositorio de modelos
- El Servicio de integración de datos y los procesos de flujo de trabajo
- El servicio de integración de PowerCenter y el servicio de repositorio de PowerCenter
- Los servicios del dominio y las herramientas cliente de Informatica y los programas de la línea de comandos

## Requisitos para la comunicación segura en el dominio

Antes de habilitar la comunicación segura en el dominio, asegúrese de que se cumplen los siguientes requisitos:

### Ha creado una solicitud de firma de certificado (CSR) y una clave privada.

Puede utilizar keytool u OpenSSL para crear el CSR y la clave privada.

Si utiliza cifrado RSA, debe utilizar más de 512 bits.

### Tiene un certificado SSL firmado.

El certificado pueden ser autofirmado o firmado por una CA. Informatica recomienda un certificado firmado por una CA.

### Ha importado el certificado en almacenes de claves.

Debe tener un almacén de claves con formato PEM denominado `infa_keystore.pem` y un almacén de claves con formato JKS denominado `infa_keystore.jks`.

**Nota:** La contraseña para el almacén de claves con formato JKS debe ser la misma que la frase de contraseña de la clave privada utilizada para generar el certificado SSL.

### Ha importado el certificado en truststores.

Debe tener un truststore con formato PEM denominado `infa_keystore.pem` y un almacén de claves con formato JKS denominado `infa_keystore.jks`.

### Los almacenes de claves y los truststores se encuentran en el directorio correcto.

Si habilita la comunicación segura durante la instalación, el almacén de claves y el truststore deben estar en un directorio al que pueda acceder el programa de instalación.

Si habilita la comunicación segura tras la instalación, el almacén de claves y el truststore deben estar en un directorio al que puedan acceder los programas de la línea de comandos.

Para obtener más información acerca de cómo crear un almacén de claves y un truststore personalizados, consulte el artículo de la Biblioteca de asistencia de Informatica sobre la creación de archivos truststore y de almacén de claves para comunicaciones seguras en el dominio de Informatica:

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

Después de proteger el dominio, configure las aplicaciones del cliente de Informatica para trabajar con un dominio de seguro.

## Habilitar la comunicación segura para el dominio desde la línea de comandos

Utilice los comandos `infacmd` e `infasetup` para habilitar la comunicación segura del dominio. Tras habilitar la comunicación segura, debe reiniciar el dominio para que el cambio surta efecto.

Para utilizar sus archivos de certificados SSL, especifique los archivos de almacén de claves y `truststore` cuando ejecute el comando `infasetup`.

Para configurar la comunicación de dominio segura desde la línea de comandos, utilice los siguientes comandos:

### **infacmd isp UpdateDomainOptions**

Utilice el comando `UpdateDomainOptions` para establecer el modo de comunicación segura para el dominio.

### **infasetup UpdateGatewayNode**

Utilice el comando `UpdateGatewayNode` para habilitar la comunicación segura del administrador de servicios en un nodo de puerta de enlace de un dominio. Si el dominio tiene varios nodos de puerta de enlace, ejecute el comando `UpdateGatewayNode` en cada nodo de puerta de enlace.

### **infasetup UpdateWorkerNode**

Utilice el comando `UpdateWorkerNode` para habilitar la comunicación segura del administrador de servicios en un nodo de trabajo de un dominio. Si el dominio tiene varios nodos de trabajo, ejecute el comando `UpdateWorkerNode` en cada nodo de trabajo.

1. Compruebe que el dominio que desea asegurar se está ejecutando.
2. Actualice el dominio.

Ejecute el comando siguiente con las opciones y los argumentos requeridos:

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

Para configurar la comunicación segura para el dominio, incluya la siguiente opción cuando ejecute el comando `infacmd`:

Opción	Argumento	Descripción
-DomainOptions -do	option_name=value	Establezca la siguiente opción para configurar la comunicación segura para el dominio: TLSMode=True

3. Cierre el dominio.  
El dominio debe estar cerrado antes de ejecutar los comandos `infasetup`.
4. Ejecute `infasetup` con las opciones y argumentos requeridos.

Introduzca el siguiente comando:

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



Para configurar la comunicación segura de los nodos, ejecute los comandos con las siguientes opciones:

Opción	Argumento	Descripción
-EnableTLS -tls	enable_tls	Configura la comunicación segura de los servicios en el dominio de Informatica.
-NodeKeystore -nk	node_keystore_directory	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Directorio que contiene los archivos de almacén de claves. El dominio de Informatica requiere que el certificado SSL tenga el formato PEM y se encuentre en archivos Java Keystore (JKS). El directorio debe contener archivos de almacén de claves en formato PEM y JKS. Los archivos de almacén de claves deben llamarse infa_keystore.jks e infa_keystore.pem. Puede utilizar el mismo archivo de almacén de claves para varios nodos.
-NodeKeystorePass -nkp	node_keystore_password	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Contraseña del archivo infa_keystore.jks.
-NodeTruststore -nt	node_truststore_directory	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Directorio que contiene los archivos de truststore. El dominio de Informatica requiere que el certificado SSL tenga el formato PEM y se encuentre en archivos Java Keystore (JKS). El directorio debe contener archivos de truststore en formato PEM y JKS. Los archivos de truststore deben llamarse infa_truststore.jks e infa_truststore.pem. Puede utilizar el mismo archivo de truststore para varios nodos.
-NodeTruststorePass -ntp	node_truststore_password	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Contraseña del archivo infa_truststore.jks.

5. Ejecute el comando infasetup en cada nodo del dominio.

Si tiene varios nodos de puerta de enlace en el dominio, ejecute infasetup UpdateGatewayNode en cada nodo de puerta de enlace. Si tiene varios nodos de trabajo, ejecute infasetup UpdateWorkerNode en cada nodo de trabajo. Debe utilizar los mismos archivos de truststore y de almacén de claves para todos los nodos del dominio.

6. Reinicie el dominio.

Cuando haya actualizado todos los nodos del dominio, debe actualizar los equipos que alojan las herramientas de cliente de Informatica. Establezca la ubicación de los certificados SSL en las variables de entorno truststore de Informatica.

## Habilitar la comunicación segura para el dominio en la herramienta Administrator

La comunicación segura para el dominio se puede habilitar mediante la herramienta Administrator. Al habilitar la comunicación segura en la herramienta Administrator, también debe ejecutar los comandos `infasetup` para actualizar los nodos.

Al habilitar la opción Comunicación segura en la herramienta Administrator, también debe ejecutar el comando `infasetup` para actualizar los archivos de configuración de Informatica en cada nodo. Para especificar los archivos de certificado SSL que se van a utilizar, especifique los archivos de almacén de claves y `truststore` cuando ejecute el comando `infasetup`.

Para actualizar los archivos de configuración de Informatica de cada nodo, utilice los siguientes comandos:

### **infasetup UpdateGatewayNode**

Utilice el comando `UpdateGatewayNode` para habilitar la comunicación segura del administrador de servicios en un nodo de puerta de enlace de un dominio. Si el dominio tiene varios nodos de puerta de enlace, ejecute el comando `UpdateGatewayNode` en cada nodo de puerta de enlace.

### **infasetup UpdateWorkerNode**

Utilice el comando `UpdateWorkerNode` para habilitar la comunicación segura del administrador de servicios en un nodo de trabajo de un dominio. Si el dominio tiene varios nodos de trabajo, ejecute el comando `UpdateWorkerNode` en cada nodo de trabajo.

Para habilitar la comunicación segura del dominio desde la herramienta del administrador, realice los siguientes pasos:

1. En la herramienta Administrator, seleccione el dominio.
2. En el panel de contenido, haga clic en la vista **Propiedades**.
3. Vaya a la sección **Propiedades generales** y haga clic en **Editar**.
4. En la ventana **Editar propiedades generales**, seleccione **Habilitar la comunicación segura**.
5. Haga clic en **Aceptar**.
6. Cierre el dominio.

El dominio debe estar cerrado antes de ejecutar los comandos `infasetup`.

7. Ejecute `infasetup` con las opciones y argumentos requeridos.

Introduzca el siguiente comando:

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

Para configurar la comunicación segura de los nodos, ejecute los comandos con las siguientes opciones:

Opción	Argumento	Descripción
-EnableTLS -tls	enable_tls	Configura la comunicación segura de los servicios en el dominio de Informatica.
-NodeKeystore -nk	node_keystore_directory	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Directorio que contiene los archivos de almacén de claves. El dominio de Informatica requiere que el certificado SSL tenga el formato PEM y se encuentre en archivos Java Keystore (JKS). El directorio debe contener archivos de almacén de claves en formato PEM y JKS. Los archivos de almacén de claves deben llamarse infa_keystore.jks e infa_keystore.pem. Puede utilizar el mismo archivo de almacén de claves para varios nodos.
-NodeKeystorePass -nkp	node_keystore_password	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Contraseña del archivo infa_keystore.jks.
-NodeTruststore -nt	node_truststore_directory	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Directorio que contiene los archivos de truststore. El dominio de Informatica requiere que el certificado SSL tenga el formato PEM y se encuentre en archivos Java Keystore (JKS). El directorio debe contener archivos de truststore en formato PEM y JKS. Los archivos de truststore deben llamarse infa_truststore.jks e infa_truststore.pem. Puede utilizar el mismo archivo de truststore para varios nodos.
-NodeTruststorePass -ntp	node_truststore_password	Es opcional si utiliza el certificado SSL predeterminado de Informatica. Es obligatorio si utiliza su propio certificado SSL. Contraseña del archivo infa_truststore.jks.

8. Ejecute el comando infasetup en cada nodo del dominio.

Si tiene varios nodos de puerta de enlace en el dominio, ejecute infasetup UpdateGatewayNode en cada nodo de puerta de enlace. Si tiene varios nodos de trabajo, ejecute infasetup UpdateWorkerNode en cada nodo de trabajo. Debe utilizar los mismos archivos de truststore y de almacén de claves para todos los nodos del dominio.

9. Reinicie el dominio.

Cuando haya actualizado todos los nodos del dominio, debe actualizar los equipos que alojan las herramientas de cliente de Informatica. Establezca la ubicación de los certificados SSL en las variables de entorno truststore de Informatica.

## Configurar las aplicaciones cliente de Informatica para trabajar con un dominio seguro

Al habilitar la comunicación segura en el dominio, también se protegen las conexiones entre el dominio y las aplicaciones cliente de Informatica, como Developer tool. Puede que necesite especificar la ubicación y la contraseña de los archivos de truststore que se utilizan para proteger el dominio en las variables de entorno. Las variables de entorno se establecen en equipos que hospedan las aplicaciones cliente que acceden a servicios dentro del dominio.

Los certificados SSL que se utilizan para proteger un dominio de Informatica se encuentran en archivos truststore denominados `infa_truststore.jks` e `infa_truststore.pem`. Los archivos de truststore deben estar disponibles en cada host cliente.

Puede que necesite configurar las siguientes variables de entorno en cada host cliente:

### **INFA\_TRUSTSTORE**

Establezca esta variable en el directorio que contiene los archivos de truststore `infa_truststore.jks` e `infa_truststore.pem`.

### **INFA\_TRUSTSTORE\_PASSWORD**

Establezca esta variable en la contraseña para el archivo truststore. La contraseña debe estar cifrada. Use el programa de línea de comandos `pmpasswd` para cifrar la contraseña.

Informatica proporciona un certificado SSL en los archivos de truststore predeterminados que puede utilizar para proteger el dominio. Al instalar los clientes de Informatica, el instalador establece las variables de entorno e instala los archivos de truststore en el siguiente directorio de forma predeterminada: `<directorío de instalación de Informatica>\clients\shared\security`

Si utiliza el certificado SSL de Informatica predeterminado y los archivos `infa_truststore.jks` e `infa_truststore.pem` están en el directorio predeterminado, no es necesario establecer las variables de entorno `INFA_TRUSTSTORE` ni `INFA_TRUSTSTORE_PASSWORD`.

Debe configurar las variables de entorno `INFA_TRUSTSTORE` e `INFA_TRUSTSTORE_PASSWORD` en cada host cliente en las siguientes situaciones:

#### **Utilice un certificado SSL personalizado para proteger el dominio.**

Si proporciona un certificado SSL para utilizar a fin de proteger el dominio, importe el certificado en los archivos de truststore denominados `infa_truststore.jks` e `infa_truststore.pem` y, a continuación, copie los archivos de truststore en cada host cliente. Debe especificar la ubicación de los archivos y la contraseña de truststore.

#### **Se sustituyen los archivos de truststore predeterminados de Informatica con sus propios archivos de truststore en el directorio predeterminado.**

Si sustituye los archivos de truststore predeterminados `infa_truststore.jks` e `infa_truststore.pem` con sus propios archivos de truststore en el directorio de Informatica predeterminado, debe especificar la contraseña de truststore. Los archivos de truststore deben tener los mismos nombres de archivo que los archivos de truststore predeterminados.

#### **Se utiliza el certificado SSL de Informatica predeterminado, pero los archivos de truststore no se encuentran en el directorio de Informatica predeterminado.**

Si utiliza el certificado SSL de Informatica predeterminado, pero los archivos de truststore predeterminados `infa_truststore.jks` e `infa_truststore.pem` no están en el directorio predeterminado, debe especificar la ubicación de los archivos y la contraseña de truststore.

## Base de datos segura del repositorio de configuración del dominio

El repositorio de configuración del dominio de Informatica almacena la información de configuración y los privilegios y permisos de la cuenta de usuario. Si crea un dominio de Informatica, debe crear también un repositorio de configuración del dominio.

Puede crear un repositorio de configuración del dominio en una base de datos que está protegida con el protocolo SSL. El protocolo SSL utiliza los certificados SSL almacenados en un archivo de truststore. Acceder a la base de datos segura requiere una truststore que contenga los certificados de la base de datos.

Puede crear una base de datos segura del repositorio de configuración del dominio al instalar los servicios de Informatica y crear un dominio. Para obtener más información sobre la configuración de un repositorio de configuración del dominio seguro, consulte las guías de instalación de Informatica.

Tras la instalación, puede configurar una base de datos segura del repositorio de configuración del dominio desde la línea de comandos.

**Nota:** Antes de configurar una base de datos segura del repositorio de configuración del dominio tras la instalación, debe habilitar la comunicación segura para el dominio.

Puede crear un repositorio de configuración del dominio seguro en las siguientes bases de datos:

- Oracle
- Microsoft SQL Server
- IBM DB2

## Configurar una base de datos del repositorio de configuración del dominio segura

Tras la instalación, puede cambiar el repositorio de configuración del dominio a una base de datos segura. Únicamente puede utilizar una base de datos segura del repositorio de configuración del dominio si se habilita la comunicación segura para el dominio.

Debe cerrar el dominio antes de cambiar la base de datos del repositorio de configuración del dominio. Utilice el comando `infasetup` para realizar una copia de seguridad de la base de datos del repositorio de configuración del dominio y restaurarla en una base de datos segura. Cuando restaure el repositorio de configuración del dominio en la base de datos segura, especifique los parámetros de seguridad para la base de datos segura. A continuación, actualice el nodo de puerta de enlace con la información del repositorio de configuración del dominio.

Para realizar una copia de seguridad de la base de datos del repositorio, restaurarla y actualizar el nodo de puerta de enlace, utilice los comandos siguientes:

### **infasetup BackupDomain**

Utilice la opción `BackupDomain` para realizar una copia de seguridad de los datos de la base de datos del repositorio de configuración del dominio.

### **infasetup RestoreDomain**

Utilice la opción `RestoreDomain` para restaurar los datos del repositorio de configuración del dominio en una base de datos segura.

### **infasetup UpdateGatewayNode**

Utilice la opción `UpdateGatewayNode` para actualizar los valores del repositorio de configuración del dominio en los nodos de puerta de enlace del dominio.

Para cambiar el repositorio de configuración del dominio a una base de datos segura, complete los pasos siguientes:

1. Verifique que la comunicación segura esté habilitada para el dominio.

El dominio debe ser seguro antes de que puede usar una base de datos segura para el repositorio de configuración del dominio.

2. Cierre el dominio.

3. Ejecute el comando `infasetup BackupDomain` y especifique la información de conexión de base de datos.

Cuando ejecute el comando `BackupDomain`, `infasetup` crea una copia de seguridad de la mayoría de las tablas de la base de datos de configuración del dominio en el nombre de archivo que especifique.

**Nota:** Si se produce un error de memoria de Java al ejecutar el comando `infasetup backup` o `restore`, aumente la memoria del sistema disponible para `infasetup`. Para aumentar la memoria del sistema, configure el valor `-Xmx` en la variable de entorno `INFA_JAVA_CMD_OPTS`.

4. Use la utilidad de copia de seguridad de la base de datos para realizar una copia de seguridad manual de las tablas del repositorio adicionales que no se incluyen en la copia de seguridad del comando `infasetup`.

Realice una copia de seguridad del contenido de la tabla siguiente:

- `ISP_RUN_LOG`

5. Para restaurar el repositorio de configuración del dominio en la base de datos segura, ejecute el comando `infasetup RestoreDomain` y especifique la información de conexión de base de datos.

Además de la información de conexión, especifique las siguientes opciones, necesarias para la base de datos segura:

Opción	Argumento	Descripción
<code>-DatabaseTlsEnabled</code> <code>-dbtls</code>	<code>database_tls_enabled</code>	Obligatorio. Indica si la base de datos en la que se restaurará el repositorio de configuración del dominio es una base de datos segura. Establezca esta opción en <code>True</code> .
<code>-DatabaseTruststoreLocation</code> <code>-dbtl</code>	<code>database_truststore_location</code>	Obligatorio. Ruta de acceso y nombre del archivo de <code>truststore</code> que contiene el certificado SSL de la base de datos.
<code>-DatabaseTruststorePassword</code> <code>-dbtp</code>	<code>database_truststore_password</code>	Obligatorio. Contraseña del archivo <code>truststore</code> de base de datos para la base de datos segura.

En la cadena de conexión, incluya los siguientes parámetros de seguridad:

#### **EncryptionMethod**

Obligatorio. Indica si los datos se transmiten cifrados a través de la red. Este parámetro se debe establecer como `SSL`.

#### **ValidateServerCertificate**

Opcional. Indica si Informatica valida el certificado que ha enviado el servidor de la base de datos.

Si este parámetro está establecido como `True`, Informatica validará el certificado que envíe el servidor de la base de datos. Si especifica el parámetro `HostNameInCertificate`, Informatica también valida el nombre del host en el certificado.

Si este parámetro está establecido como False, Informatica no validará el certificado que envíe el servidor de la base de datos. Informatica omite toda la información de truststore que especifique.

El valor predeterminado es True.

#### HostNameInCertificate

Opcional. El nombre de host del equipo que aloja la base de datos segura. Si especifica un nombre de host, Informatica lo comparará con el nombre de host incluido en el certificado SSL.

#### cryptoProtocolVersion

Obligatorio. Especifica el protocolo de cifrado que debe utilizarse para conectarse a una base de datos segura. Puede establecer el parámetro en `cryptoProtocolVersion=TLSv1.1` o `cryptoProtocolVersion=TLSv1.2` según el protocolo de cifrado utilizado por el servidor de base de datos.

6. Utilice la utilidad de restauración de la base de datos para restaurar las tablas del repositorio cuyas copias de seguridad se crearon manualmente.

Restaura la tabla siguiente:

- ISP\_RUN\_LOG

7. Para actualizar los nodos del dominio con información sobre el repositorio de configuración del dominio seguro, ejecute el comando `infasetup UpdateGatewayNode` y especifique la información de conexión de base de datos segura.

Además de las opciones de nodo, especifique las siguientes opciones, necesarias para la base de datos segura:

Opción	Argumento	Descripción
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Obligatorio. Indica que la base de datos que se utiliza para el repositorio de configuración del dominio es una base de datos segura. Establezca esta opción en True.
-DatabaseConnectionString -cs	database_connection_string	Obligatorio. Cadena de conexión que se usa para conectar con la base de datos segura. La cadena de conexión debe incluir los parámetros de seguridad que incluyó en la cadena de conexión al ejecutar el comando <code>infasetup RestoreDomain</code> en el paso <a href="#">5</a>
-DatabaseTruststorePassword -dbtp	database_truststore_password	Obligatorio. Contraseña del archivo truststore de base de datos para la base de datos segura.

Si tiene varios nodos de puerta de enlace en el dominio, ejecute `infasetup UpdateGatewayNode` en cada nodo de puerta de enlace.

8. Reinicie el dominio.

## Base de datos segura del repositorio de PowerCenter

Al crear un servicio de repositorio de PowerCenter, puede crear el repositorio de PowerCenter asociado en una base de datos protegida con el protocolo SSL.

El servicio de repositorio de PowerCenter se conecta a la base de datos del repositorio de PowerCenter mediante la conectividad nativa.

Al crear un repositorio de PowerCenter en una base de datos segura, verifique que los archivos del cliente de la base de datos contienen la información de conexión segura para la base de datos. Por ejemplo, si crea un repositorio de PowerCenter en una base de datos Oracle segura, configure los archivos del cliente `tnsnames.ora` y `sqlnet.ora` de la base de datos de Oracle con la información de conexión segura.

## Base de datos segura del repositorio de modelos

Al crear un servicio de repositorio de modelos, puede crear el repositorio de modelos asociado en una base de datos protegida con el protocolo SSL.

El servicio de repositorio de modelos se conecta a la base de datos del repositorio de modelos mediante controladores de JDBC.

1. Configure una base de datos protegida con el protocolo SSL.
2. En la herramienta Administrator, cree un servicio de repositorio de modelos.
3. En el cuadro de diálogo **Nuevo servicio de repositorio de modelos**, introduzca las propiedades generales para el servicio de repositorio de modelos y haga clic en **Siguiente**.
4. Especifique las propiedades de la base de datos y la cadena de conexión JDBC para el servicio de repositorio de modelos.

Para conectarse a una base de datos segura, especifique los parámetros de la base de datos segura en el campo **Parámetros JDBC seguros**. Informatica trata el valor de **Parámetros JDBC seguros** como datos confidenciales y almacena la cadena de parámetros cifrada.

La siguiente lista describe los parámetros de base de datos segura:

### **EncryptionMethod**

Obligatorio. Indica si los datos se transmiten cifrados a través de la red. Este parámetro se debe establecer como `SSL`.

### **ValidateServerCertificate**

Opcional. Indica si Informatica valida el certificado que ha enviado el servidor de la base de datos.

Si este parámetro está establecido como `True`, Informatica validará el certificado que envíe el servidor de la base de datos. Si especifica el parámetro `HostNameInCertificate`, Informatica también valida el nombre del host en el certificado.

Si este parámetro está establecido como `False`, Informatica no validará el certificado que envíe el servidor de la base de datos. Informatica omite toda la información de truststore que especifique.

El valor predeterminado es `True`.

### **HostNameInCertificate**

Opcional. El nombre de host del equipo que aloja la base de datos segura. Si especifica un nombre de host, Informatica lo comparará con el nombre de host incluido en el certificado SSL.

### **cryptoProtocolVersion**

Obligatorio. Especifica el protocolo de cifrado que debe utilizarse para conectarse a una base de datos segura. Puede establecer el parámetro en `cryptoProtocolVersion=TLSv1.1` o `cryptoProtocolVersion=TLSv1.2` según el protocolo de cifrado utilizado por el servidor de base de datos.

### **TrustStore**

Obligatorio. Ruta de acceso y nombre del archivo de truststore que contiene el certificado SSL de la base de datos.



Si no incluye la ruta al archivo truststore, Informatica busca el archivo en el siguiente directorio predeterminado: <InformaticaInstallationDirectory>/tomcat/bin

#### **TrustStorePassword**

Obligatorio. Contraseña para el archivo truststore para la base de datos segura.

**Nota:** Informatica añade los parámetros JDBC seguros a la cadena de conexión JDBC. Si incluye los parámetros JDBC seguros directamente en la cadena de conexión, no especifique ningún parámetro en el campo **Parámetros JDBC seguros**.

5. Pruebe la conexión para verificar que la conexión a la base de datos segura del repositorio sea válida.
6. Complete el proceso para crear un servicio de repositorio de modelos.

## Comunicación segura para flujos de trabajo y sesiones

De forma predeterminada, cuando se habilita la opción de comunicación segura para el dominio, Informatica asegura la conexión entre el servicio de integración de datos y el servicio de integración de PowerCenter y los procesos DTM.

Además, si se ejecutan las sesiones de PowerCenter en una malla, es posible habilitar una opción para asegurar la comunicación de datos entre los procesos DTM.

Para habilitar la comunicación de datos segura entre procesos DTM en sesiones de PowerCenter, seleccione la opción **Habilitar el cifrado de datos** para el servicio de integración de PowerCenter.

**Nota:** Las sesiones de PowerCenter requieren más CPU y memoria cuando los procesos DTM se ejecutan en modo seguro. Antes de habilitar la comunicación de datos segura entre procesos DTM para sesiones de PowerCenter, es necesario determinar si los recursos del dominio son los adecuados para la carga adicional.

### Habilitar la comunicación segura en los procesos DTM de PowerCenter

Para asegurar la conexión entre los procesos DTM en las sesiones de PowerCenter que se ejecutan en una malla, configure el servicio de integración de PowerCenter para habilitar el cifrado de datos en procesos DTM.

1. En el navegador de la herramienta Administrator, seleccione el servicio de integración de PowerCenter.
2. En el panel de contenido, haga clic en la vista Propiedades.
3. Vaya a la sección Propiedades del servicio de integración de PowerCenter y haga clic en Editar.
4. En la ventana **Editar las propiedades del servicio de integración de PowerCenter**, seleccione **Habilitar el cifrado de datos**.
5. Haga clic en **Aceptar**.

Cuando se ejecuta una sesión de PowerCenter en una malla, los procesos DTM envían datos cifrados cuando se comunican con otros procesos DTM.

## Conexiones seguras a un servicio de aplicación web

Para proteger los datos que se transmiten entre un servicio de aplicación web y el navegador, proteja la conexión entre el servicio de aplicación web y el navegador.

Puede proteger las siguientes conexiones:

### **Conexiones con la Herramienta del administrador**

Puede proteger la conexión entre la Herramienta del administrador y el navegador.

### **Conexiones con servicios de aplicación web**

Puede proteger la conexión entre los siguientes servicios de aplicación web y el navegador:

- Servicio del analista
- Servicio de Metadata Manager
- Servicio de Test Data Manager
- Servicio de la consola del concentrador de servicios web

## **Requisitos de las conexiones seguras con servicios de aplicación web**

Antes de proteger la conexión con un servicio de aplicación web, asegúrese de que se cumplen estos requisitos:

### **Ha creado una solicitud de firma de certificado (CSR) y una clave privada.**

Puede utilizar keytool u OpenSSL para crear el CSR y la clave privada.

Si utiliza cifrado RSA, debe utilizar más de 512 bits.

### **Tiene un certificado SSL firmado.**

El certificado pueden ser autofirmado o firmado por una CA. Informatica recomienda un certificado firmado por una CA.

### **Ha importado el certificado en un almacén de claves con formato JKS.**

Un almacén de claves solo debe contener un certificado. Si utiliza un certificado único para cada servicio de aplicación web, cree un almacén de claves independiente para cada certificado. Por otro lado, puede utilizar un certificado y un almacén de claves compartido.

Si utiliza el certificado SSL generado por el programa de instalación para la Herramienta del administrador, no necesita importar el certificado en un almacén de claves con formato JKS.

### **El almacén de claves se encuentra en un directorio accesible.**

El almacén de claves debe estar en un directorio al que puedan acceder la Herramienta del administrador y los programas de la línea de comandos.

## **Habilitar conexiones seguras con la Herramienta del administrador**

Tras la instalación, puede configurar conexiones seguras con la Herramienta del administrador desde la línea de comandos.

Debe actualizar los nodos de puerta de enlace del dominio con las propiedades para una conexión segura entre el navegador y el servicio Informatica Administrator.

Para actualizar el nodo de puerta de enlace con las propiedades de conexión segura, ejecute el comando siguiente: `infasetup UpdateGatewayNode`

Incluya las siguientes opciones:

Opción	Argumento	Descripción
-HttpsPort -hs	AdminConsole_https_port	Número de puerto que se debe utilizar para una conexión segura con el servicio Informatica Administrator.
-KeystoreFile -kf	AdminConsole_Keystore_File	La ruta y el nombre de archivo del archivo de almacén de claves que se utiliza para la conexión HTTPS con el servicio de Informatica Administrator.
-KeystorePass -kp	AdminConsole_Keystore_Password	Contraseña para el archivo de almacén de claves.

Si tiene varios nodos de puerta de enlace en el dominio, ejecute el comando en cada uno de ellos.

## Servicios de aplicación web de Informatica

Configure una conexión segura para un servicio de aplicación web al crearlo o configurarlo. Cada servicio de aplicación tiene propiedades específicas para la conexión HTTPS segura.

### Seguridad de la Herramienta del analista

Al crear el Servicio del analista, puede configurar las propiedades HTTPS seguras para la Herramienta del analista.

Para asegurar la conexión entre el navegador y el Servicio del analista, configure las siguientes propiedades del Servicio del analista:

Propiedad	Descripción
Habilitar la comunicación segura	Seleccione esta propiedad para habilitar una conexión segura entre la Herramienta del analista y el Servicio del analista.
Puerto HTTPS	Número de puerto en el que se ejecuta la aplicación web de Informatica Analyst al habilitar el protocolo Seguridad de la capa de transporte (TLS). Utilice un número de puerto diferente al número de puerto HTTP.
Archivo de almacén de claves	Directorio en el que se almacena el archivo de almacén de claves que contiene los certificados digitales.
Contraseña del almacén de claves	La contraseña de texto sin formato del archivo de almacén de claves. Si no se establece esta propiedad, el Servicio del analista utiliza la contraseña predeterminada, la cual es <i>changeit</i> .
Protocolo SSL	Informatica recomienda dejar este campo vacío. La versión de TLS habilitada depende del valor. Un campo en blanco habilita la versión más alta de TLS disponible. Si especifica un valor, podría habilitarse una versión anterior de TLS. El comportamiento se basa en la versión de Java de su entorno. Para obtener más información, consulte la documentación de su versión de Java.

## Seguridad de la consola del concentrador de servicios web

Cuando cree el servicio del concentrador de servicios web, puede configurar las propiedades HTTPS seguras para la consola del concentrador de servicios web.

Para asegurar la conexión entre el navegador y el servicio del concentrador de servicios web, configure las siguientes propiedades del servicio del concentrador de servicios web:

Propiedad	Descripción
URLScheme	Indica el protocolo de seguridad que configura para el concentrador de servicios web: <ul style="list-style-type: none"><li>- HTTP. Permite ejecutar el concentrador de servicios web solo en HTTP.</li><li>- HTTPS. Permite ejecutar el concentrador de servicios web solo en HTTPS.</li><li>- HTTP y HTTPS. Permite ejecutar el concentrador de servicios web en los modos HTTP y HTTPS.</li></ul>
HubPortNumber (https)	Número de puerto del concentrador de servicios web en HTTPS. Aparece cuando el esquema URL seleccionado incluye HTTPS. Es necesario si se elige ejecutar el concentrador de servicios web en HTTPS. El valor predeterminado es 7343.
Archivo de almacén de claves	Ruta y nombre del archivo de almacén de claves que contiene las claves y los certificados que se necesitan en una conexión HTTPS.
Contraseña del almacén de claves	La contraseña para el archivo del almacén de claves. Si no se establece esta propiedad, el concentrador de servicios web utiliza la contraseña predeterminada <i>changeit</i> .

## Seguridad de Metadata Manager

Al crear el servicio de Metadata Manager, se pueden configurar las propiedades HTTPS seguras de la aplicación web de Metadata Manager.

Para asegurar la conexión entre el navegador y el servicio de Metadata Manager, configure las siguientes propiedades del servicio de Metadata Manager:

Propiedad	Descripción
Habilitar capa de conexión segura	Indica que desea configurar una conexión segura para la aplicación web de Metadata Manager. <b>Nota:</b> Esta propiedad se muestra al crear un servicio de Metadata Manager. Para proteger la conexión con un servicio de Metadata Manager existente, defina la propiedad de configuración <b>Esquema URL</b> como HTTPS.
Número de puerto	Número de puerto en el que se ejecuta la aplicación Metadata Manager. El valor predeterminado es 10250.
Archivo de almacén de claves	Archivo de almacén de claves que contiene las claves y certificados necesarios si configura una conexión segura para la aplicación web de Metadata Manager. <b>Nota:</b> El servicio de Metadata Manager utiliza cifrado RSA. Por lo tanto, Informática recomienda utilizar un certificado de seguridad generado con el algoritmo RSA.
Contraseña del almacén de claves	Contraseña para el archivo de almacén de claves.

# Conjuntos de cifrado para el dominio de Informatica

Puede configurar los conjuntos de cifrado que usa el dominio de Informatica cuando cifra las conexiones en el dominio de Informatica. Las conexiones del dominio de Informatica con los recursos externos al dominio no se verán afectadas por la configuración de los conjuntos de cifrado.

Cuando se habilitan la comunicación segura del dominio de Informatica o las conexiones seguras con los servicios de aplicación web, el dominio de Informatica utiliza conjuntos de cifrado para cifrar el tráfico.

Informatica crea la lista efectiva de conjuntos de cifrado que utiliza en función de las siguientes listas:

## **Lista negra**

La lista de conjuntos de cifrado que desea que el dominio de Informatica bloquee. Cuando se incluye un conjunto de cifrado en la lista negra, el dominio de Informatica lo elimina de la lista efectiva. Se pueden añadir conjuntos de cifrado de la lista predeterminada a la lista negra.

## **Lista predeterminada**

La lista de conjuntos de cifrado que el dominio de Informatica admite de forma predeterminada. Si no se configura una lista blanca o una lista negra, el dominio de Informatica utiliza la lista predeterminada como la lista efectiva.

Para obtener más información, consulte [Apéndice C, “Lista predeterminada de conjuntos de cifrado” en la página 260](#)

## **Lista blanca**

La lista de conjuntos de cifrado que desea que el dominio de Informatica admita. Cuando se añade un conjunto de cifrado a la lista blanca, el dominio de Informatica lo añade a la lista efectiva. No es necesario añadir conjuntos de cifrado que están en la lista predeterminada a la lista blanca.

Informatica crea la lista efectiva añadiendo los conjuntos de cifrado de la lista blanca a la lista predeterminada y quitando de la lista predeterminada los conjuntos de cifrado que aparecen en la lista negra.

Tenga en cuenta las siguientes directrices para las listas efectivas:

- Para utilizar una lista efectiva personalizada para las conexiones seguras con los clientes web, el dominio de Informatica debe usar la comunicación segura en el dominio. Si el dominio no utiliza la comunicación segura, Informatica usará la lista predeterminada como lista efectiva.
- La lista efectiva solo rige las conexiones internas del dominio de Informatica. Las conexiones con los orígenes de datos no utilizan la lista efectiva.
- La lista efectiva debe contener al menos un conjunto de cifrado compatible con TLS 1.1 o 1.2.
- La lista efectiva debe ser un conjunto de cifrado válido para Windows, Java Runtime Environment y OpenSSL.

## Configurar el dominio de Informatica para utilizar cifrado avanzado

Si desea utilizar conjuntos de cifrado avanzados que utilizan AES-256 para proporcionar un nivel de seguridad más elevado, debe sustituir los archivos de directiva de Java Cryptography Extension (JCE) que se instalan con Java Runtime Environment (JRE) en cada nodo del dominio por los archivos de directiva de JCE de fortaleza ilimitada. Los archivos de directiva de fortaleza ilimitada de JCE no contienen restricciones de fortaleza de cifrado.

1. Descargue el archivo Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8.
2. Cierre el dominio.

3. Vaya al directorio siguiente del nodo del dominio.  
`<directorio de instalación de Informatica>\java\jre\lib\security\`
4. Sustituya los siguientes archivos JAR con los archivos JAR extraídos del archivo:
  - local\_policy.jar
  - US\_export\_policy.jar
5. Reinicie el dominio.

## Creación de las listas de conjuntos de cifrado

Para configurar el dominio de Informatica para utilizar suites de cifrado específicas, cree una lista blanca que especifique las suites de cifrado adicionales que se deben admitir. También puede crear una lista negra para especificar las suites de cifrado que se deben bloquear.

Colabore con su administrador de seguridad de red para determinar los conjuntos de cifrado adecuados para el dominio de Informatica.

La lista de conjuntos de cifrado debe ser una lista separada por comas. Utilice nombres de la Autoridad para la asignación de números de Internet (IANA) para los conjuntos de cifrado de la lista. Por otro lado, puede utilizar una expresión regular de Java.

La lista blanca y la lista negra se configura con infasetup. Puede proporcionar las listas directamente en los parámetros de comando o especificar archivos de texto sin formato que contengan listas separadas por comas.

El siguiente texto de ejemplo muestra una lista con dos conjuntos de cifrado:

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Puede configurar la lista blanca y la lista negra de conjuntos de cifrado para el dominio de Informatica al crear el dominio. Utilice infasetup para crear el dominio de Informatica, los nodos de puerta de enlace y los nodos de trabajo. Para obtener más información sobre los comandos infasetup, consulte *Referencia de comando de Informatica*.

Por otra parte, puede configurar la lista blanca y la lista negra para un dominio de Informatica existente.

## Configuración del dominio de Informatica con una nueva lista efectiva de conjuntos de cifrado

Para configurar los conjuntos de cifrado que usa el dominio de Informatica, debe actualizar el dominio de Informatica, todos los nodos de puerta de enlace y todos los nodos de trabajo con la misma lista blanca y la misma lista negra.

**Nota:** Los cambios realizados en la lista negra, la lista blanca y la lista efectiva no son acumulativos. Informatica crea una nueva lista efectiva en función de la lista negra, la lista predeterminada y la lista blanca cuando se ejecuta el comando. La nueva lista efectiva sobrescribe la anterior.

Para configurar un dominio de Informatica existente con una nueva lista efectiva de conjuntos de cifrado, siga estos pasos:

1. Cierre el dominio de Informatica.
2. Opcionalmente, ejecute el comando `infasetup listDomainCiphers` para ver las listas de conjuntos de cifrado que un dominio o un nodo admite o bloquea.

Por ejemplo, ejecute el siguiente comando para ver todas las listas de conjuntos de cifrados:

```
infasetup listDomainCiphers -l ALL -dc true
```

3. Ejecute el comando `infasetup updateDomainCiphers` en un nodo de puerta de enlace y especifique una lista blanca, una lista negra o ambas.

Por ejemplo, ejecute el siguiente comando para añadir un conjunto de cifrados a la lista efectiva y quitar dos conjuntos de cifrado de esta:

```
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. Ejecute el comando `infasetup updateGatewayNode` en cada nodo de puerta de enlace y especifique una lista blanca, una lista negra o ambas.

Utilice la misma lista blanca y la misma lista negra que el dominio.

Por ejemplo, ejecute el siguiente 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. Actualice cada nodo de trabajo con el mismo grupo de conjuntos de cifrado que el dominio de Informática.

Utilice la misma lista blanca y la misma lista negra que el dominio.

Por ejemplo, ejecute el siguiente 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 el dominio de Informática.
7. Opcionalmente, ejecute el comando `infacmd isp listDomainCiphers` para ver las listas de conjuntos de cifrado que usa un dominio o un nodo.

Por ejemplo, ejecute el siguiente comando para ver la lista efectiva de conjuntos de cifrado que utiliza el dominio:

```
infacmd isp listCiphers -l EFFECTIVE -dc true
```

## Orígenes y destinos seguros

Informática utiliza objetos de conexión para conectarse a bases de datos relacionales como origen o destino. Puede crear un objeto de conexión a una base de datos relacional que esté protegida con un certificado SSL.

Los objetos de conexión de PowerCenter se crean en el administrador de flujos de trabajo. Cree las conexiones de Servicio de datos, Calidad de datos o Creación de perfiles en Developer tool o la herramienta Administrator.

Puede crear una conexión a un origen o destino seguro en las siguientes bases de datos:

- Oracle
- Microsoft SQL Server
- IBM DB2

## Orígenes y destinos del servicio de integración de datos

Cuando se crea un objeto de conexión para que el servicio de integración de datos procese asignaciones, perfiles de datos, tarjetas de puntuación o servicios de datos SQL, se puede definir una conexión a una base de datos protegida con el protocolo SSL.

El servicio de integración de datos se conecta a la base de datos de origen o destino a través de los controladores de JDBC. Al configurar la conexión a una base de datos del repositorio seguro, debe incluir los parámetros de conexión segura en la cadena de conexión JDBC.

1. Configure una base de datos protegida con el protocolo SSL para usarla como origen o destino.
2. En la herramienta Administrator, cree una conexión.
3. En el cuadro de diálogo **Nueva conexión**, seleccione el tipo de conexión y haga clic en **Aceptar**.  
Puede crear una conexión a una base de datos DB2, Microsoft SQL Server u Oracle segura.
4. En el cuadro de diálogo **Nueva conexión - Paso 1 de 3**, introduzca las propiedades para la conexión y haga clic en **Siguiente**.
5. En la página **Nueva conexión - Paso 2 de 3**, introduzca la cadena de conexión en la base de datos.

Para conectarse a una base de datos segura, especifique los parámetros de la base de datos segura en el campo **Opciones avanzadas de seguridad JDBC**. Informatica trata el valor del campo **Opciones avanzadas de seguridad JDBC** como datos confidenciales y almacena la cadena de parámetros cifrada.

La siguiente lista describe los parámetros de base de datos segura:

### **EncryptionMethod**

Obligatorio. Indica si los datos se transmiten cifrados a través de la red. Este parámetro se debe establecer como `SSL`.

### **ValidateServerCertificate**

Opcional. Indica si Informatica valida el certificado que ha enviado el servidor de la base de datos.

Si este parámetro está establecido como `True`, Informatica validará el certificado que envíe el servidor de la base de datos. Si especifica el parámetro `HostNameInCertificate`, Informatica también valida el nombre del host en el certificado.

Si este parámetro está establecido como `False`, Informatica no validará el certificado que envíe el servidor de la base de datos. Informatica omite toda la información de truststore que especifique.

El valor predeterminado es `True`.

### **HostNameInCertificate**

Opcional. El nombre de host del equipo que aloja la base de datos segura. Si especifica un nombre de host, Informatica lo comparará con el nombre de host incluido en el certificado SSL.

### **TrustStore**

Obligatorio. Ruta de acceso y nombre del archivo de truststore que contiene el certificado SSL de la base de datos.

### **TrustStorePassword**

Obligatorio. Contraseña para el archivo truststore para la base de datos segura.

**Nota:** Informatica añade los parámetros JDBC seguros a la cadena de conexión. Si incluye los parámetros JDBC seguros directamente en la cadena de conexión, no especifique ningún parámetro en el campo **Opciones avanzadas de seguridad JDBC**.

6. Pruebe la conexión para verificar que la conexión a la base de datos segura sea válida.
7. Complete el proceso para crear la conexión relacional.



## Orígenes y destinos de PowerCenter

Al crear un objeto de conexión para una sesión de PowerCenter, se puede definir una conexión a una base de datos protegida con el protocolo SSL.

Puede conectarse a los orígenes y destinos de PowerCenter relacionales mediante la conectividad nativa o los controladores ODBC.

Si se conecta a un origen o destino relacional seguro mediante la conectividad nativa, verifique que el cliente de la base de datos contenga la información de conexión de la base de datos segura. Por ejemplo, si se conecta a un destino de PowerCenter en una base de datos Oracle segura, configure el archivo del cliente de la base de datos Oracle *tnsnames.ora* con la información de conexión de la base de datos segura.

Si se conecta a un origen o destino relacional seguro mediante controladores ODBC, verifique que el cliente de la base de datos contenga la información de conexión de la base de datos segura y el origen de datos ODBC defina correctamente la conexión a la base de datos segura.

## Almacenamiento de datos seguro

Informatica cifra los datos confidenciales, como las contraseñas y los parámetros de conexión segura, antes de almacenar los datos en el repositorio de configuración del dominio. Informatica utiliza una palabra clave que se proporcione para crear una clave de cifrado con la que se cifrarán los datos confidenciales.

Durante la instalación, debe proporcionar una palabra clave que el programa de instalación utilice para generar la clave de cifrado para el dominio. Todos los nodos de un dominio deben utilizar la misma clave de cifrado. Si instala varios nodos, el programa de instalación utiliza la misma clave de cifrado para todos los nodos del dominio. Para obtener más información sobre cómo generar una clave de cifrado para el dominio durante la instalación, consulte las guías de instalación de Informatica.

Tras la instalación, puede cambiar la clave de cifrado para el dominio. Ejecute el comando `infasetup` para generar una clave de cifrado y cambiar la clave de cifrado para el dominio. Después de cambiar la clave de cifrado para el dominio, debe actualizar el contenido de los repositorios del dominio para actualizar los datos cifrados.

**Nota:** Debe conservar en una ubicación segura el nombre del dominio, la palabra clave para la clave de cifrado y el archivo de clave de cifrado. El nombre del dominio, la palabra clave y la clave de cifrado son necesarios para cambiar la clave de cifrado para el dominio o mover un repositorio a otro dominio. Si se pierde el archivo de clave de cifrado, necesitará la palabra clave para generar la clave de cifrado de nuevo. Si se pierde la palabra clave y la clave de cifrado, no podrá cambiar la clave de cifrado para el dominio ni mover un repositorio a otro dominio.

## Directorio seguro en UNIX

Al instalar Informatica, el programa de instalación crea un directorio para almacenar los archivos de Informatica que requieren acceso restringido, tales como el archivo de clave de cifrado del dominio. En UNIX, el programa de instalación asigna diferentes permisos para el directorio y los archivos del directorio.

De forma predeterminada, el programa de instalación crea el siguiente directorio en el directorio de instalación de Informatica para almacenar la clave de cifrado: `<INFA_HOME>/isp/config/keys`

El directorio `/keys` contiene el archivo de clave de cifrado del nodo. Si configura el dominio para usar la autenticación Kerberos, el directorio también contiene los archivos de tabla de claves de Kerberos.

Durante la instalación, puede especificar un directorio diferente en el que almacenar el archivo de cifrado. El programa de instalación asigna los mismos permisos al directorio especificado como directorio predeterminado.

El directorio /keys y los archivos del directorio tienen los siguientes permisos:

#### Permisos de directorios

El propietario del directorio tiene los permisos `-wx` en el directorio, pero no el permiso `r`. El propietario del directorio es la cuenta de usuario utilizada para ejecutar el programa de instalación. El grupo al que pertenece el propietario también tiene permisos `los -wx` en el directorio, pero no el permiso `r`.

Por ejemplo, la cuenta de usuario *ediqa* posee el directorio y pertenece al grupo *infaadmin*. La cuenta de usuario *ediqa* y el grupo *infaadmin* tienen los siguientes permisos: `-wx-wx---`

La cuenta de usuario *ediqa* y el grupo *infaadmin* pueden escribir en el directorio y ejecutar los archivos del directorio. No pueden mostrar la lista de archivos del directorio, pero pueden indicar un archivo específico por nombre.

Si conoce el nombre de un archivo en el directorio, puede copiar el archivo del directorio a otra ubicación. Si no conoce el nombre del archivo, deberá cambiar el permiso del directorio para que incluya el permiso de lectura antes de poder copiar el archivo. Puede utilizar el comando `chmod 730` para conceder permiso de lectura al propietario del directorio y los subdirectorios.

Por ejemplo, deberá copiar el archivo de clave de cifrado llamado *siteKey* en un directorio temporal para que sea accesible a otro nodo del dominio. Ejecute el comando `chmod 730` en el directorio `<directorio de instalación de Informatica>/isp/config` para asignar los siguientes permisos: `rw-x-wx---`. A continuación podrá copiar el archivo de clave de cifrado del subdirectorio /keys en otro directorio.

Después de terminar de copiar los archivos, vuelva a cambiar los permisos del directorio a escritura y ejecute los permisos. Puede utilizar el comando `chmod 330` para quitar el permiso de lectura.

**Nota:** No utilice la opción `-R` para cambiar recursivamente los permisos del directorio y de los archivos. El directorio y los archivos del directorio tienen permisos distintos.

#### Permisos de archivos

El propietario de los archivos del directorio tiene los permisos `rxw` en los archivos. El propietario de los archivos del directorio es la cuenta de usuario utilizada para ejecutar el programa de instalación. El grupo al que pertenece el propietario también tiene los permisos `rxw` en los archivos del directorio.

El propietario y el grupo tienen acceso total al archivo y pueden mostrar o editar el archivo en el directorio.

**Nota:** Debe conocer el nombre del archivo para poder enumerar o editar el archivo.

## Cambiar la clave de cifrado desde la línea de comandos

Después de la instalación, puede cambiar la clave de cifrado para el dominio desde la línea de comandos. Debe cerrar el dominio antes de cambiar la clave de cifrado.

Utilice el comando `infasetup` para generar una clave de cifrado y configure el dominio para utilizar la nueva clave de cifrado.

Los siguientes comandos `infasetup` generan y cambian la clave de cifrado:

#### **generateEncryptionKey**

Genera una clave de cifrado en un archivo denominado *sitekey*. Si el directorio especificado para la clave de cifrado contiene un archivo llamado *sitekey*, Informatica cambia el nombre del archivo a *siteKey\_old*.

#### **migrateEncryptionKey**

Cambia la clave de cifrado utilizada para almacenar datos confidenciales en el dominio de Informatica.

Para cambiar la clave de cifrado de un dominio, complete los pasos siguientes:

1. Cierre el dominio.
2. Cree una copia de seguridad del dominio antes de cambiar la clave de cifrado.

Para asegurarse de que puede recuperar el dominio en caso de tener problemas al cambiar la clave de cifrado, cree una copia de seguridad del dominio antes de ejecutar los comandos `infasetup`.

3. Para generar una clave de cifrado para el dominio, ejecute el comando `infasetup generateEncryptionKey`. Especifique las siguientes opciones, necesarias para generar una clave de cifrado:

Opción	Argumento	Descripción
-keyword -kw	keyword	La cadena de texto que se utiliza como palabra base a partir de la cual se genera una clave de cifrado.  La palabra clave debe cumplir los siguientes criterios: <ul style="list-style-type: none"><li>- De 8 a 20 caracteres de longitud</li><li>- Incluye, al menos, una letra mayúscula</li><li>- Incluye, al menos, una letra minúscula</li><li>- Incluye, al menos, un número</li><li>- No contiene espacios</li></ul>
-domainName -dn	domain_name	Nombre del dominio de Informática.
-encryptionKeyLocation -kl	encryption_key_location	Directorio que contiene la clave de cifrado actual. El nombre del archivo de cifrado es <i>sitekey</i> .  Informática cambia el nombre del archivo <i>sitekey</i> actual a <i>sitekey_old</i> y genera una clave de cifrado en un archivo nuevo denominado <i>sitekey</i> en el mismo directorio.

4. Para cambiar la clave de cifrado del dominio, ejecute el comando `infasetup migrateEncryptionKey` y especifique la ubicación de la clave de cifrado antigua y de la nueva.

Especifique las siguientes opciones, necesarias para cambiar la clave de cifrado del dominio:

Opción	Argumento	Descripción
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	<p>Directorio donde se almacenan el archivo con la clave de cifrado antigua, llamado <i>siteKey_old</i>, y el archivo con la clave de cifrado nueva, llamado <i>siteKey</i>.</p> <p>El directorio debe contener los archivos con la clave de cifrado antigua y la nueva. Si los archivos con la clave de cifrado antigua y la nueva se almacenan en directorios diferentes, copie los archivos con las claves de cifrado en el mismo directorio.</p> <p>Si el dominio tiene varios nodos, cualquiera de los nodos del dominio donde se ejecute el comando <code>migrateEncryptionKey</code> debe poder acceder a este directorio.</p> <p><b>Nota:</b> En UNIX, el nombre de archivo <i>siteKey_old</i> distingue entre mayúsculas y minúsculas. Si cambia el nombre del archivo de clave de cifrado anterior de forma manual, compruebe que el nombre de archivo tiene el formato de mayúsculas y minúsculas correcto.</p>
-IsDomainMigrated -mig	is_domain_migrated	<p>Indica si el dominio se ha actualizado para utilizar la clave de cifrado más reciente.</p> <p>Cuando ejecute el comando <code>migrateEncryptionKey</code> por primera vez, establezca esta opción en <code>False</code> para indicar que el dominio utiliza la clave de cifrado antigua.</p> <p>Tras la primera vez, cuando ejecute el comando <code>migrateEncryptionKey</code> para actualizar otros nodos del dominio, establezca esta opción en <code>True</code> para indicar que el dominio se ha actualizado para utilizar la clave de cifrado más reciente. O bien, puede ejecutar el comando <code>migrateEncryptionKey</code> sin esta opción.</p> <p>El valor predeterminado es <code>True</code>.</p>

- Ejecute el comando `infasetup` en cada nodo del dominio.  
Si el dominio tiene varios nodos, ejecute `infasetup migrateEncryptionKey` en cada nodo. Ejecute el comando en los nodos de puerta de enlace antes de ejecutar el comando en los nodos de trabajo. Puede omitir la opción `IsDomainMigrated` después de la primera vez que ejecute el comando.
- Reinicie el dominio.  
Debe actualizar todos los servicios de repositorio del dominio para actualizar y cifrar los datos confidenciales de los repositorios con la nueva clave de cifrado.
- Actualice todos los Servicios de repositorio de modelos, los Servicios de repositorio de PowerCenter y los Servicios de Metadata Manager.  
El Servicio de repositorio de modelos y el Servicio de repositorio de PowerCenter se pueden actualizar en la Herramienta del administrador o en la línea de comandos. El Servicio de Metadata Manager se puede actualizar en la Herramienta del administrador.

**Nota:** El Servicio de Metadata Manager debe estar deshabilitado para poder actualizarlo.

Para actualizar un servicio en la Herramienta del administrador, seleccione **Administrar > Actualizar** en el área de encabezado. Si selecciona varios servicios, la Herramienta del administrador actualizará los servicios en el orden correcto.

Para actualizar un servicio en la línea de comandos, utilice los siguientes comandos:

Tipo de servicio de repositorio	Comando
Servicio de repositorio de modelos	<code>infacmd mrs UpgradeContents</code>
Servicio de repositorio de PowerCenter	<code>pmrep Upgrade</code>

## Servicios de aplicación y puertos

Los servicios del dominio de Informatica y los servicios de aplicación del dominio de Informatica tiene puertos único.

### Dominio de Informatica

La siguiente tabla describe los puertos que se pueden definir:

Puerto	Descripción
Puerto del administrador de servicios	Número de puerto utilizado por el administrador de servicios en el nodo. El administrador de servicios detecta las solicitudes de conexión entrantes en este puerto. Las aplicaciones cliente utilizan este puerto para comunicarse con los servicios en el dominio. Los programas de la línea de comandos de Informatica utilizan este puerto para comunicarse con el dominio. Este es también el puerto para el controlador JDBC/ODBC del servicio de datos SQL. El valor predeterminado es 6006.
Puerto de cierre del administrador de servicios	El número de puerto que controla el cierre del servidor para el administrador de servicios del dominio. El administrador de servicios detecta los comandos de cierre en este puerto. El valor predeterminado es 6007.
Puerto de Informatica Administrator	Número de puerto utilizado por Informatica Administrator. El valor predeterminado es 6008.
Puerto de cierre de Informatica Administrator	Número de puerto que controla el apagado del servidor de Informatica Administrator. Informatica Administrator detecta los comandos de apagado en este puerto. El valor predeterminado es 6009.
Número de puerto mínimo	El número de puerto más bajo del intervalo de números de puerto dinámico que se pueden asignar a los procesos de servicio de aplicación que se ejecutan en este nodo. El valor predeterminado es 6014.
Número de puerto máximo	El número de puerto más alto del intervalo de números de puerto dinámico que se pueden asignar a los procesos de servicio de aplicación que se ejecutan en este nodo. El valor predeterminado es 6114.

### Servicio del analista

La siguiente tabla muestra el puerto predeterminado asociado con el servicio del analista:

Tipo	Puerto predeterminado
Servicio del analista (HTTP)	8085
Servicio del analista (HTTPS)	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio.
Servicio del analista (Base de datos de transferencia provisional)	Sin puerto predeterminado. Introduzca el número de puerto de la base de datos.

### Servicio de administración de contenido

La siguiente tabla muestra el puerto predeterminado asociado con el servicio de administración de contenido:

Tipo	Puerto predeterminado
Servicio de administración de contenido (HTTP)	8105
Servicio de administración de contenido (HTTPS)	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio.

### Servicio Data Director

La siguiente tabla muestra el puerto predeterminado asociado con el servicio Data Director:

Tipo	Puerto predeterminado
Servicio Data Director (HTTP)	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio.
Servicio Data Director (HTTPS)	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio.

### Servicio de integración de datos

La siguiente tabla muestra el puerto predeterminado asociado con el servicio de integración de datos:

Tipo	Puerto predeterminado
Servicio de integración de datos (proxy HTTP)	8085
Servicio de integración de datos (HTTP)	8095
Servicio de integración de datos (HTTPS)	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio.

Tipo	Puerto predeterminado
Base de datos de almacén de creación de perfiles	Sin puerto predeterminado. Introduzca el número de puerto de la base de datos.
Base de datos de tarea humana	Sin puerto predeterminado. Introduzca el número de puerto de la base de datos.

#### Servicio de Metadata Manager

La siguiente tabla muestra el puerto predeterminado asociado con el servicio de Metadata Manager:

Tipo	Puerto predeterminado
Servicio de Metadata Manager (HTTP)	El valor predeterminado es 10250.
Servicio de Metadata Manager (HTTPS)	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio.

#### Servicio de escucha de PowerExchange®

Use el mismo número de puerto que especificó en la instrucción SVCNODE del archivo DBMOVE.

Si especifica más de un servicio de escucha para que se ejecute en un nodo, debe definir un número de puerto SVCNODE único para cada servicio.

#### Servicio de registrador de PowerExchange

Use el mismo número de puerto que especificó en la instrucción SVCNODE del archivo DBMOVE.

Si especifica más de un servicio de escucha para que se ejecute en un nodo, debe definir un número de puerto SVCNODE único para cada servicio.

#### Servicio del concentrador de servicios web

La siguiente tabla muestra el puerto predeterminado asociado con el servicio del concentrador de servicios web:

Tipo	Puerto predeterminado
Servicio del concentrador de servicios web (HTTP)	7333
Servicio del concentrador de servicios web (HTTPS)	7343

## CAPÍTULO 6

# Inicio de sesión único para aplicaciones web de Informatica

Este capítulo incluye los siguientes temas:

- [Resumen del inicio de sesión único basado en SAML, 80](#)
- [Proceso de autenticación del inicio de sesión único basado en SAML, 80](#)
- [Experiencia de usuario de las aplicaciones web, 81](#)
- [Configuración del inicio de sesión único basado en SAML, 81](#)

## Resumen del inicio de sesión único basado en SAML

Puede configurar el inicio de sesión único (SSO) utilizando el lenguaje de marcado de aserción de seguridad (SAML) para la Herramienta del administrador, la Herramienta del analista y la Herramienta de supervisión.

El lenguaje de marcado de aserción de seguridad es un formato de datos basado en XML para intercambiar información de autenticación y autorización entre un proveedor de servicios y un proveedor de identidad. En un dominio de Informatica, la aplicación web de Informatica es el proveedor de servicios. Los servicios de federación de Microsoft Active Directory (AD FS) 2.0. son el proveedor de identidad, que autentican a los usuarios de aplicaciones web con el almacén de identidades de LDAP o Active Directory de la organización.

**Nota:** El inicio de sesión único basado en SAML no se puede utilizar en un dominio de Informatica configurado para utilizar la autenticación Kerberos.

## Proceso de autenticación del inicio de sesión único basado en SAML

Las aplicaciones web de Informatica y los servicios de federación de Active Directory intercambian información de autenticación y autorización para habilitar el inicio de sesión único en un dominio de Informatica.

Los pasos siguientes describen el flujo de autenticación básico del inicio de sesión único basado en SAML.

1. Un usuario inicia sesión en una aplicación web de Informatica.
2. La aplicación envía una solicitud de autenticación SAML a AD FS.



3. AD FS autentica las credenciales del usuario comparándolas con la información de la cuenta del usuario en el almacén de identidades de LDAP o Active Directory.
4. AD FS crea una sesión para el usuario y envía a la aplicación web un token de aserción de SAML que contiene información relacionada con la seguridad sobre el usuario.
5. La aplicación valida la aserción.

## Experiencia de usuario de las aplicaciones web

Los usuarios inician sesión en las aplicaciones web de Informatica habilitadas para utilizar el inicio de sesión único basado en SAML mediante un dominio de seguridad que contiene las cuentas de inicio de sesión único.

Al iniciar sesión en una aplicación web, el usuario selecciona el dominio de seguridad mediante el cual desea iniciar sesión en la página de inicio de sesión de la aplicación. Los usuarios habilitados para utilizar el inicio de sesión único seleccionan el dominio de seguridad de LDAP que contiene las cuentas de inicio de sesión único. A continuación, el usuario escribe su nombre de usuario y contraseña. Las credenciales se envían a AD FS en una solicitud de autenticación de SAML y, a continuación, se autentica al usuario.

Las autenticaciones subsiguientes se administran mediante las cookies de sesión establecidas en el navegador web durante la autenticación inicial. Cuando finaliza la autenticación, el usuario puede acceder a otra aplicación web de Informatica configurada para utilizar el inicio de sesión único basado en SAML en la misma sesión de navegador. Para ello, debe seleccionar el dominio de seguridad de LDAP en la página de inicio de sesión de la aplicación. El usuario no necesita proporcionar un nombre de usuario o contraseña.

Cuando finaliza la autenticación, el usuario permanece conectado a todas las aplicaciones web de Informatica que se están ejecutando en la misma sesión de navegador. Si AD FS está configurado para emitir cookies persistentes, el usuario permanece conectado después de cerrar y reiniciar el navegador.

Sin embargo, si el usuario cierra la sesión en una aplicación web de Informatica, el usuario también la cierra para el resto de aplicaciones web de Informatica que se ejecutan en la misma sesión de navegador.

Los usuarios que no están habilitados para utilizar el inicio de sesión único basado en SAML seleccionan el dominio de seguridad nativo en la página de inicio de sesión de la aplicación web y, a continuación, proporcionan el nombre de usuario y la contraseña de la cuenta nativa.

## Configuración del inicio de sesión único basado en SAML

Configure los servicios de federación de Active Directory (AD FS) y el dominio de Informatica para utilizar el inicio de sesión único basado en SAML.

Para configurar el inicio de sesión único basado en SAML para las aplicaciones web de Informatica compatibles, lleve a cabo las siguientes tareas:

1. Cree un dominio de seguridad de LDAP para las cuentas de usuario de la aplicación web de Informatica y, a continuación, importe los usuarios al dominio desde Active Directory.
2. Exporte el certificado de firma de la aserción del proveedor de identidad de AD FS.

3. Importe el certificado de firma de la aserción del proveedor de identidad al archivo de truststore predeterminado de Informatica en cada nodo de puerta de enlace del dominio.
4. Añada Informatica como relación de confianza para usuario autenticado en AD FS y asigne los atributos de LDAP a los tipos correspondientes utilizados en los tokens de seguridad emitidos por AD FS.
5. Añada la URL de cada aplicación web de Informatica a AD FS.
6. Habilite el inicio de sesión único para las aplicaciones web de Informatica dentro del dominio de Informatica.

## Antes de habilitar el inicio de sesión único

Asegúrese de que los nodos de puerta de enlace del dominio de Informatica y la red de Windows estén configurados para utilizar el inicio de sesión único.

Valide los siguientes requisitos para asegurarse de que el dominio de Informatica puede utilizar el inicio de sesión único:

**Verifique que los servicios requeridos estén implementados y configurados en la red de Windows.**

El inicio de sesión único requiere los servicios siguientes:

- Microsoft Active Directory
- Servicios de federación de Microsoft Active Directory 2.0

**Asegúrese de que los servicios de aplicaciones web de Informatica utilicen conexiones seguras HTTPS.**

De forma predeterminada, AD FS requiere que las URL de las aplicaciones web utilicen el protocolo HTTPS.

**Asegúrese de que los relojes del sistema en el host de AD FS y todos los nodos de puerta de enlace del dominio estén sincronizados.**

La vigencia de los tokens de SAML emitidos por AD FS se establece de acuerdo con el reloj del sistema del host. Asegúrese de que los relojes del sistema en el host de AD FS y todos los nodos de puerta de enlace del dominio estén sincronizados.

Para evitar problemas de autenticación, la vigencia del token de SAML emitido por AD FS es válida si la hora de inicio o de finalización definida en el token se encuentra dentro de un plazo de 120 segundos de la hora del sistema de un nodo de puerta de enlace.

## Paso 1. Crear un dominio de seguridad para las cuentas de usuario de las aplicaciones web

Cree un dominio de seguridad para las cuentas de usuario de las aplicaciones web que utilizarán el inicio de sesión único basado en SAML y, a continuación, importe la cuenta de LDAP de cada usuario de Active Directory al dominio.

Debe importar al dominio de seguridad las cuentas de LDAP para todos los usuarios que utilizan el inicio de sesión único basado en SAML para acceder a la Herramienta del administrador, la Herramienta del analista y la Herramienta de supervisión. Después de importar las cuentas al dominio, asigne las funciones, los privilegios y los permisos del dominio de Informatica pertinentes a las cuentas dentro del dominio de seguridad de LDAP.

1. En la Herramienta del administrador, haga clic en la ficha **Usuarios** y, a continuación, seleccione la vista **Seguridad**.
2. Haga clic en el menú **Acciones** y seleccione **Configuración de LDAP**.  
Se abre el cuadro de diálogo **Configuración de LDAP**.

3. Haga clic en la ficha **Conectividad de LDAP**.
4. Configure las propiedades de conexión para el servidor de Active Directory.

En la siguiente tabla se describen las propiedades de conexión del servidor:

Propiedad	Descripción
Nombre de servidor	Nombre o dirección IP del host del servidor de Active Directory.
Puerto	Puerto de escucha para el servidor. El valor predeterminado es 389.
Servicio de directorio de LDAP	Seleccione Microsoft Active Directory.
Nombre	El nombre distinguido (DN) del usuario de LDAP principal. El nombre de usuario suele estar formado por un nombre común (CN), un nombre de organización (O) y un país (C). El nombre de usuario principal es un usuario administrativo que tiene acceso al directorio. Especifique un usuario que tenga permiso para leer otras entradas de usuario en el servicio de directorio.
Contraseña	La contraseña del usuario de LDAP principal.
Usar certificado SSL	Indica que el servidor de LDAP utiliza el protocolo de capa de conexión segura (SSL). Si el servidor de LDAP utiliza SSL, debe importar el certificado a un archivo de truststore en cada nodo de puerta de enlace del dominio de Informática. También debe establecer las variables de entorno INFA_TRUSTSTORE e INFA_TRUSTSTORE_PASSWORD si no importa el certificado al truststore de Informática predeterminado.
Confiar en certificado LDAP	Determina si el administrador de servicios puede confiar en el certificado SSL del servidor de LDAP. Si selecciona esta propiedad, el administrador de servicios se conecta con el servidor de LDAP sin verificar el certificado SSL. Si no la selecciona, el administrador de servicios comprueba que el certificado SSL esté firmado por una entidad certificadora antes de conectarse con el servidor de LDAP.
No distingue entre mayúsculas y minúsculas	Indica que el Administrador de servicios no debe distinguir entre mayúsculas y minúsculas para los atributos de nombre distinguido al asignar usuarios a grupos. Habilite esta opción.
Atributo de pertenencia a grupos	Nombre del atributo que contiene información de pertenencia a grupos para un usuario. Es el atributo del objeto de grupo de LDAP que contiene los nombres distinguidos (DN) de los usuarios o grupos que son miembros de un grupo. Por ejemplo, <i>member</i> o <i>memberof</i> .
Tamaño máximo	Número máximo de cuentas de usuario que se importan a un dominio de seguridad. Si el número de usuarios para importar excede el valor de esta propiedad, el administrador de servicios genera un mensaje de error y no importa ningún usuario. Defina esta propiedad en un valor más alto si tiene muchos usuarios para importar. El valor predeterminado es 1000.

La siguiente imagen muestra los detalles de conexión para un servidor de LDAP configurado en el Panel de conectividad de LDAP del cuadro de diálogo **Configuración de LDAP**.

**LDAP Configuration** [X]

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 \*

[?]

5. Haga clic en **Probar conexión** para verificar que la conexión al servidor de Active Directory sea válida.
6. Haga clic en la ficha **Dominios de seguridad**.
7. Haga clic en **Añadir** para crear un dominio de seguridad.
8. Especifique las propiedades del dominio de seguridad.

La tabla siguiente describe las propiedades del dominio de seguridad:

Propiedad	Descripción
Dominio de seguridad	<p>Nombre del dominio de seguridad de LDAP. La distinción entre mayúsculas y minúsculas no se aplica a este nombre, el cual debe ser único dentro del dominio. El nombre no puede exceder 128 caracteres ni incluir los siguientes caracteres especiales:  , + / &lt; &gt; @ ; \ % ?</p> <p>El nombre puede contener un carácter de espacio ASCII, menos en el primer y último carácter. Los otros caracteres de espacio no están permitidos.</p>
Base de búsqueda de usuarios	<p>El nombre distinguido (DN) de la entrada que sirve de punto de inicio para buscar nombres de usuario en el servicio de directorio de LDAP. La búsqueda encuentra un objeto en el directorio de acuerdo con la ruta del nombre distinguido del objeto.</p> <p>En Active Directory, el nombre distinguido de un objeto de usuario puede ser cn=UserName,ou=OrganizationalUnit,dc=DomainName, donde la serie de nombres distinguidos relativos que denota dc=DomainName identifica el dominio DNS del objeto.</p>

Propiedad	Descripción
Filtro de usuarios	Una cadena de consulta de LDAP que especifica los criterios para buscar usuarios en Active Directory. El filtro puede especificar tipos de atributo, valores de aserción y criterios coincidentes. Para Active Directory, utilice el siguiente formato para la cadena: sAMAccountName=<cuenta>
Base de búsqueda de grupos	El nombre distinguido (DN) de la entrada que sirve de punto de inicio para buscar nombres de grupo en Active Directory.
Filtro de grupos	Una cadena de consulta de LDAP que especifica los criterios para buscar grupos en el servicio de directorio.

La siguiente imagen muestra las propiedades de un dominio de seguridad de LDAP con el nombre SAML\_USERS establecido en el panel Dominios de seguridad del cuadro de diálogo **Configuración de LDAP**. El filtro de usuarios está configurado para importar todos los usuarios que comiencen por "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

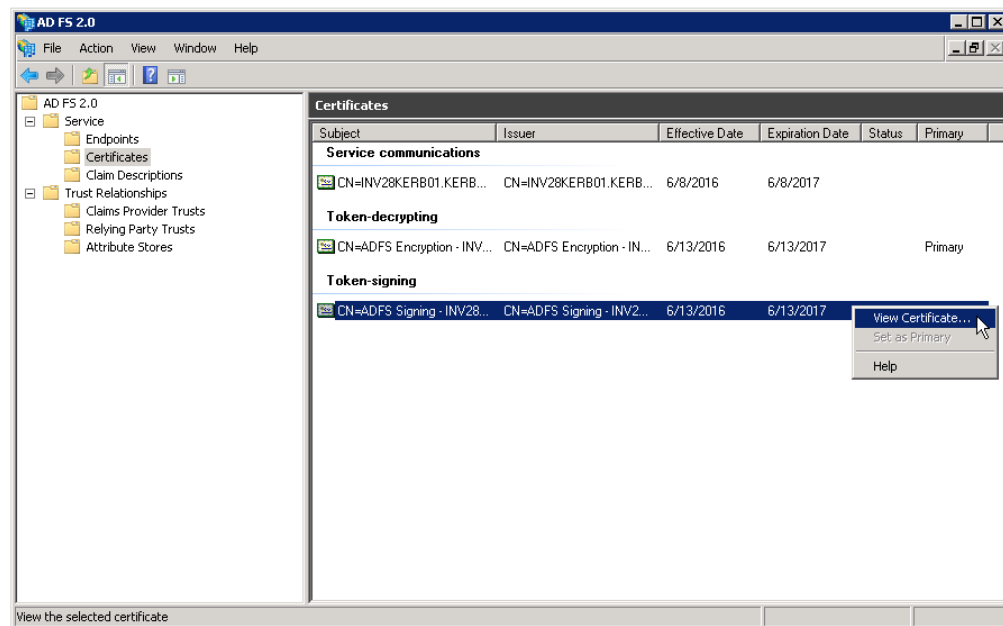
- Haga clic en **Sincronizar ahora**.  
El dominio de seguridad aparece en la vista Usuarios.
- Expanda el dominio en el Navegador para ver las cuentas de usuario importadas.
- Establezca las funciones, los privilegios y los permisos adecuados en las cuentas de usuario que accederán cada aplicación web.

## Paso 2. Exportar el certificado de AD FS

Exporte el certificado de firma de aserción de AD FS.

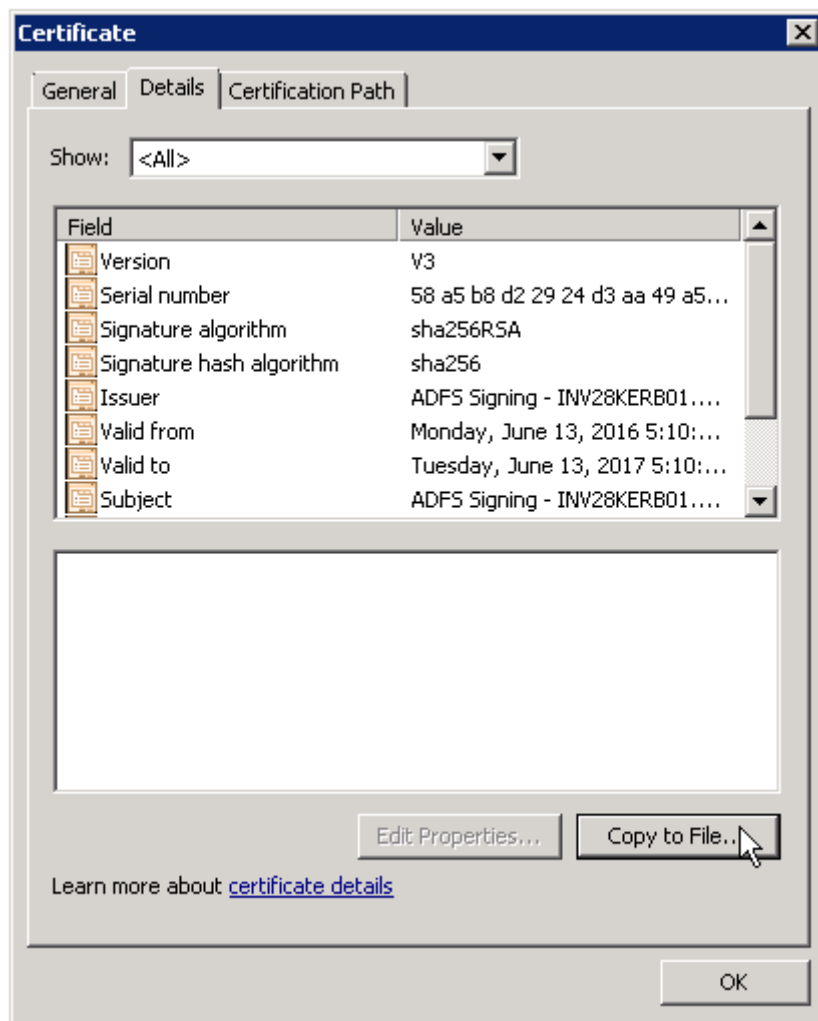
El certificado es un certificado X.509 estándar utilizado para firmar las aserciones dentro de los tokens de SAML que AD FS emite a las aplicaciones web de Informática. Puede generar un certificado de capa de sockets seguros (SSL) autofirmado para AD FS, o puede obtener un certificado de una entidad certificadora e importarlo a AD FS.

1. Inicie sesión en la consola de administración de AD FS.
2. Expanda la carpeta **Certificados > de servicio**.
3. Haga clic con el botón derecho en el certificado bajo Firma de token en el panel Certificados y, a continuación, seleccione **Ver certificado**, tal y como se muestra en la imagen siguiente:



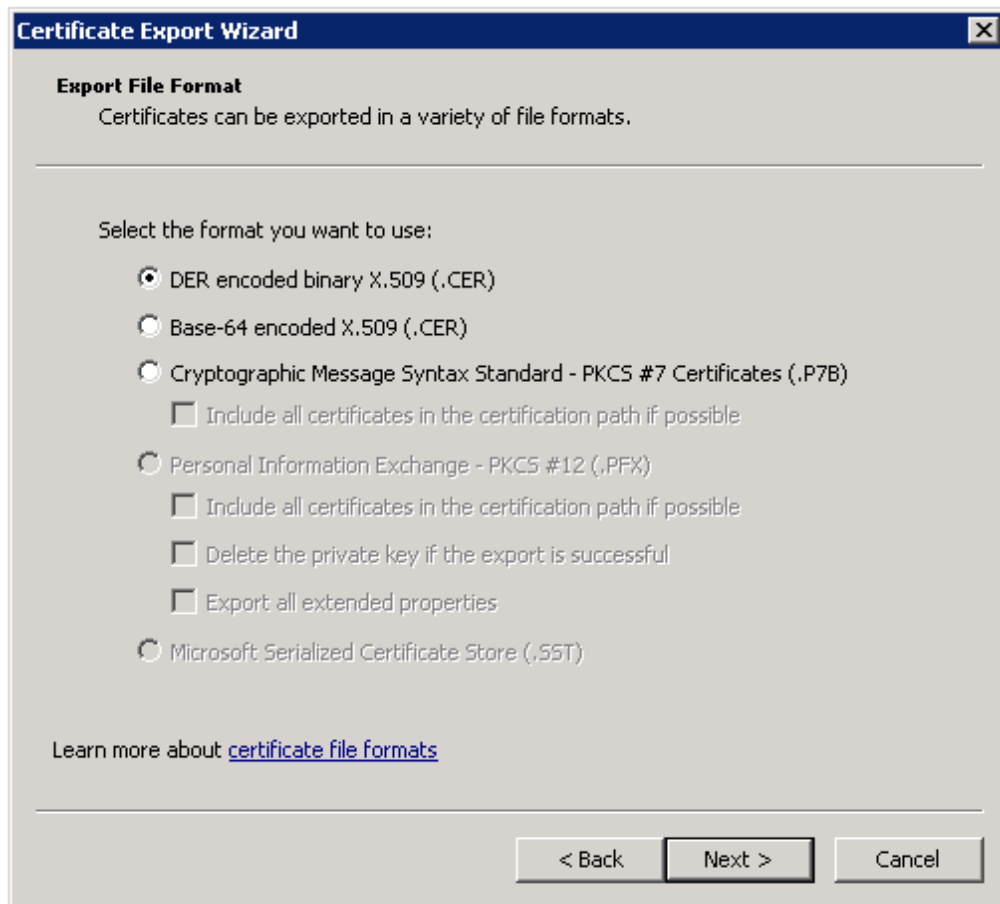
Aparece el cuadro de diálogo **Certificado**.

4. Haga clic en la ficha **Detalles** y, a continuación, haga clic en **Copiar a archivo**, tal y como se muestra en la imagen siguiente:



Aparece el **Asistente para exportación de certificados**.

5. Seleccione **DER binario codificado X.509 (.CER)** como el formato, tal y como se muestra en la imagen siguiente:



6. Haga clic en **Siguiente**.
7. Escriba el nombre del archivo de certificado y la ubicación de exportación y haga clic en **Siguiente**.
8. Haga clic en **Aceptar** y haga clic en **Finalizar** para completar la exportación.

## Paso 3. Importar el certificado al truststore de Informatica

Importe el certificado de firma de aserción al archivo de truststore de Informatica predeterminado en cada nodo de puerta de enlace dentro del dominio de Informatica.

Utilice la herramienta de administración de claves y certificados Java keytool para importar el certificado al archivo de truststore de Informatica. El archivo de truststore predeterminado, `infa_truststore.jks`, está instalado en el siguiente directorio de cada nodo:

```
<directorio de instalación de Informatica>\services\shared\security\
```

1. Copie los archivos de certificado a una carpeta local en un nodo de puerta de enlace dentro del dominio de Informatica.
2. En la línea de comandos, acceda a la ubicación de la herramienta keytool en el nodo:  

```
<directorio de instalación de Informatica>\java\jre\bin
```
3. En la línea de comandos, ejecute el siguiente comando:



```
keytool -importcert -alias <nombre del alias del certificado> -file <ruta del
certificado>\<nombre de archivo del certificado> -keystore <directorio de instalación de
Informatica>\services\shared\security\infa_truststore.jks -storepass <contraseña>
```

Tenga en cuenta que debe incluir la contraseña para el truststore predeterminado de Informatica.

4. Reinicie el nodo.

## Paso 4. Configurar los servicios de federación de Active Directory

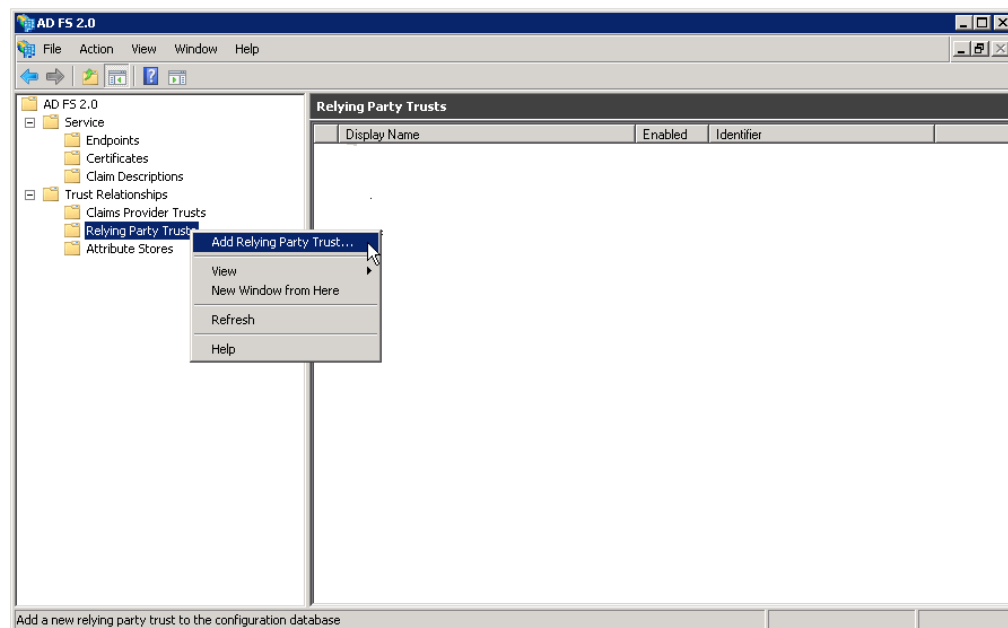
Configure AD FS para emitir tokens de SAML a las aplicaciones web de Informatica.

Utilice la consola de administración de AD FS para realizar las tareas siguientes:

- Agregar Informatica como relación de confianza para usuario autenticado en AD FS. La definición de relación de confianza para usuario autenticado permite a AD FS aceptar las solicitudes de autenticación de las aplicaciones web de Informatica.
- Edite la regla Enviar atributos LDAP como notificaciones para asignar atributos de LDAP en su almacén de identidades a los tipos correspondientes utilizados en los tokens de SAML emitidos por AD FS.

**Nota:** Todas las cadenas distinguen entre mayúsculas y minúsculas en AD FS, también las URL.

1. Inicie sesión en la consola de administración de AD FS.
2. Expanda la carpeta **Relaciones de confianza** > **Relaciones de confianza para usuario autenticado**.
3. Haga clic con el botón derecho en la carpeta **Relaciones de confianza para usuario autenticado** y seleccione **Agregar veracidad del usuario de confianza** tal y como se muestra en la imagen siguiente:

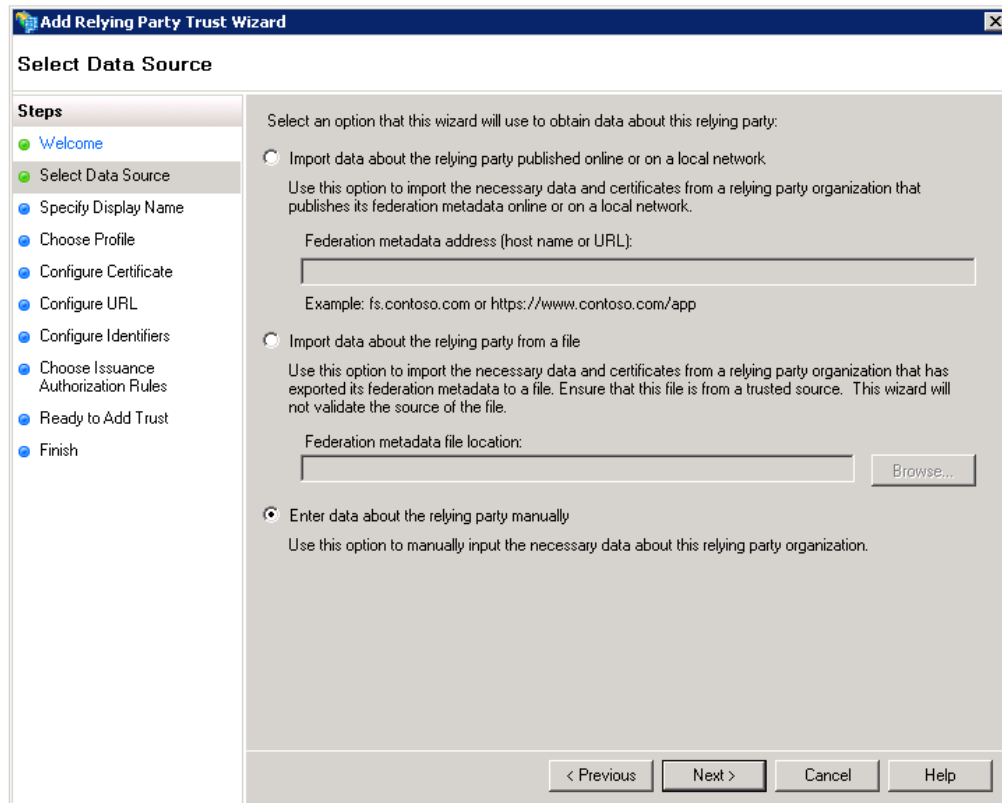


Aparece el **Asistente para agregar veracidad del usuario de confianza**.

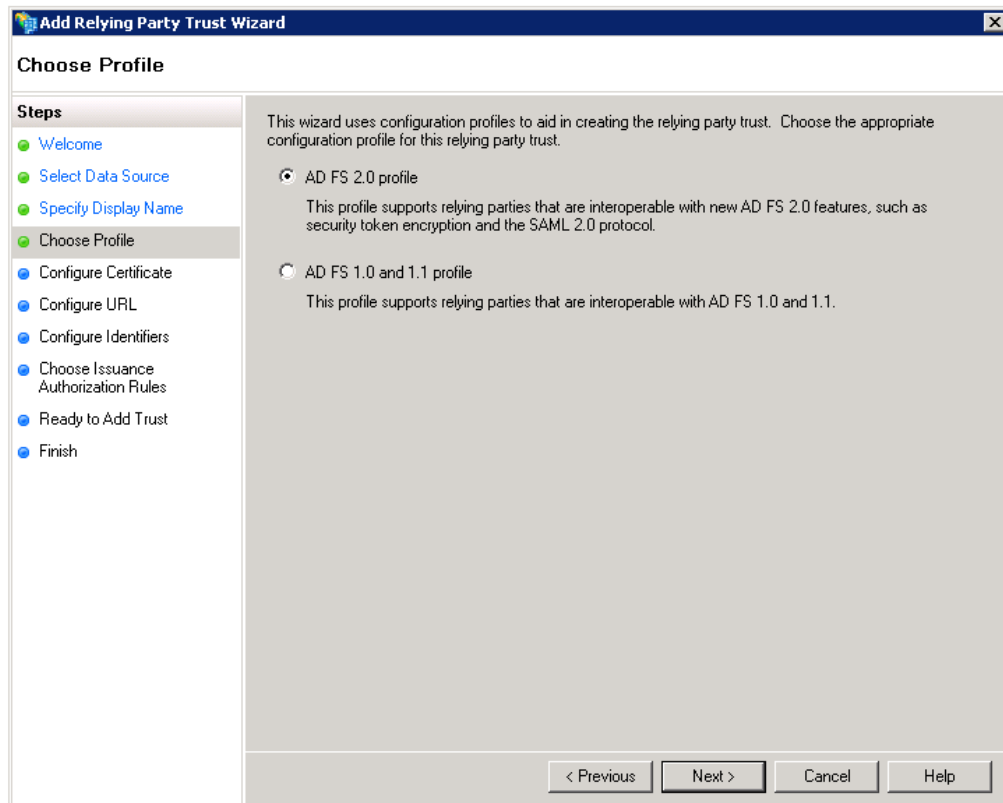
4. Haga clic en **Iniciar**.

Aparece el panel **Seleccionar origen de datos**.

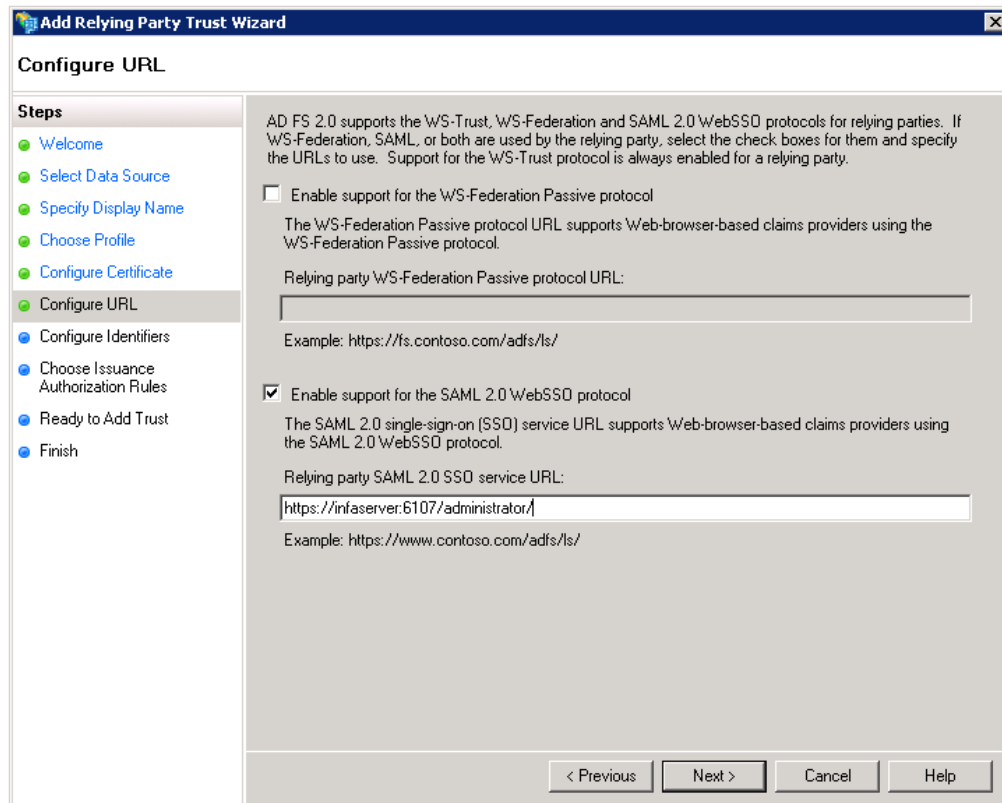
5. Haga clic en **Escribir manualmente los datos sobre el usuario de confianza** tal y como se muestra en la imagen siguiente:



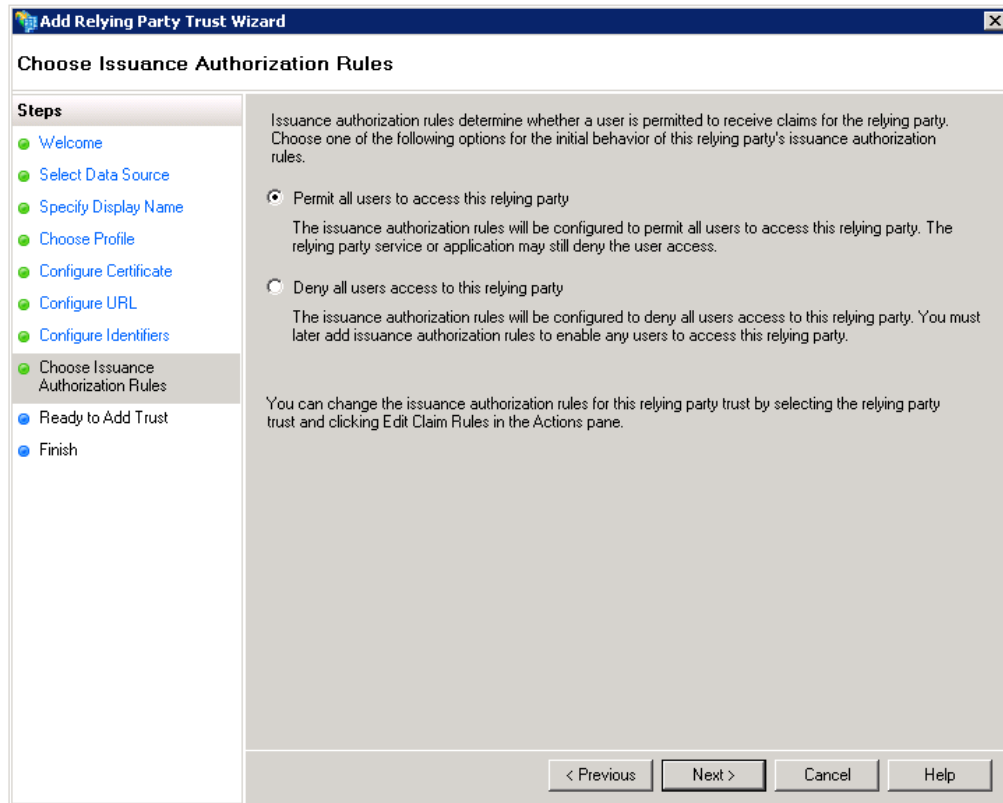
6. Haga clic en **Siguiente**
7. Escriba "Informatica" como nombre para mostrar y, a continuación, haga clic en **Siguiente**.
8. Haga clic en **Perfil de AD FS 2.0** tal y como se muestra en la imagen siguiente:



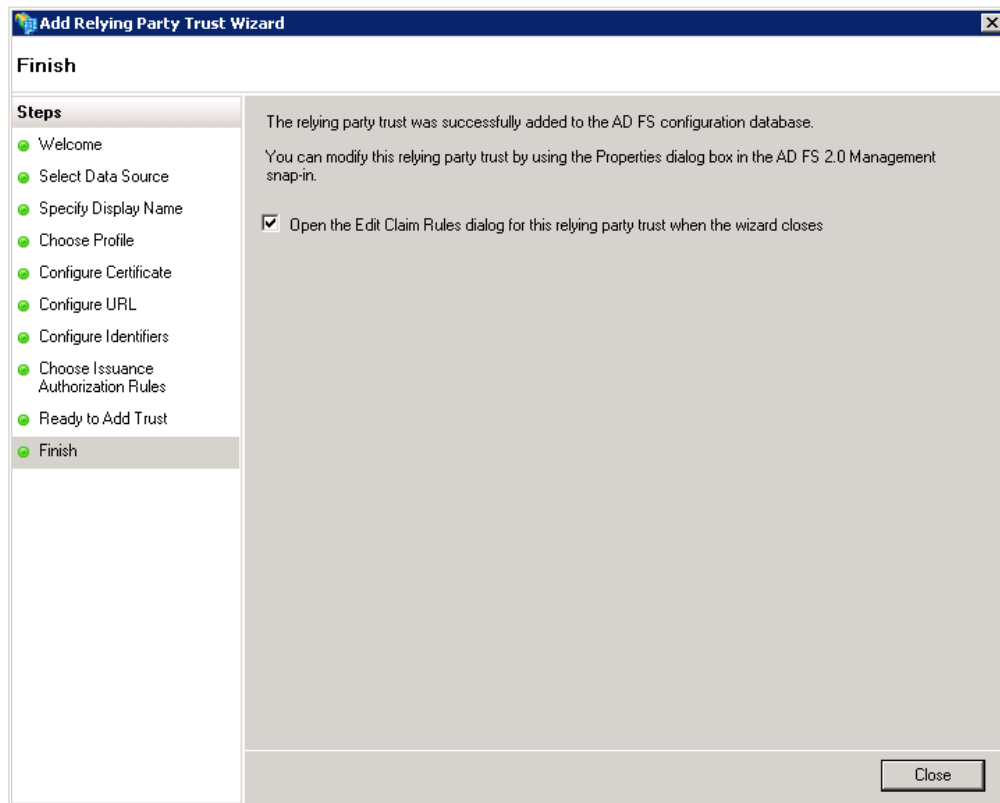
9. Haga clic en **Siguiente**.  
Omita el panel de configuración del certificado en el asistente.
10. Marque la opción **Habilitar compatibilidad con el protocolo SAML WebSSO** y escriba la URL completa de la Herramienta del administrador tal y como se muestra a continuación:



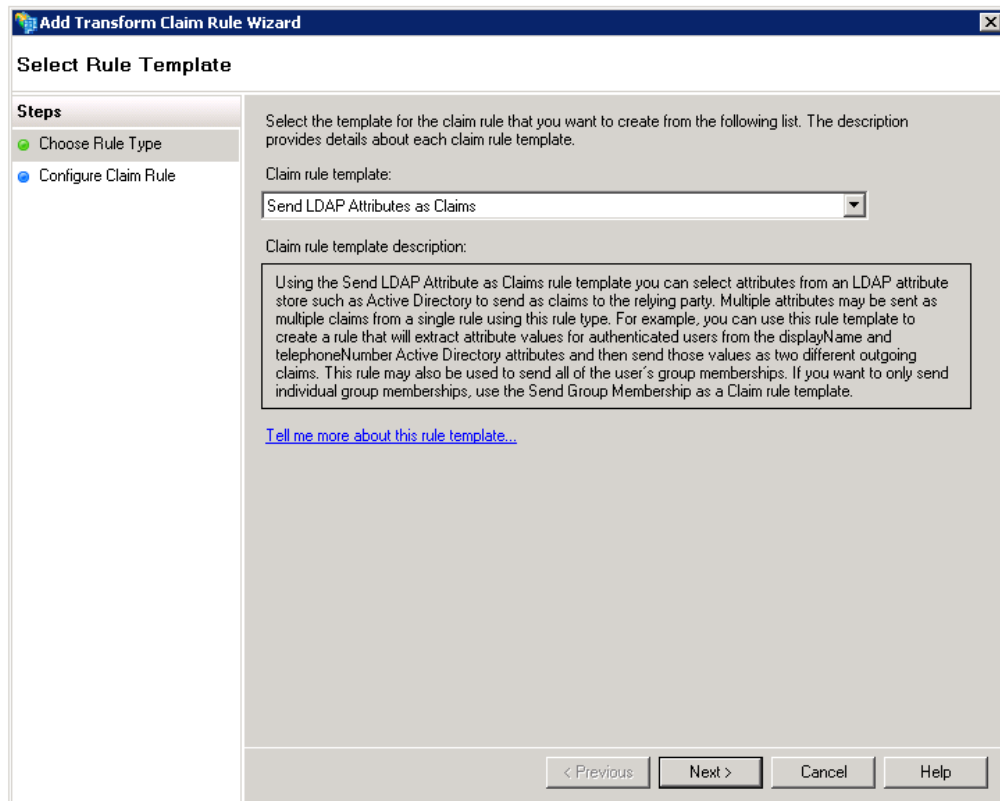
11. Haga clic en **Siguiente**.
12. Escriba "Informatica" en el campo de identificador de relación de confianza para usuario autenticado. Haga clic en **Agregar** y, a continuación, haga clic en **Siguiente**.
13. Seleccione **Permitir que todos los usuarios tengan acceso a este usuario de confianza** tal y como se muestra en la imagen siguiente:



14. Haga clic en **Siguiente**.
15. Marque la opción **Abrir el cuadro de diálogo Editar reglas de notificación para esta relación de confianza para usuario autenticado cuando el asistente se cierre** tal y como se muestra en la imagen siguiente:



16. Haga clic en **Cerrar**.  
Aparece el cuadro de diálogo **Editar reglas de notificación para Informatica**.
17. Haga clic en **Agregar regla**.  
Se abre el **Asistente para agregar regla de notificación de transformación**.
18. Seleccione **Enviar atributos LDAP como notificaciones** en el menú, tal y como se muestra en la imagen siguiente:



19. Haga clic en **Siguiente**.
20. Escriba cualquier cadena de caracteres como el nombre de la regla de notificación, como se muestra en la siguiente imagen:

**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. Seleccione Active Directory en el menú **Almacén de atributos**.
22. Seleccione Nombre de cuenta SAM en el menú **Asignación de LDAP**.
23. Escriba "username" en el campo **Tipo de notificación saliente**.
24. Haga clic en **Finalizar** y, a continuación, en **Aceptar** para cerrar el asistente.

## Paso 5. Añadir las URL de la aplicación web de Informatica a AD FS

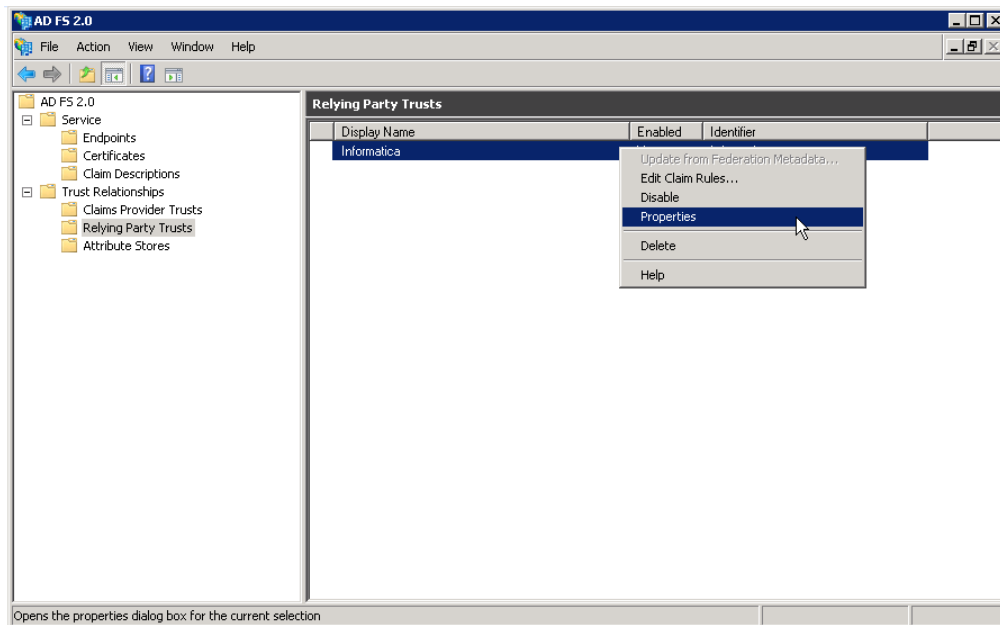
Añada la URL de cada aplicación web de Informatica que utiliza el inicio de sesión único a AD FS.

Se proporciona la URL de una aplicación web de Informatica para permitir que AD FS acepte las solicitudes de autenticación enviadas por la aplicación. Proporcionar la URL también permite a AD FS enviar el token de SAML a la aplicación tras autenticar al usuario.

No necesita añadir la URL para la Herramienta del administrador, puesto que ya la ha introducido durante la configuración de AD FS.

1. Inicie sesión en la consola de administración de AD FS.
2. Expanda la carpeta **Relaciones de confianza > Relaciones de confianza para usuario autenticado**.
3. Haga clic con el botón derecho en la entrada **Informatica** y seleccione **Propiedades**, tal y como se muestra en la imagen siguiente:



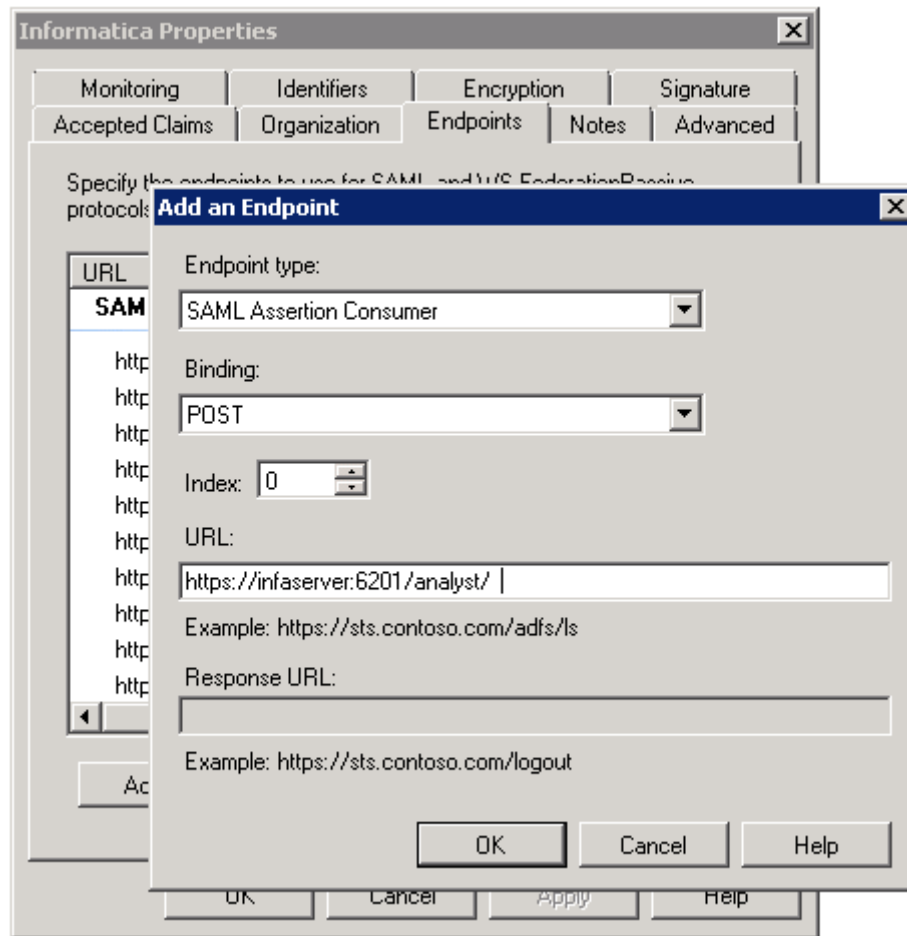


Aparece el cuadro de diálogo **Propiedades de Informatica**.

4. Haga clic en la ficha **Extremos**.

Aparece el cuadro de diálogo **Agregar un extremo**.

5. Seleccione **Consumidor de aserciones SAML** en el menú del tipo **Extremo** y, a continuación, seleccione **POST** en el menú **Enlace**, tal y como se muestra en la imagen siguiente:



6. Escriba la URL completa de una aplicación web de Informatica compatible y haga clic en **Aceptar**. Repita este procedimiento para cada aplicación web.

## Paso 6. Habilitar el inicio de sesión único basado en SAML

Puede habilitar el inicio de sesión único basado en SAML en un dominio de Informatica existente o puede habilitarlo al instalar o crear un dominio.

Seleccione una de las siguientes opciones:

### **Habilitar el inicio de sesión único al instalar los servicios de Informatica.**

Puede habilitar el inicio de sesión único basado en SAML y especificar la URL del proveedor de identidad al configurar el dominio como parte del proceso de instalación.

### **Habilitar el inicio de sesión único en un dominio existente.**

Utilice el comando `infasetup updateSamlConfig` para habilitar el inicio de sesión único en un dominio de Informatica existente. Puede ejecutar el comando en cualquier nodo de puerta de enlace dentro del dominio.

Cierre el dominio antes de ejecutar el comando.

Especifique la URL del proveedor de identidad como el valor de la opción `-iu`. En el ejemplo siguiente se muestra el uso del comando:

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

#### Habilitar el inicio de sesión único al crear un dominio.

Utilice el comando `infasetup defineDomain` para habilitar el inicio de sesión único al crear un dominio.

El ejemplo siguiente muestra las opciones de SAML como las dos últimas opciones de la línea de comandos:

```
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/
```

## Opciones del comando `infasetup`

Establezca las opciones de SAML en el comando `infasetup updateSamlConfig` para habilitar el inicio de sesión único en un dominio o en el comando `infasetup defineDomain` si crea un dominio.

La tabla siguiente describe las opciones y argumentos disponibles:

Opción	Argumento	Descripción
-EnableSaml -saml	true false	Obligatorio. Establezca este valor en true para habilitar el inicio de sesión único basado en SAML para las aplicaciones web de Informatica compatibles dentro del dominio de Informatica. Establezca este valor en false para deshabilitar el inicio de sesión único basado en SAML para las aplicaciones web de Informatica compatibles dentro del dominio de Informatica.
-IdpUrl -iu	identity_provider_url	Obligatorio si la opción -saml es true. Especifique la URL del proveedor de identidad para el dominio. Debe especificar la cadena de URL completa.

Consulte la *Referencia de comando de Informatica* para obtener instrucciones sobre el uso de los comandos `infasetup updateSamlConfig` e `infasetup defineDomain`.

## Obtener la URL del proveedor de identidad

Debe proporcionar la URL de SAML 2.0/WS-Federation para que el servidor de AD FS habilite el inicio de sesión único.

Se establece esta URL como el valor para la opción `-iu` al ejecutar el comando `infasetup updateSamlConfig` o el comando `infasetup defineDomain`. Utilice Windows PowerShell en el servidor de AD FS para obtener la URL.

1. Abra la ventana de línea de comandos de Windows PowerShell en el servidor de AD FS. Seleccione la opción Ejecutar como administrador para abrir la línea de comandos.
2. Escriba el siguiente comando en la línea de comandos de Windows PowerShell.

```
Get-ADFSEndpoint
```

3. Localice el valor FullUrl devuelto por el protocolo SAML 2.0/WS-Federation, tal y como se muestra en la imagen siguiente:

```
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

# Administración de seguridad en Informatica Administrator

Este capítulo incluye los siguientes temas:

- [Introducción al uso de Informatica Administrator, 101](#)
- [Seguridad del usuario, 102](#)
- [Ficha Seguridad, 105](#)
- [Gestión de contraseñas, 108](#)
- [Administración de seguridad de dominios, 108](#)
- [Administración de seguridad del usuario, 109](#)

## Introducción al uso de Informatica Administrator

Informatica Administrator es la herramienta que se usa para administrar el dominio y la seguridad de Informatica.

Use la Herramienta del administrador para completar los siguientes tipos de tareas:

- Tareas administrativas del dominio. Administrar registros, objetos de dominio, permisos de usuario e informes sobre el dominio. Generar y cargar diagnósticos de nodos. Supervisar trabajos y aplicaciones del servicio de integración de datos. Los objetos del dominio incluyen servicios de aplicación, nodos, mallas, carpetas, conexiones de base de datos, perfiles de sistema operativo y licencias.
- Tareas administrativas del dominio. Administrar registros, objetos de dominio y permisos de usuario. Supervisar trabajos y aplicaciones del servicio de integración de datos.
- Tareas administrativas del dominio. Administrar registros, objetos de dominio y permisos de usuario.
- Tareas administrativas de seguridad. Administrar usuarios, grupos, funciones y privilegios.

**Nota:** Si dispone de PowerCenter Express Personal Edition, no tiene acceso a las características de seguridad.

La Herramienta del administrador tiene las siguientes fichas:

- **Administrar.** Permite ver y editar las propiedades del dominio y los objetos de dicho dominio.
- **Supervisar.** Permite ver el estado de los trabajos de perfil, los trabajos de cuadros de mandos, los trabajos de vista previa, los trabajos de asignación, los servicios de datos SQL, los servicios web y los flujos de trabajo de cada servicio de integración de datos.

- **Supervisar.** Permite ver el estado de los trabajos de perfil, los trabajos de vista previa, los trabajos de asignación, los servicios de datos SQL y los servicios web de cada servicio de integración de datos.
- **Supervisar.** Permite ver el estado de los trabajos de perfil, los trabajos de vista previa, los trabajos de asignación y los flujos de trabajo para el servicio de integración de datos.
- **Supervisar.** Permite ver y supervisar implementaciones de Ultra Messaging.
- **Registros.** Permite ver los eventos de registro para el dominio y los servicios del dominio.
- **Informes.** Permite ejecutar un informe de servicios web o un informe de administración de licencias.
- **Seguridad.** Permite administrar usuarios, grupos, funciones y privilegios.
- **Seguridad.** Permite administrar usuarios, grupos, funciones y privilegios. Si dispone de PowerCenter Express Personal Edition, no tiene acceso a la ficha Seguridad.
- **Nube.** Permite ver información acerca de su organización de Informatica Cloud®.

La Herramienta del administrador tiene los siguientes elementos de encabezado:

- **Cerrar sesión.** Permite salir de la Herramienta del administrador.
- **Administrar.** Permite administrar la cuenta.
- **Ayuda.** Permite acceder a la ayuda de la ficha actual y determinar la versión de Informatica.
- **Ayuda.** Permite acceder a la ayuda de la ficha actual, determinar la versión de Informatica y configurar la directiva de uso de datos.

## Seguridad del usuario

El administrador de servicios y algunos servicios de aplicación controlan la seguridad del usuario en las aplicaciones cliente. Las aplicaciones cliente incluyen los clientes de Informatica Administrator, Informatica Analyst, Informatica Developer, Metadata Manager y PowerCenter. El administrador de servicios y algunos servicios de aplicación controlan la seguridad del usuario en las aplicaciones cliente. Las aplicaciones cliente incluyen Informatica Administrator e Informatica Developer. El administrador de servicios y algunos servicios de aplicación controlan la seguridad del usuario en las aplicaciones cliente. La aplicación cliente incluye Informatica Administrator.

El administrador de servicios y los servicios de aplicación controlan la seguridad del usuario mediante las siguientes funciones:

### Cifrado

Cuando inicie sesión en una aplicación cliente, el administrador de servicios cifrará la contraseña.

### Autenticación

Cuando inicie sesión en una aplicación cliente, el administrador de servicios autenticará la cuenta de usuario en función del nombre de usuario y contraseña del token de autenticación del usuario.

### Autorización

Cuando solicite un objeto en una aplicación cliente, el administrador de servicios y algunos servicios de aplicación autorizarán la solicitud en función de sus privilegios, funciones y permisos.

También puede usar HTTPS para la conexión segura con el dominio y los servicios de aplicación. Los siguientes servicios de aplicación proporcionan una conexión HTTPS junto con el dominio de Informatica:

- Servicio de integración de datos

- Servicio del analista
- Servicio de administración de contenido
- Servicio de Metadata Manager
- Servicio de concentrador de servicios web

También puede usar HTTPS para la conexión segura con el dominio y los servicios de aplicación. Los siguientes servicios de aplicación admiten la conexión HTTPS junto con el dominio de Informatica:

- Servicio de integración de datos
- Servicio del analista

También puede usar HTTPS para la conexión segura con el dominio y los servicios de aplicación.

## Cifrado

Informatica cifra las contraseñas enviadas por las aplicaciones cliente al administrador de servicios. Informatica emplea cifrado AES con varias claves de 128 bits para cifrar las contraseñas y guarda las contraseñas cifradas en la base de datos de configuración del dominio. Configure HTTPS para que cifre las contraseñas que las aplicaciones cliente envían al administrador de servicios.

## Autenticación

El administrador de servicios autentica a los usuarios que inician sesión en las aplicaciones cliente.

La primera vez que se inicia sesión en una aplicación cliente, se escribe un nombre de usuario, una contraseña y un dominio de seguridad. Un dominio de seguridad es un conjunto de cuentas de usuario y grupos en un dominio de Informatica.

El dominio de seguridad que seleccione determinará el método de autenticación que utilizará el administrador de servicios para autenticar la cuenta de usuario:

- Nativo. Cuando se inicia sesión en una aplicación cliente como usuario nativo, el administrador de servicios autentica el nombre de usuario y la contraseña utilizando las cuentas de usuario de la base de datos de configuración del dominio.
- Protocolo ligero de acceso a directorios (LDAP). Cuando se inicia sesión en una aplicación cliente como usuario LDAP, el administrador de servicios pasa el nombre de usuario y la contraseña al servicio de directorio LDAP externo para la autenticación.

Cuando se inicia sesión en una aplicación cliente como usuario nativo, el administrador de servicios autentica el nombre de usuario y la contraseña utilizando las cuentas de usuario de la base de datos de configuración del dominio.

Cuando se inicia sesión en una aplicación cliente como usuario nativo, el administrador de servicios autentica el nombre de usuario y la contraseña utilizando las cuentas de usuario de la base de datos de configuración del dominio.

## Inicio de sesión único

Después de iniciar sesión en una aplicación cliente, el administrador de servicios le permite iniciar otra aplicación cliente o acceder a varios repositorios dentro de la aplicación cliente. No es necesario haber iniciado sesión en la otra aplicación cliente o repositorio.

La primera vez que el administrador de servicios autentica su cuenta de usuario, crea un token de autenticación cifrado para su cuenta y devuelve el token de autenticación a la aplicación cliente. El token de autenticación contiene su nombre de usuario, el dominio de seguridad y la hora de vencimiento. El

administrador de servicios renueva el token de autenticación periódicamente antes de la hora de vencimiento.

Cuando acceda a varios repositorios dentro de una aplicación cliente, ésta enviará el token de autenticación al administrador de servicios para la autenticación del usuario.

Cuando se inicia un cliente de aplicación web desde otro, el cliente de aplicación transfiere el token de autenticación al siguiente cliente de aplicación. El siguiente cliente de aplicación web envía el token de autenticación al administrador de servicios para autenticar al usuario. Debe cerrar la sesión de cada cliente de aplicación web por separado. Por ejemplo, si abre la Herramienta del analista desde la herramienta Administrator, debe cerrar la sesión de las dos herramientas por separado.

**Nota:** Para utilizar un inicio de sesión único entre las herramientas Administrator, Analyst y Monitoring, deberá agregar sus nombres de dominio completos al archivo de host de cada nodo.

No se puede utilizar un inicio de sesión único para conectarse a un cliente de aplicación web desde una herramienta de cliente. Por ejemplo, si inicia la herramienta Administrator desde Developer tool, debe iniciar sesión en la herramienta Administrator.

## Autorización

El administrador de servicios autoriza las solicitudes de los usuarios para los objetos de dominio. Las solicitudes pueden proceder de la herramienta Administrator. Los siguientes servicios de aplicación autorizan las solicitudes de usuario para otros objetos:

- Servicio de integración de datos
- Servicio de Metadata Manager
- Servicio de repositorio de modelos
- Servicio de repositorio de PowerCenter

El administrador de servicios autoriza las solicitudes de los usuarios para los objetos de dominio. Las solicitudes pueden proceder de la herramienta Administrator. Los siguientes servicios de aplicación autorizan las solicitudes de usuario para otros objetos:

- Servicio de integración de datos
- Servicio de repositorio de modelos

Al crear usuarios y grupos nativos o al importar usuarios y grupos de LDAP, el administrador de servicios almacena la información de la base de datos de configuración del dominio en los siguientes repositorios:

- Repositorio de modelos
- Repositorio de PowerCenter
- Repositorio de PowerCenter para Metadata Manager

El administrador de servicios sincroniza la información de usuarios y grupos entre los repositorios y la base de datos de configuración del dominio cuando se producen los siguientes eventos:

- Reinicia el servicio de Metadata Manager, el servicio de repositorio de modelos o el servicio de repositorio de PowerCenter.
- Cuando añade o quita usuarios o grupos nativos.
- El administrador de servicios sincroniza la lista de usuarios y grupos de LDAP de la base de datos de configuración del dominio con la lista de usuarios y grupos del servicio de directorio de LDAP.



El administrador de servicios sincroniza la información de usuarios y grupos entre los repositorios y la base de datos de configuración del dominio cuando se producen los siguientes eventos:

- Cuando reinicia el servicio de repositorio de modelos.
- Cuando añade o quita usuarios o grupos nativos.

Al asignar permisos a usuarios y grupos en una aplicación cliente, el servicio de aplicación almacena las asignaciones de permisos junto con la información de los usuarios y grupos en el repositorio adecuado.

Al solicitar un objeto en una aplicación cliente, el servicio de aplicación apropiado autoriza su solicitud. Por ejemplo, si intenta editar un proyecto en Informatica Developer, el servicio de repositorio de modelos autoriza su solicitud en función de sus asignaciones de privilegios, funciones y permisos.

## Ficha Seguridad

La seguridad de Informatica se administra en la ficha Seguridad de la Herramienta del administrador.

La ficha Seguridad cuenta con los siguientes componentes:

- Sección de búsqueda. Busque usuarios, grupos o funciones por su nombre.
- Navegador. El navegador aparece en el panel izquierdo y muestra grupos, usuarios y funciones.
- Panel de contenido. El panel de contenido muestra propiedades y opciones según el objeto seleccionado en el navegador y la ficha seleccionada en el propio panel de contenido.
- Menú Acciones de seguridad. Contiene opciones para crear o eliminar un grupo, usuario o función. Es posible administrar LDAP y los perfiles de sistema operativo. También es posible ver los usuarios que disponen de privilegios para un servicio.

**Nota:** Si dispone de PowerCenter Express Personal Edition, no puede tener acceso a la ficha Seguridad

## Uso de la sección Buscar

Use la sección Buscar para buscar usuarios, grupos y funciones por nombre. Esta función no distingue entre mayúsculas y minúsculas.

1. En la sección Buscar, seleccione si desea buscar usuarios, grupos o funciones.
2. Indique el nombre o una parte del nombre que desee buscar.

Puede incluir un asterisco (\*) en un nombre para usar un carácter comodín en la búsqueda. Indique, por ejemplo, "ad\*" si desea buscar todos los objetos que empiecen por "ad". Indique "\*ad" si desea buscar todos los objetos que acaben en "ad".

3. Haga clic en Ir a.

Se abre la sección Resultados de búsqueda, mostrando un máximo de 100 objetos. Si la búsqueda devuelve más de 100 objetos, limite los criterios de búsqueda para ajustar los resultados.

4. Seleccione un objeto en la sección Resultados de búsqueda para visualizar información sobre el objeto en el panel Contenido.

## Uso del navegador de seguridad

El navegador se halla en el panel Contenido de la ficha Seguridad. Cuando seleccione un objeto en el navegador, el panel Contenido mostrará información sobre dicho objeto.

El navegador de la ficha Seguridad mostrará una de las siguientes secciones en función de lo que esté viendo:

- Sección Grupos. Seleccione un grupo si desea ver las propiedades del grupo y los usuarios, funciones y privilegios asignados a dicho grupo.
- Sección Usuarios. Seleccione un usuario si desea ver sus propiedades, los grupos a los que pertenece y las funciones y privilegios que tiene asignados.
- Sección Funciones. Seleccione una función para ver sus propiedades, los usuarios y grupos que tiene asignados y los privilegios asignados a la función.

El navegador ofrece diferentes formas de completar una tarea. Puede usar uno de los siguientes métodos para administrar grupos, usuarios y funciones:

- Haga clic en el menú Acciones. Cada sección del navegador incorpora un menú Acciones que permite administrar los grupos, usuarios o funciones. Seleccione un objeto en el navegador y haga clic en el menú Acciones para crear, eliminar o mover grupos, usuarios o funciones.
- Haga clic con el botón derecho en un objeto. Haga clic con el botón derecho en el navegador para mostrar las opciones disponibles para crear, eliminar y mover en el menú Acciones.
- Use los accesos directos. Use los accesos directos del teclado para desplazarse hasta diferentes secciones del navegador.

## Grupos

Un grupo es un conjunto de usuarios y grupos que pueden tener los mismos privilegios, funciones y permisos.

En la sección Grupos del navegador, los grupos se organizan en carpetas de dominio de seguridad. Un dominio de seguridad es un conjunto de cuentas de usuario y grupos en un dominio de Informática. La autenticación nativa usa el dominio de seguridad nativo, que contiene los usuarios y los grupos creados y administrados en la herramienta Administrator. La autenticación de LDAP usa los dominios de seguridad de LDAP que contienen los usuarios y grupos importados del servicio de directorio de LDAP.

En la sección Grupos del navegador, los grupos se organizan en carpetas de dominio de seguridad. Un dominio de seguridad es un conjunto de cuentas de usuario y grupos en un dominio de Informática. La autenticación nativa usa el dominio de seguridad nativo, que contiene los usuarios y los grupos creados y administrados en la herramienta Administrator.

En la sección Grupos del navegador, los grupos se organizan en carpetas de dominio de seguridad. Un dominio de seguridad es un conjunto de cuentas de usuario y grupos en un dominio de Informática. La autenticación nativa usa el dominio de seguridad nativo, que contiene los usuarios y los grupos creados y administrados en la herramienta Administrator.

Cuando seleccione una carpeta del dominio de seguridad en la sección Grupos del navegador, el panel de contenido mostrará todos los grupos que pertenezcan al dominio de seguridad. Haga clic con el botón derecho en un grupo y seleccione Navegar al elemento para mostrar los detalles del grupo en el panel de contenido.

Cuando seleccione un grupo en el navegador, el panel de contenido mostrará las fichas siguientes:

- Resumen. Muestra las propiedades generales del grupo y los usuarios asignados al grupo.
- Privilegios. Muestra los privilegios y las funciones asignados al grupo para el dominio y para los servicios de aplicación del dominio.

## Usuarios

Un usuario con una cuenta en el dominio de Informatica puede iniciar sesión en las siguientes aplicaciones cliente:

- Informatica Administrator
- Cliente de PowerCenter
- Metadata Manager
- Informatica Developer
- Informatica Analyst

Un usuario con una cuenta en el dominio de Informatica puede iniciar sesión en las siguientes aplicaciones cliente:

- Informatica Administrator
- Informatica Developer

Un usuario con una cuenta en el dominio de Informatica puede iniciar sesión en Informatica Administrator:

La sección Usuarios del navegador organiza los usuarios en carpetas de dominio de seguridad. Un dominio de seguridad es un conjunto de cuentas de usuario y grupos en un dominio de Informatica. La autenticación nativa usa el dominio de seguridad nativo, que contiene los usuarios y los grupos creados y administrados en la herramienta Administrator. La autenticación de LDAP usa los dominios de seguridad de LDAP que contienen los usuarios y grupos importados del servicio de directorio de LDAP.

La sección Usuarios del navegador organiza los usuarios en carpetas de dominio de seguridad. Un dominio de seguridad es un conjunto de cuentas de usuario y grupos en un dominio de Informatica.

La sección Usuarios del navegador organiza los usuarios en carpetas de dominio de seguridad. Un dominio de seguridad es un conjunto de cuentas de usuario y grupos en un dominio de Informatica.

Cuando seleccione una carpeta de dominio de seguridad en la sección Usuarios del navegador, el panel Contenido mostrará todos los usuarios que pertenezcan al dominio de seguridad. Haga clic con el botón derecho en un usuario y seleccione Navegar al elemento para mostrar los detalles de usuario en el panel Contenido.

Cuando seleccione un usuario en el navegador, el panel Contenido mostrará las siguientes fichas:

- Resumen. Muestra las propiedades generales del usuario y de todos los grupos a los que pertenece el usuario.
- Privilegios. Muestra los privilegios y funciones asignados al usuario para el dominio y los servicios de aplicación del dominio.

## Funciones

Una función es una recopilación de privilegios que se asignan a un usuario o grupo. Los privilegios determinan las acciones que los usuarios pueden realizar. Las funciones se asignan a usuarios y grupos para el dominio y para servicios de aplicación del dominio.

La sección Funciones del navegador organiza las funciones en las siguientes carpetas:

- Funciones definidas por el sistema. Contiene las funciones que no se pueden editar o eliminar. La función de administrador es una función definida por el sistema.
- Funciones personalizadas. Contiene las funciones que se pueden crear, editar y eliminar. Administrator Tool incluye algunas funciones personalizadas que se pueden editar y asignar a usuarios y grupos.

Cuando seleccione una carpeta en la sección Funciones del navegador, el panel de contenido mostrará todas las funciones que pertenecen a esa carpeta. Haga clic con el botón derecho en una función y seleccione Navegar al elemento para mostrar los detalles de la función en el panel de contenido.

Cuando seleccione una función en el navegador, el panel de contenido mostrará las fichas siguientes:

- **Resumen.** Muestra las propiedades generales de la función, así como los usuarios y grupos que tienen asignada esa función para el dominio y los servicios de aplicación.
- **Privilegios.** Muestra los privilegios asignados a la función para el dominio y los servicios de aplicación.

## Gestión de contraseñas

Puede cambiar la contraseña mediante la aplicación Cambiar contraseña.

Puede abrir la aplicación Cambiar contraseña desde la herramienta Administrator o accediendo a la siguiente URL: `http://<nombre de host completo>:<puerto>/passwordchange`

El administrador de servicios utiliza la contraseña de usuario asociada con un nodo de trabajo para autenticar al usuario del dominio. Si cambia una contraseña de usuario asociada a uno o varios nodos de trabajo, el administrador de servicios actualizará consecuentemente la contraseña para cada nodo de trabajo. El administrador de servicios no puede actualizar los nodos que no estén en ejecución. El administrador de servicios actualizará la contraseña de los nodos que no estén en ejecución cuando estos se reinicien.

**Nota:** Las contraseñas de las cuentas de usuario LDAP se cambian en el servicio de directorio de LDAP.

### Modificación de la contraseña

La contraseña de una cuenta de usuario nativo se puede cambiar en cualquier momento. Si el creador de la cuenta de usuario es otra persona, cambie la contraseña la primera vez que inicie sesión en Administrator Tool.

1. En el área del encabezado de Administrator Tool, haga clic en **Administrar > Cambiar contraseña**.  
La aplicación de cambio de contraseña se abre en una nueva ventana del navegador.
2. Introduzca la contraseña actual en el cuadro **Contraseña** y la nueva contraseña, en los cuadros **Nueva contraseña** y **Confirmar contraseña**.
3. Haga clic en **Actualizar**.

## Administración de seguridad de dominios

Puede configurar los componentes del dominio de Informatica para que usen el protocolo de capa de conexión segura (SSL) o el protocolo de seguridad de la capa de transporte (TLS) para cifrar las conexiones con otros componentes. Cuando habilite SSL o TLS para los componentes del dominio, se garantizará la comunicación segura.

Puede configurar la comunicación segura de varias maneras:

#### Entre servicios dentro del dominio

Puede configurar la comunicación segura entre servicios del dominio.

### Entre el dominio y componentes externos

Puede configurar la comunicación segura entre los componentes de dominio de Informatica y navegadores web o clientes de servicios web.

Cada método para configurar la comunicación segura es independiente de los otros métodos. Cuando configure la comunicación segura para un conjunto de componentes, no será necesario configurar la comunicación segura para ningún otro conjunto.

**Nota:** Si cambia un dominio seguro a un dominio no seguro, o un dominio no seguro a un dominio seguro, debe eliminar la configuración del dominio de la herramienta del desarrollador y las herramientas cliente de PowerCenter y configurar el dominio de nuevo en el cliente.

## Administración de seguridad del usuario

La seguridad del usuario se administra dentro del dominio con privilegios y permisos.

Los privilegios determinan las acciones que los usuarios pueden efectuar en aplicaciones cliente. Los permisos definen el nivel de acceso de un usuario a un objeto de dominio. Los objetos del dominio son el dominio, las carpetas, los nodos, las mallas, las licencias, las conexiones de base de datos, los perfiles del sistema operativo y los servicios de aplicación.

Los privilegios determinan las acciones que los usuarios pueden efectuar en los objetos del dominio. Los permisos definen el nivel de acceso de un usuario a un objeto de dominio. Los objetos de dominio incluyen el dominio, el nodo, la licencia, las conexiones de base de datos y los servicios de aplicación.

Aunque un usuario tenga el privilegio del dominio para completar determinadas acciones, es posible que necesite el permiso adecuado para efectuar una acción en un objeto específico. Un usuario, por ejemplo, tiene el privilegio del dominio para administrar servicios, que le concede la posibilidad de editar los servicios de aplicación. El usuario debe tener también, sin embargo, el permiso adecuado para el servicio de aplicación. Si un usuario tiene el privilegio del dominio para administrar servicios y el permiso para el servicio de repositorio de desarrollo pero no tiene el permiso para el servicio del repositorio de producción, puede editar el servicio de repositorio de desarrollo, pero no el de producción.

Aunque un usuario tenga el privilegio del dominio para completar determinadas acciones, es posible que necesite el permiso adecuado para efectuar una acción en un objeto específico.

Para iniciar sesión en la herramienta Administrator, un usuario debe tener el privilegio del dominio de acceso a Informatica Administrator. Si un usuario tiene este privilegio de acceso a Informatica Administrator y el permiso para un objeto, pero no tiene el privilegio del dominio que concede la posibilidad de modificar el tipo de objeto, el usuario sólo puede ver el objeto. Si un usuario, por ejemplo, tiene permiso para un nodo, pero no tiene el privilegio para administrar nodos y mallas, el usuario puede ver las propiedades del nodo pero no puede ni configurarlo, ni cerrarlo ni quitarlo.

Para iniciar sesión en la herramienta Administrator, un usuario debe tener el privilegio del dominio de acceso a Informatica Administrator. Si un usuario tiene este privilegio de acceso a Informatica Administrator y el permiso para un objeto, pero no tiene el privilegio del dominio que concede la posibilidad de modificar el tipo de objeto, el usuario sólo puede ver el objeto.

Si un usuario no tiene permiso para un determinado objeto del navegador, el panel Contenido muestra un mensaje que indica que se ha denegado el permiso para dicho objeto.

## CAPÍTULO 8

# Usuarios y grupos

Este capítulo incluye los siguientes temas:

- [Resumen de usuarios y grupos](#) Usuarios y grupos , 110
- [Grupos predeterminados](#), 111
- [Descripción de cuentas de usuario](#), 112
- [Administración de usuarios](#), 115
- [Administración de grupos](#), 123
- [Administración de perfiles de sistema operativo](#), 125
- [Bloqueo de cuenta](#), 133

## Resumen de usuarios y grupos

Para tener acceso a los servicios de aplicación y a los objetos del dominio de Informatica y para usar las aplicaciones cliente, debe tener una cuenta de usuario. Las tareas que puede realizar dependen del tipo de cuenta de usuario que tenga y el tipo de licencia de PowerCenter Express.

Para tener acceso a los servicios de aplicación y a los objetos del dominio de Informatica y para usar las aplicaciones cliente, debe tener una cuenta de usuario.

Durante la instalación, se crea una cuenta de usuario de administrador predeterminada. Use la cuenta de administrador predeterminada para iniciar sesión en el dominio de Informatica y administrar los servicios de aplicación, los objetos de dominio y otras cuentas de usuario. Cuando inicie sesión en el dominio de Informatica tras la instalación, cambie la contraseña para garantizar la seguridad del dominio y de las aplicaciones de Informatica.

**Nota:** Si instala PowerCenter Express Personal Edition, debe usar la cuenta de administrador predeterminada para todas las operaciones. No se pueden crear usuarios o grupos y administrar permisos.

La administración de cuentas de usuario en Informatica supone la administración de los siguientes componentes clave:

- **Usuarios.** En el dominio de Informatica, puede configurar diferentes tipos de cuentas de usuario. Los usuarios pueden efectuar tareas según las funciones, los privilegios y los permisos que tengan asignados.
- **Autenticación.** Cuando un usuario inicia sesión en un cliente de aplicación, el administrador de servicios autentica la cuenta del usuario en el dominio de Informatica y comprueba que el usuario pueda usar el cliente de aplicación. El dominio de Informatica puede usar la autenticación nativa o de LDAP para autenticar a los usuarios. El administrador de servicios organiza las cuentas de usuario y los grupos por

dominio de seguridad. Autentica a los usuarios en función del dominio de seguridad al que pertenece el usuario.

- Autenticación. Cuando un usuario inicia sesión en un cliente de aplicación, el administrador de servicios autentica la cuenta del usuario en el dominio de Informatica y comprueba que el usuario pueda usar el cliente de aplicación.
- Autenticación. Cuando un usuario inicia sesión en un cliente de aplicación, el administrador de servicios autentica la cuenta del usuario en el dominio de Informatica y comprueba que el usuario pueda usar el cliente de aplicación.
- Grupos. Puede configurar grupos de usuarios y asignar diferentes funciones, privilegios y permisos a cada grupo. Las funciones, privilegios y permisos asignados al grupo determinan las tareas que los usuarios del grupo pueden efectuar en el dominio de Informatica.
- Privilegios y funciones. Los privilegios determinan las acciones que los usuarios pueden efectuar en las aplicaciones cliente. Una función es un conjunto de privilegios que se pueden asignar a usuarios y a grupos. Los privilegios o las funciones se asignan a los usuarios, a los grupos del dominio y a los servicios de aplicación del dominio.
- Perfiles de sistema operativo. Si ejecuta el servicio de integración en UNIX o Linux, puede configurar el servicio de integración para que utilice perfiles de sistema operativo. Utilice perfiles de sistema operativo para aumentar la seguridad y aislar el entorno en tiempo de ejecución para los usuarios. Puede crear y administrar perfiles del sistema operativo en la ficha Seguridad de la Herramienta del administrador.
- Bloqueo de cuenta. Puede configurar el bloqueo de cuenta para bloquear una cuenta de usuario cuando el usuario especifica un inicio de sesión incorrecto en la Herramienta del administrador o cualquier cliente de aplicación, como Developer tool y la Herramienta del analista. También puede desbloquear una cuenta de usuario.
- Bloqueo de cuenta. Puede configurar el bloqueo de cuenta para bloquear una cuenta de usuario cuando el usuario especifica un inicio de sesión incorrecto en la Herramienta del administrador o Developer tool. También puede desbloquear una cuenta de usuario.
- Bloqueo de cuenta. Puede configurar el bloqueo de cuenta para bloquear una cuenta de usuario cuando el usuario especifica un inicio de sesión incorrecto en la Herramienta del administrador. También puede desbloquear una cuenta de usuario.

## Grupos predeterminados

El dominio de Informatica tiene un conjunto de grupos de usuarios que se han creado durante la instalación.

De forma predeterminada, el dominio de Informatica tiene los siguientes grupos de usuarios después de la instalación:

- Administrador
- Todos
- Operador

### Grupo Administrador

El dominio de Informatica incluye un grupo predeterminado llamado Administrador. La cuenta de administrador predeterminada que se crea durante la instalación pertenece a este grupo.

El grupo Administrador tiene permisos y privilegios de administrador en el dominio y en todos los servicios de la aplicación. Puede añadir usuarios o eliminarlos del grupo Administrador. Todos los usuarios del grupo

Administrador tienen los mismos permisos y privilegios que el administrador predeterminado que se crea durante la instalación.

No puede eliminar la cuenta de administrador predeterminada desde el grupo Administrador y no puede eliminar el grupo Administrador.

## Grupo Todos

El dominio de Informatica incluye un grupo predeterminado llamado Todos. Todos los usuarios del dominio pertenecen a este grupo.

De forma predeterminada, el grupo Todos no tiene ningún privilegio. Puede asignar privilegios, funciones y permisos al grupo Todos para otorgar el mismo acceso a todos los usuarios.

No se pueden realizar las siguientes tareas en el grupo Todos:

- Editar o eliminar el grupo Todos.
- Añadir o eliminar usuarios del grupo Todos.
- Mover un grupo al grupo Todos.

## Grupo Operador

El dominio de Informatica incluye un grupo predeterminado llamado Operador.

El grupo Operador tiene, de forma predeterminada, permiso en todos los objetos del dominio. Puede asignar la función Operador al grupo Operador y utilizarla para administrar los usuarios que sean operadores del dominio.

En el grupo Operador puede realizar las siguientes tareas:

- Asignar privilegios y roles al grupo.
- Añadir o eliminar usuarios del grupo.
- Mover un grupo al grupo.
- Editar o eliminar el grupo.

# Descripción de cuentas de usuario

Un dominio de Informatica puede tener los siguientes tipos de cuenta:

- Administrador predeterminado
- Administrador de dominio
- Administrador de la aplicación cliente
- Usuario

Un dominio de Informatica puede tener los siguientes tipos de cuenta:

- Administrador predeterminado
- Administrador de dominio
- Administrador de la aplicación cliente
- Usuario

El dominio de Informática tiene una cuenta de administrador predeterminada.



## Administrador predeterminado

Cuando se instalan servicios de Informática, el instalador crea el administrador predeterminado con el nombre de usuario y la contraseña proporcionados. Es posible usar la cuenta de administrador predeterminada para iniciar sesión en la herramienta Administrator de manera provisional.

El administrador predeterminado tiene permisos y privilegios de administrador en el dominio y en todos los servicios de aplicación.

El administrador predeterminado puede realizar las tareas siguientes:

- Crear, configurar y administrar todos los objetos del dominio, incluidos nodos, servicios de aplicación y cuentas de administrador y usuario.
- Configurar y administrar todos los objetos y cuentas de usuario que hayan creado otros administradores de dominio y administradores de aplicaciones cliente.
- Iniciar sesión en cualquier aplicación cliente.

El administrador predeterminado es una cuenta de usuario en el dominio de seguridad nativo. No es posible crear un administrador predeterminado. No es posible deshabilitar ni modificar el nombre de usuario ni los privilegios del administrador predeterminado. La contraseña del administrador predeterminado se puede cambiar.

## Administrador del dominio

Un administrador del dominio puede crear y administrar los objetos del dominio.

El administrador del dominio puede iniciar sesión en la herramienta Administrator y crear y configurar servicios de aplicación en el dominio. No obstante, de manera predeterminada, el administrador del dominio no puede iniciar sesión en aplicaciones cliente. El administrador predeterminado debe dar explícitamente permisos y privilegios totales de administrador del dominio a los servicios de aplicación de forma tal que estos puedan iniciar sesión y realizar tareas administrativas en las aplicaciones cliente.

El administrador del dominio puede iniciar sesión en la herramienta Administrator y configurar servicios de aplicación en el dominio. No obstante, de manera predeterminada, el administrador del dominio no puede iniciar sesión en aplicaciones cliente. El administrador predeterminado debe dar explícitamente permisos y privilegios totales de administrador del dominio a los servicios de aplicación de forma tal que estos puedan iniciar sesión y realizar tareas administrativas en las aplicaciones cliente.

Para crear un administrador del dominio, asigne a un usuario la función de administrador para un dominio.

## Administrador de la aplicación cliente

Un administrador de la aplicación cliente puede crear y administrar objetos en una aplicación cliente. Debe crear cuentas de administrador para las aplicaciones cliente. Para limitar los privilegios de administrador y preservar la seguridad de las aplicaciones cliente, cree una cuenta de administrador independiente para cada aplicación cliente.

De forma predeterminada, el administrador de la aplicación cliente no tiene permisos ni privilegios en el dominio. En caso de no tener permisos ni privilegios en el dominio, el administrador de la aplicación cliente no puede iniciar sesión en Administrator Tool para administrar el servicio de aplicación.

Puede configurar los siguientes administradores de aplicación cliente:

### **Administrador de Informática Analyst**

Tiene permisos y privilegios totales en Informática Analyst. El administrador de Informática Analyst puede iniciar sesión en Informática Analyst para crear y administrar proyectos y objetos de proyectos, y realizar todas las tareas en la aplicación cliente.

Para crear un administrador de Informatica Analyst, asigne a un usuario el rol de administrador para un servicio del analista y para el servicio de repositorio de modelos asociado.

#### **Administrador de Informatica Developer**

Tiene permisos y privilegios totales en Informatica Developer. El administrador de Informatica Developer puede iniciar sesión en Informatica Developer para crear y administrar proyectos y objetos de proyectos, y realizar todas las tareas en la aplicación cliente.

Para crear un administrador de Informatica Developer, asigne a un usuario el rol de administrador para un servicio de repositorio de modelos.

#### **Administrador de Metadata Manager**

Tiene permisos y privilegios totales en Metadata Manager. El administrador de Metadata Manager puede iniciar sesión en Metadata Manager para crear y administrar objetos de Metadata Manager y realizar todas las tareas en la aplicación cliente.

Para crear un administrador de Metadata Manager, asigne a un usuario el rol de administrador para un servicio de Metadata Manager.

#### **Administrador de Test Data**

Tiene permisos y privilegios totales en Test Data Manager. El administrador de Test Data Manager puede iniciar sesión en Test Data Manager para crear y administrar los objetos de Test Data Manager y realizar todas las tareas en el cliente de aplicación.

Para crear un administrador de Test Data, asigne a un usuario la función de administrador para un servicio de Test Data Manager.

#### **Administrador del cliente de PowerCenter**

Tiene permisos y privilegios totales en todos los objetos del cliente de PowerCenter. El administrador del cliente de PowerCenter puede iniciar sesión en el cliente de PowerCenter para administrar los objetos del repositorio de PowerCenter y realizar todas las tareas en el cliente de PowerCenter. Además, el administrador del cliente de PowerCenter puede realizar todas las tareas en los programas de línea de comandos pmrep y pmcmd.

Para crear un administrador del cliente de PowerCenter, asigne a un usuario el rol de administrador para un servicio de repositorio de PowerCenter.

## **Usuario**

Un usuario con una cuenta en el dominio de Informatica puede efectuar tareas en las aplicaciones cliente.

Por regla general, el administrador predeterminado o un administrador de dominio crea y administra las cuentas de usuario y asigna funciones, permisos y privilegios en el dominio de Informatica. Cualquier usuario con los privilegios y permisos de dominio necesarios, sin embargo, puede crear una cuenta de usuario y asignar funciones, permisos y privilegios.

Los usuarios pueden efectuar tareas en las aplicaciones cliente según las funciones, privilegios y permisos que tengan asignados.

# Administración de usuarios

Es posible crear, editar y eliminar usuarios en el dominio de seguridad nativo. No puede eliminar ni modificar las propiedades de las cuentas de usuario en los dominios de seguridad de LDAP. No puede modificar las asignaciones de usuarios a grupos de LDAP.

Puede crear, editar y eliminar usuarios según el tipo de licencia de PowerCenter Express. Puede asignar funciones, permisos y privilegios a una cuenta de usuario. Las funciones, los permisos y los privilegios asignados al usuario determinan las tareas que el usuario puede realizar en el dominio de Informatica. Si dispone de PowerCenter Express Personal Edition, no puede crear usuarios o grupos. Debe utilizar el usuario predeterminado de Administrator para realizar todas las tareas.

Puede crear, editar y eliminar usuarios según el tipo de licencia. Puede asignar funciones, permisos y privilegios a una cuenta de usuario. Las funciones, los permisos y los privilegios asignados al usuario determinan las tareas que el usuario puede realizar en el dominio de Informatica.

Puede asignar funciones, permisos y privilegios a una cuenta de usuario en el dominio de seguridad nativo o en un dominio de seguridad de LDAP. Las funciones, los permisos y los privilegios asignados al usuario determinan las tareas que el usuario puede realizar en el dominio de Informatica.

También puede desbloquear una cuenta de usuario.

## Cómo crear usuarios nativos

En la ficha Seguridad, puede añadir, editar o eliminar usuarios nativos.

1. En la herramienta Administrator, haga clic en la ficha Seguridad.
2. En el menú Acciones de seguridad, haga clic en Crear usuario.
3. Introduzca la siguiente información para el usuario:

Propiedad	Descripción
Nombre de inicio de sesión	El nombre de inicio de sesión de la cuenta de usuario. El nombre de inicio de sesión de una cuenta de usuario debe ser único dentro del dominio de seguridad al que pertenece. La distinción entre mayúsculas y minúsculas no se aplica al nombre, el cual no puede contener más de 128 caracteres. Además, este nombre no puede incluir tabulaciones, caracteres de nueva línea ni los siguientes caracteres especiales: , + " \ < > ; / * % ? & El nombre puede incluir un carácter de espacio ASCII siempre y cuando no sea el primer y último carácter. Los otros caracteres de espacio no están permitidos.
Contraseña	La contraseña de la cuenta de usuario. La contraseña puede contener entre 1 y 80 caracteres.
Confirmar contraseña	Vuelva a especificar la contraseña para confirmarla. Es necesario que vuelva a introducir la contraseña. No copie y pegue la contraseña.
Nombre completo	El nombre completo de la cuenta de usuario. El nombre completo no puede incluir los siguientes caracteres especiales: < > "

Propiedad	Descripción
Descripción	La descripción de la cuenta de usuario. La descripción no puede exceder 765 caracteres ni incluir los siguientes caracteres especiales: < > "
Correo electrónico	Dirección de correo electrónico del usuario. La dirección de correo electrónico no puede incluir los siguientes caracteres especiales: < > " Escriba la dirección de correo electrónico con el formato NombreUsuario@Dominio.
Teléfono	El número de teléfono del usuario. El número de teléfono no puede incluir los siguientes caracteres especiales: < > "

- Haga clic en Aceptar para guardar la cuenta de usuario.

Después de crear una cuenta de usuario, en el panel de detalles aparecen las propiedades de la cuenta de usuario y los grupos a los que está asignado el usuario.

## Cómo editar las propiedades generales de usuarios nativos

No puede cambiar el nombre que un usuario nativo emplea para iniciar sesión. Sí puede cambiar la contraseña y otros detalles de la cuenta de un usuario nativo.

- En Administrator Tool, haga clic en la ficha Seguridad.
- En la sección Usuarios del navegador, seleccione una cuenta de usuario nativo y haga clic en Editar.
- Para cambiar la contraseña, seleccione Cambiar contraseña.  
En la ficha Seguridad, aparecen vacíos los campos Contraseña y Confirmar contraseña.
- Escriba una nueva contraseña y confirme.
- Puede modificar el nombre completo, la descripción, el correo electrónico y el teléfono según sea necesario.
- Haga clic en Aceptar para aplicar los cambios.

## Asignar usuarios nativos a grupos nativos

Asigne usuarios nativos a grupos nativos en la ficha Seguridad.

- En Administrator Tool, haga clic en la ficha Seguridad.
- En la sección Usuarios del navegador, seleccione una cuenta de usuario nativo y haga clic en **Editar**.
- Haga clic en la ficha Grupos.
- Para asignar un usuario nativo a un grupo, seleccione un nombre de grupo en la columna Todos los grupos y haga clic en **Añadir**.

Si no se muestran los grupos anidados en la columna Todos los grupos, expanda cada grupo para mostrar todos los grupos anidados.

Puede asignar un usuario nativo a más de un grupo. Use la tecla Ctrl o Mayús para seleccionar varios grupos al mismo tiempo.

- Para quitar un usuario nativo de un grupo, seleccione un grupo en la columna Grupos asignados y haga clic en **Quitar**.

6. Haga clic en **Aceptar** para guardar las asignaciones de grupos.

## Asignar usuarios de LDAP a grupos nativos

Puede asignar cuentas de usuario de LDAP a grupos nativos. No puede cambiar la asignación de las cuentas de usuario de LDAP a los grupos de LDAP.

1. En Administrator Tool, haga clic en la ficha Seguridad.
2. En la sección Grupos del navegador, seleccione un grupo nativo y haga clic en Editar.
3. Haga clic en la ficha Usuarios.
4. Para asignar un usuario de LDAP a un grupo, seleccione un usuario de LDAP en la columna Todos los usuarios y haga clic en Añadir.
5. Para quitar un usuario de LDAP de un grupo, seleccione un usuario de LDAP en la columna Usuarios asignados y haga clic en Quitar.
6. Haga clic en Aceptar para guardar las asignaciones de usuarios.

## Cómo habilitar y deshabilitar cuentas de usuario

Los usuarios con cuentas activas pueden iniciar sesión en las aplicaciones cliente y realizar tareas en función de sus permisos y privilegios. Si no desea que los usuarios accedan a las aplicaciones cliente temporalmente, puede deshabilitar sus cuentas. Puede habilitar o deshabilitar las cuentas de usuario en un dominio de seguridad nativo o de LDAP. Cuando deshabilite una cuenta de usuario, éste no podrá iniciar sesión en las aplicaciones cliente.

Los usuarios con cuentas activas pueden iniciar sesión en las aplicaciones cliente y realizar tareas en función de sus permisos y privilegios. Si no desea que los usuarios accedan a las aplicaciones cliente temporalmente, puede deshabilitar sus cuentas. Cuando deshabilite una cuenta de usuario, éste no podrá iniciar sesión en las aplicaciones cliente.

Para deshabilitar una cuenta de usuario, selecciónela en la sección Usuarios del navegador y haga clic en Deshabilitar. Cuando seleccione una cuenta de usuario deshabilitada, la ficha Seguridad mostrará un mensaje para indicar que la cuenta de usuario está deshabilitada. Cuando una cuenta de usuario está deshabilitada, el botón Habilitar estará disponible. Para habilitar la cuenta de usuario, haga clic en Habilitar.

La cuenta de administrador predeterminada no se puede deshabilitar.

**Nota:** Cuando el administrador del servicio importa una cuenta de usuario desde el servicio de directorio de LDAP, no importa el atributo LDAP que indica si una cuenta de usuario está habilitada o deshabilitada. El administrador del servicio importa todas las cuentas de usuario como habilitadas. Debe deshabilitar una cuenta de usuario LDAP en la herramienta Administrator si no desea que el usuario acceda a las aplicaciones cliente. Durante la posterior sincronización con el servidor LDAP, la cuenta de usuario conserva el estado habilitado o deshabilitado establecido en la herramienta Administrator.

## Cómo eliminar usuarios nativos

Para eliminar una cuenta de usuario nativo, haga clic con el botón derecho sobre el nombre de la cuenta de usuario, en la sección Usuarios del navegador, y seleccione Eliminar usuario. Confirme que desea eliminar la cuenta de usuario.

No se puede eliminar la cuenta del administrador predeterminado. Si inicia sesión en Administrator Tool, no puede eliminar su propia cuenta de usuario.

## Cómo eliminar usuarios de PowerCenter

Si elimina un usuario que posee objetos en el repositorio de PowerCenter, estará eliminando toda propiedad que el usuario tenga sobre carpetas, objetos de conexión, grupos de implementación, etiquetas o consultas. Después de eliminar un usuario, el administrador predeterminado se convierte en el propietario de todos los objetos que pertenecían al usuario eliminado.

Si revisa el historial de un objeto con versiones que antes perteneció a un usuario eliminado, verá el nombre del usuario eliminado acompañado de la palabra "eliminado".

## Cómo eliminar usuarios de Metadata Manager

Si elimina un usuario que posee accesos directos y carpetas, Metadata Manager mueve la carpeta personal del usuario a una carpeta llamada Usuarios eliminados, perteneciente al administrador predeterminado. La carpeta personal del usuario eliminado contiene todos los accesos directos y carpetas creados por ese usuario. Todas las carpetas compartidas seguirán estando compartidas después de que elimine al usuario.

Si la carpeta Usuarios eliminados contiene una carpeta con el mismo nombre de usuario, Metadata Manager cambia el nombre de la carpeta adicional por "Copia (n) de <username>".

## Usuarios de LDAP

No es posible añadir, editar ni eliminar usuarios de LDAP en Administrator Tool. Debe administrar las cuentas de usuario de LDAP en el servicio de directorio de LDAP.

## Cómo desbloquear una cuenta de usuario

El administrador del dominio puede desbloquear una cuenta de usuario que está bloqueada fuera del dominio. Si el usuario es un usuario nativo, el administrador puede solicitar que el usuario restablezca su contraseña antes de volver a registrarse en el dominio.

El usuario debe tener una dirección de correo electrónico válida configurada en el dominio para recibir notificaciones cuando se restablece la contraseña de su cuenta.

Si el usuario está bloqueado del servidor de autenticación de LDAP, el administrador de LDAP debe desbloquear la cuenta de usuario en el servidor de LDAP.

1. En la herramienta Administrator, haga clic en la ficha **Seguridad**.
2. Haga clic en **Administración de cuentas**.

La página Administración de cuentas muestra las siguientes listas de usuarios bloqueados:

### **Usuarios nativos bloqueados**

Incluye las cuentas de usuario del dominio de seguridad nativo que están bloqueadas.

### **Usuarios LDAP bloqueados**

Incluye las cuentas de usuario de los dominios de seguridad de LDAP que están bloqueadas.

3. Seleccione los usuarios que desea desbloquear.
4. Seleccione **Desbloquear el usuario y restablecer la contraseña** para generar una nueva contraseña para el usuario después de desbloquear la cuenta.  
El usuario recibe la nueva contraseña en un correo electrónico.
5. Haga clic en el botón **Desbloquear usuarios seleccionados**.

## Cómo aumentar la memoria del sistema para un gran número de usuarios

El tiempo de procesamiento para el reinicio de un dominio de Informatica, la sincronización de usuarios LDAP y algunos comandos infacmd e infasetup aumenta proporcionalmente según el número de usuarios en el dominio de Informatica.

El número de usuarios influye en el tiempo de procesamiento de los siguientes comandos:

- infasetup BackupDomain, DeleteDomain y RestoreDomain
- infacmd isp ExportDomainObjects, ExportUsersandGroups, ImportDomainObjects e ImportUsersandGroups
- infacmd oie ExportObjects e ImportObjects

Tal vez deba aumentar la memoria del sistema que utilizan los servicios de Informatica, infasetup e infacmd cuando tenga un gran número de usuarios en el dominio. Para aumentar el tamaño de heap máximo, configure las siguientes variables de entorno y especifique el valor en megabytes:

- INFA\_JAVA\_OPTS. Determina el tamaño de heap máximo utilizado por Informatica Services. Configure las variables en cada nodo donde se instalan los servicios de Informatica.
- ICMD\_JAVA\_OPTS. Determina el tamaño de heap máximo utilizado por infacmd. Configure las variables en cada equipo donde ejecuta infacmd.
- INFA\_JAVA\_CMD\_OPTS. Determina el tamaño de heap máximo utilizado por infasetup. Configure las variables en cada equipo donde ejecuta infasetup.

Por ejemplo, para configurar 2.048 MB de memoria de sistema en UNIX para la variable de entorno INFA\_JAVA\_OPTS, utilice el siguiente comando:

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

En Windows, configure las variables como variables del sistema.

La siguiente tabla muestra los requisitos mínimos para la configuración del tamaño máximo del montón, en función del número de usuarios y servicios del dominio:

Número de usuarios del dominio	Tamaño máximo del montón (de 1 a 5 servicios)	Tamaño máximo del montón (de 6 a 10 servicios)
1.000 o menos	512 MB (predeterminado)	1.024 MB
5.000	2.048 MB	3.072 MB
10.000	3.072 MB	5.120 MB
20.000	5.120 MB	6.144 MB
30.000	5.120 MB	6.144 MB

**Nota:** La configuración máxima de tamaño de heap que aparece en la tabla se basa en el número de servicios de aplicación del dominio.

Después de configurar estas variables del entorno, reinicie el nodo para que los cambios tengan efecto.

## Visualización de la actividad del usuario

Utilice el comando `infacmd isp getUserActivityLog` o la ficha Registros de la herramienta del administrador para ver registros de actividad del usuario. Consulte los eventos de registro de actividad del usuario para determinar el momento en el que un usuario ha creado, actualizado o quitado servicios, nodos, usuarios, grupos o funciones.

Ejecute el siguiente comando para ver los eventos de registro de actividad del usuario de todos los usuarios:

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

El comando requiere que tenga asignada la función de administrador o que pertenezca al grupo Administrador.

Puede ver los eventos de registro con base en los siguientes filtros opcionales:

- Nombre de usuario
- Dominio de seguridad
- Fecha y hora
- Orden cronológico
- Código de actividad
- Texto de actividad

Puede mostrar los eventos de registro en la línea de comandos o escribirlos en un archivo de uno de los siguientes formatos:

- Binario
- Texto
- XML

Si imprime un registro en formato binario, puede utilizar el comando `infacmd isp convertUserActivityLog` para convertirlo en texto o en formato XML.

Para obtener más información sobre los registros de actividad del usuario y la ficha Registros de la herramienta del administrador, consulte *Guía del Informatica Administrator*.

## Filtros de registros de actividad del usuario

Utilice uno o varios filtros para recuperar eventos de registro de usuarios, fechas o eventos específicos.

Utilice uno o más de los parámetros siguientes del comando `infacmd isp getUserActivityLog` para filtrar eventos de registro:

### Usuarios y dominios de seguridad

Opcional. La lista de usuarios de los que desea obtener eventos de registro. Utilice un espacio para separar varios usuarios. Utilice el carácter comodín (\*) para ver los registros de varios usuarios en uno o en todos los dominios de seguridad. Por ejemplo, las siguientes cadenas son valores válidos de la opción:

```
user:Native
"user:*"
"user*"
"*_users *"
"*:Native"
```

Añada el siguiente parámetro al comando `getUserActivityLog` para filtrar los eventos de registro por usuario o dominio de seguridad:

```
-usrs <UserName>:<SecurityDomain>
```



Por ejemplo, puede añadir el siguiente parámetro para recuperar la actividad del usuario de un usuario llamado User1 en todos los dominios de seguridad:

```
-usrs "User1:*
```

### Fecha y hora

Opcional. El intervalo de fechas para el que desea consultar eventos de registro.

Si especifica una fecha de finalización anterior a la fecha de inicio, el comando no devuelve ningún evento de registro.

Introduzca la fecha y hora con uno de los formatos siguientes:

- MM/dd/aaaa
- MM/dd/aaaa HH:mm:ss
- aaaa-MM-dd
- aaaa-MM-dd HH:mm:ss

Añada el siguiente parámetro al comando getUserActivityLog para filtrar los registros por fecha de inicio o de finalización:

```
-sd <start_date> -ed <end_date>
```

Por ejemplo, puede añadir el siguiente parámetro para recuperar la actividad del usuario entre el 1 de enero de 2014 y el 3 febrero de 2014:

```
-sd 01/01/2014 -ed 02/03/2014
```

### Código de actividad

Opcional. Devuelve eventos de registro con base en el código de actividad.

Utilice el carácter comodín (\*) para recuperar eventos de registro de varios códigos de actividad. Entre los códigos de actividad válidos se incluyen:

- CCM\_10437. Indica que una actividad se ha realizado correctamente.
- CCM\_10438. Indica que no se ha podido realizar una actividad.

Añada el siguiente parámetro al comando getUserActivityLog para filtrar por código de actividad:

```
-ac <activity_code>
```

Por ejemplo, puede añadir el siguiente parámetro para recuperar eventos de registro que se han realizado correctamente:

```
-ac CCM_10437
```

Si utiliza el carácter comodín, escriba el argumento entre comillas.

### Texto de actividad

Opcional. Devuelve eventos de registro con base en una cadena en el texto de la actividad.

Añada el siguiente parámetro al comando getUserActivityLog para filtrar por texto de actividad:

```
-atxt <activity_text>
```

Utilice el carácter comodín (\*) para recuperar registros de varios eventos. Por ejemplo, el siguiente parámetro devuelve todos los eventos de registro cuya descripción contiene la frase "Enabling service":

```
-atxt "*Enabling service"
```

Si utiliza el carácter comodín, escriba el argumento entre comillas.

### Orden cronológico

Opcional. Imprime los eventos de registro en orden cronológico inverso. Si este parámetro no se especifica, el comando muestra los eventos de registro en orden cronológico.

Añada el siguiente parámetro al comando `getUserActivityLog` para imprimir el evento más reciente primero:

```
-ro true
```

## Escritura y visualización de eventos de registro de actividad del usuario

Si utiliza el comando `infacmd isp getUserActivityLog`, puede escribir eventos de registro de actividad del usuario en un archivo o mostrarlos la línea de comando. Escriba los eventos de registro de actividad del usuario en un formato determinado en función de la manera en que utilizará el archivo de eventos de registro que se exporte.

### Escritura y visualización de archivos de registro

Para escribir eventos de registro de actividad del usuario en un archivo, ejecute el comando con el parámetro de archivo de salida `-lo`:

```
-lo output_file_name
```

Si no especifica un formato de salida, el comando escribe los eventos de registro en un archivo de texto. Por ejemplo, puede ejecutar el siguiente comando para escribir eventos de registro en un archivo llamado `log.txt`:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo log.txt
```

Para especificar un formato de salida, ejecute el comando con el parámetro de formato `-fm`:

```
-fm output_format_BIN_TEXT_XML
```

Entre los formatos válidos se incluyen:

- Bin (binario). Utilice un archivo binario para hacer copias de seguridad de los eventos de registro en formato binario. Es posible que necesite emplear este formato para enviar eventos de registro al servicio internacional de atención al cliente de Informática.
- Texto. Utilice el formato de texto si desea analizar los eventos de registro con un editor de texto.
- XML. Utilice el formato XML si desea analizar los eventos de registro con una herramienta externa que emplee XML o si desea utilizar herramientas XML, como XSLT.

Si establece el formato de texto o XML como formato de salida, pero no especifica un archivo de salida, el comando muestra el registro de texto o XML en la línea de comandos.

Si selecciona el formato binario como formato de salida, debe proporcionar un nombre de archivo de salida.

Por ejemplo, puede ejecutar el siguiente comando para imprimir los eventos de registro en un archivo llamado `log.xml`:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm xml -lo log.xml
```

## Conversión de archivos de registro

Si utiliza el comando `getUserActivity` para escribir eventos de registro en un archivo binario, puede convertir el archivo en formatos de texto o XML.

Ejecute el siguiente comando para convertir un registro binario que ha recuperado en formato de texto o XML:

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm output_format_TEXT_XML -lo output_file_name
```

Por ejemplo, puede ejecutar el siguiente comando para convertir un archivo de entrada binario llamado `log.bin` en formato XML y, a continuación, obtener un archivo llamado `convertedLog.xml` como salida:

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

Para mostrar el registro en la línea de comandos, omita el nombre del archivo de salida.

Si omite el formato, el comando utiliza formato de texto.

## Administración de grupos

Es posible crear, editar y eliminar grupos en el dominio de seguridad nativo.

Puede asignar funciones, permisos y privilegios a un grupo en el dominio de seguridad nativo o en un dominio de seguridad de LDAP. No se pueden eliminar ni modificar las propiedades de las cuentas de grupo en los dominios de seguridad de LDAP. Las funciones, permisos y privilegios asignados al grupo determinan las tareas que los usuarios del grupo pueden realizar en el dominio de Informática.

Puede asignar funciones, permisos y privilegios a un grupo. Las funciones, permisos y privilegios asignados al grupo determinan las tareas que los usuarios del grupo pueden realizar en el dominio de Informática.

Puede asignar funciones, permisos y privilegios a un grupo. Las funciones, permisos y privilegios asignados al grupo determinan las tareas que los usuarios del grupo pueden realizar en el dominio de Informática.

### Cómo añadir un grupo nativo

En la ficha Seguridad, puede añadir, editar o quitar grupos nativos.

Un grupo nativo puede contener cuentas de usuario nativas o de LDAP, u otros grupos nativos. Asimismo, puede crear varios niveles de grupos nativos. Por ejemplo, el grupo Finance contiene el grupo AccountsPayable que, a su vez, contiene el grupo OfficeSupplies. En este caso, el grupo Finance es el grupo primario del grupo AccountsPayable y este último, a su vez, es el grupo primario del grupo OfficeSupplies. Por tanto, cada grupo puede contener otros grupos nativos.

Un grupo nativo puede contener cuentas de usuario u otros grupos nativos. Asimismo, puede crear varios niveles de grupos nativos. Por ejemplo, el grupo Finance contiene el grupo AccountsPayable que, a su vez, contiene el grupo OfficeSupplies. En este caso, el grupo Finance es el grupo primario del grupo AccountsPayable y este último, a su vez, es el grupo primario del grupo OfficeSupplies. Por tanto, cada grupo puede contener otros grupos nativos.

Un grupo nativo puede contener cuentas de usuario u otros grupos nativos. Asimismo, puede crear varios niveles de grupos nativos. Por ejemplo, el grupo Finance contiene el grupo AccountsPayable que, a su vez, contiene el grupo OfficeSupplies. En este caso, el grupo Finance es el grupo primario del grupo AccountsPayable y este último, a su vez, es el grupo primario del grupo OfficeSupplies. Por tanto, cada grupo puede contener otros grupos nativos.

1. En la herramienta del administrador, haga clic en la ficha Seguridad.
2. En el menú Acciones de seguridad, haga clic en Crear grupo.

3. Introduzca la siguiente información para el grupo:

Propiedad	Descripción
Nombre	Nombre del grupo. La distinción entre mayúsculas y minúsculas no se aplica a este nombre, el cual no puede contener más de 128 caracteres. Además, este nombre no puede incluir tabulaciones, caracteres de nueva línea ni los siguientes caracteres especiales: , + " \ < > ; / * % ? El nombre puede incluir un carácter de espacio ASCII siempre y cuando no sea el primer y último carácter. No se permiten otros caracteres de espacio.
Grupo primario	Grupo al que pertenece el nuevo grupo. Si selecciona un grupo nativo antes de hacer clic en Crear grupo, el grupo seleccionado será el grupo primario. De lo contrario, en el campo Grupo primario aparecerá el texto Nativo, que indica que el nuevo grupo no pertenece a ningún otro grupo.
Descripción	Descripción del grupo. La descripción del grupo no puede exceder 765 caracteres ni incluir los siguientes caracteres especiales: < > "

4. Haga clic en Examinar para seleccionar un grupo primario distinto.  
Puede crear más de un nivel de grupos y subgrupos.
5. Haga clic en Aceptar para guardar el grupo.

## Edición de las propiedades de un grupo nativo

Después de crear un grupo, puede cambiar la descripción del grupo y la lista de usuarios del grupo. No puede cambiar el nombre del grupo ni su elemento primario. Para cambiar el elemento primario del grupo, debe mover el grupo a otro grupo.

1. En la herramienta del administrador, haga clic en la ficha Seguridad.
2. En la sección Grupos del navegador, seleccione un grupo nativo y haga clic en Editar.
3. Cambie la descripción del grupo.
4. Para cambiar la lista de usuarios del grupo, haga clic en la ficha Usuarios.  
La ficha Usuarios muestra la lista de usuarios del dominio y la lista de usuarios asignados al grupo.
5. Para asignar usuarios al grupo, seleccione una cuenta de usuario en la columna Todos los usuarios y haga clic en Añadir.
6. Para quitar un usuario de un grupo, seleccione una cuenta de usuario en la columna Usuarios asignados y haga clic en Quitar.
7. Haga clic en Aceptar para guardar los cambios.

## Movimiento de un grupo nativo a otro

Para organizar los grupos de usuarios en el dominio de seguridad nativo, es posible configurar grupos anidados y mover un grupo a otro.

Para mover un grupo nativo a otro, haga clic con el botón derecho en el nombre de un grupo nativo en la sección de grupos del navegador y seleccione Mover grupo.

## Cómo eliminar un grupo nativo

Para eliminar un grupo nativo, haga clic con el botón derecho sobre el nombre del grupo en la sección Grupos del navegador y seleccione Eliminar grupo.

Al eliminar un grupo, los usuarios de ese grupo pierden su pertenencia al grupo y todos los permisos o privilegios heredados del grupo.

Cuando elimine un grupo, el administrador de servicio eliminará todos los grupos y subgrupos que pertenezcan a ese grupo.

## Grupos de LDAP

No es posible añadir, editar ni eliminar grupos de LDAP ni modificar las asignaciones de usuarios a grupos de LDAP en Administrator Tool. Debe administrar los grupos y las asignaciones de usuarios en el servicio de directorio de LDAP.

# Administración de perfiles de sistema operativo

Cree y administre los perfiles de sistema operativo en la ficha Seguridad de la Herramienta del administrador o desde la línea de comandos. Puede crear, editar y eliminar perfiles de sistema operativo. Puede asignar o cambiar el perfil de sistema operativo predeterminado para los usuarios y grupos.

Si el servicio de integración de datos está configurado para utilizar perfiles de sistema operativo, ejecutará asignaciones, perfiles y flujos de trabajo con el perfil de sistema operativo. Si el servicio de integración de PowerCenter está configurado para utilizar perfiles de sistema operativo, ejecutará flujos de trabajo con el perfil de sistema operativo.

Cree, edite y elimine perfiles de sistema operativo en la vista **Perfiles de sistema operativo** de la ficha **Seguridad**.

Siga los pasos que se indican a continuación para crear un perfil de sistema operativo:

1. Especifique un nombre de perfil de sistema operativo y un nombre de usuario del sistema.
2. Seleccione los servicios de integración y configure las propiedades del perfil de sistema operativo.
3. Opcionalmente, asigne permisos en el perfil de sistema operativo.

Puede asignar usuarios y grupos a los perfiles de sistema operativo y asignar un perfil predeterminado a usuarios y grupos después de crear un perfil de sistema operativo.

## Propiedades de perfil de sistema operativo para el servicio de integración de PowerCenter

Las variables del proceso de servicio que se definen en las propiedades de la sesión y en los archivos de parámetro anulan la configuración del perfil de sistema operativo.

La siguiente tabla describe las propiedades de perfil de sistema operativo para el servicio de integración de PowerCenter:

Propiedad	Descripción
Nombre	Nombre de sólo lectura del perfil de sistema operativo. El nombre no puede exceder los 128 caracteres. No puede contener espacios ni los siguientes caracteres especiales: \ / : * ? " < >   [ ] = + ; ,
Nombre del usuario del sistema	Nombre de sólo lectura de un usuario del sistema operativo que ya existe en el equipo en el que se ejecuta el servicio de integración de PowerCenter. El servicio de integración de PowerCenter ejecuta los flujos de trabajo con el acceso al sistema del usuario del sistema definido para el perfil de sistema operativo.
\$PMRootDir	El directorio raíz al que se puede tener acceso mediante el nodo. Este es el directorio raíz para otras variables del proceso de servicio. No puede contener los siguientes caracteres especiales: * ? < > "   ,
\$PMSessionLogDir	El directorio para los registros de sesión. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/SessLogs.
\$PMBadFileDir	El directorio para los archivos de rechazo. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/BadFiles.
\$PMCacheDir	El directorio para el índice y los archivos de memoria caché de datos. Puede incrementar el rendimiento cuando el directorio de la memoria caché es una unidad local en el proceso del servicio de integración de PowerCenter. Para los archivos de la memoria caché, no use una unidad asignada o montada. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/Cache.
\$PMTargetFileDir	El directorio para los archivos de destino. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/TgtFiles.
\$PMSourceFileDir	El directorio para los archivos de origen. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/SrcFiles.
\$PmExtProcDir	El directorio para los procedimientos externos. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/ExtProc.

Propiedad	Descripción
\$PMTempDir	El directorio para los archivos temporales. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/Temp.
\$PMLookupFileDir	El directorio para los archivos de búsqueda. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/LkpFiles.
\$PMStorageDir	El directorio para los archivos de tiempo de ejecución. Los archivos de recuperación del flujo de trabajo se guardan en el directorio \$PMStorageDir configurado en las propiedades del servicio de integración de PowerCenter. Los archivos de recuperación de la sesión se guardan en el directorio \$PMStorageDir configurado en el perfil de sistema operativo. No puede contener los siguientes caracteres especiales: * ? < > "   , El valor predeterminado es \$PMRootDir/Storage.
Variables de entorno	Nombre y valor de las variables de entorno utilizadas por el servicio de integración durante el tiempo de ejecución.  Si especifica la variable de entorno LD_LIBRARY_PATH en las propiedades del perfil de sistema operativo, el servicio de integración agrega el valor de esta variable a su variable de entorno LD_LIBRARY_PATH. El servicio de integración usa el valor de la variable de entorno LD_LIBRARY_PATH para definir las variables de entorno de los procesos secundarios generados para el perfil de sistema operativo.  Si no especifica la variable de entorno LD_LIBRARY_PATH en las propiedades del perfil de sistema operativo, el servicio de integración usa su variable de entorno LD_LIBRARY_PATH.

## Propiedades de perfil de sistema operativo para el servicio de integración de datos

La siguiente tabla describe las propiedades de perfil de sistema operativo para el servicio de integración de datos:

Propiedad	Descripción
Nombre	Nombre de sólo lectura del perfil de sistema operativo. El nombre no puede exceder los 128 caracteres. No puede contener espacios ni los siguientes caracteres especiales: \ / : * ? " < >   [ ] = + ; ,
Nombre del usuario del sistema	Nombre de sólo lectura de un usuario del sistema operativo que ya existe en los sistemas en los que se ejecuta el servicio de integración de datos. El servicio de integración de datos ejecuta asignaciones, flujos de trabajo y tareas de creación de perfiles mediante el acceso al sistema del usuario del sistema operativo.
\$DISRootDir	El directorio raíz al que se puede tener acceso mediante el nodo. Este es el directorio raíz para otras variables del proceso de servicio. No puede contener los siguientes caracteres especiales: * ? < > "   , [ ]

Propiedad	Descripción
\$DISTempDir	<p>Directorio de los archivos temporales creados cuando se ejecutan los trabajos. No puede contener los siguientes caracteres especiales:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>El valor predeterminado es &lt;directorio raíz&gt;/disTemp.</p>
\$DISCacheDir	<p>El directorio de los archivos de índice y memoria caché de datos de las transformaciones. No puede contener los siguientes caracteres especiales:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>El valor predeterminado es &lt;directorio raíz&gt;/cache.</p>
\$DISSourceDir	<p>El directorio para archivos sin formato de origen utilizados en una asignación. No puede contener los siguientes caracteres especiales:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>El valor predeterminado es &lt;directorio raíz&gt;/source.</p>
\$DISTargetDir	<p>El directorio para los archivos sin formato de destino utilizados en una asignación. No puede contener los siguientes caracteres especiales:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>El valor predeterminado es &lt;directorio raíz&gt;/target.</p>
\$DISRejectedFilesDir	<p>El directorio para los archivos de rechazo. Los archivos de rechazo contienen filas que se rechazaron al ejecutar una asignación. No puede contener los siguientes caracteres especiales:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>El valor predeterminado es &lt;directorio raíz&gt;/reject.</p>
\$DISLogDir	<p>Directorio para los registros. No puede contener los siguientes caracteres especiales:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>El valor predeterminado es &lt;directorio raíz&gt;/disLogs.</p>
Habilitar propiedades de suplantación de Hadoop	<p>Indica que el servicio de integración de datos utiliza el usuario de suplantación de Hadoop para ejecutar asignaciones, flujos de trabajo y tareas de creación de perfiles en un entorno de Hadoop.</p> <p>El usuario de suplantación de Hadoop predeterminado es el usuario que ha iniciado sesión. Para especificar otro usuario de suplantación de Hadoop diferente, seleccione <b>Utilizar el usuario especificado como usuario de suplantación de Hadoop</b> e introduzca un nombre de usuario.</p>



Propiedad	Descripción
Variables de entorno	<p>Nombre y valor de las variables de entorno utilizadas por el servicio de integración durante el tiempo de ejecución.</p> <p>Si especifica la variable de entorno LD_LIBRARY_PATH en las propiedades del perfil de sistema operativo, el servicio de integración agrega el valor de esta variable a su variable de entorno LD_LIBRARY_PATH. El servicio de integración usa el valor de la variable de entorno LD_LIBRARY_PATH para definir las variables de entorno de los procesos secundarios generados para el perfil de sistema operativo.</p> <p>Si no especifica la variable de entorno LD_LIBRARY_PATH en las propiedades del perfil de sistema operativo, el servicio de integración usa su variable de entorno LD_LIBRARY_PATH.</p> <p><b>Nota:</b> En AIX, debe establecer la variable de entorno LD_LIBRARY_PATH en INFA_HOME/services/shared/bin para que el servicio de integración de datos ejecute correctamente las asignaciones, perfiles y flujos de trabajo con perfiles del sistema operativo.</p>
Directorio de la memoria caché de archivos sin formato	<p>El directorio de la memoria caché de archivos sin formato donde la herramienta del analista almacena los archivos sin formato cargados.</p> <p>Si el servicio del analista se conecta a un servicio de integración de datos que utiliza perfiles de sistema operativo, el usuario del sistema operativo especificado en el perfil deberá tener acceso a este directorio de memoria caché de archivos sin formato. Cuando importe una tabla de referencia o un origen de archivo sin formato, la Herramienta del analista usará los archivos de este directorio para crear una tabla de referencia o un objeto de datos de archivo sin formato. Reinicie el servicio del analista si cambia la ubicación de los archivos sin formato.</p>

## Cómo crear un perfil del sistema operativo

Cree un perfil de sistema operativo y asígnelo a los usuarios y grupos para aumentar la seguridad y aislar el entorno de usuario en tiempo de ejecución. Puede crear uno o varios perfiles de sistema operativo. El servicio de integración de PowerCenter usa el perfil de sistema operativo para ejecutar flujos de trabajo. El servicio de integración de datos utiliza el perfil de sistema operativo para ejecutar asignaciones, perfiles y flujos de trabajo.

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. En el menú Acciones de seguridad, haga clic en **Crear perfil de sistema operativo**.

El cuadro de diálogo **Crear perfil de sistema operativo: paso 1 de 3** aparece.

3. Especifique las siguientes propiedades generales para el perfil de sistema operativo:

Propiedad	Descripción
Nombre	Nombre del perfil de sistema operativo. No se aplica la distinción entre mayúsculas y minúsculas al nombre, el cual debe ser único en el dominio. Este nombre no puede tener más de 128 caracteres ni empezar por @. Tampoco puede contener los siguientes caracteres especiales: % * + \ / ? ; < > El nombre puede contener un carácter de espacio ASCII, menos en el primer y último carácter. Los otros caracteres de espacio no están permitidos.
Nombre del usuario del sistema	Nombre de un usuario del sistema operativo que existe en los equipos en los que se ejecuta el servicio de integración. El servicio de integración ejecuta flujos de trabajo o tareas usando el acceso al sistema del usuario del sistema definido en el perfil del sistema operativo. <b>Nota:</b> Cuando cree perfiles de sistema operativo, no puede especificar el nombre del usuario del sistema como raíz o utilizar un usuario que no sea raíz con uid==0.

4. Haga clic en **Siguiente**.

El cuadro de diálogo **Configurar perfiles de sistema operativo: paso 2 de 3** aparece.

5. Seleccione uno de los servicios de integración, o ambos, que utilizarán el perfil de sistema operativo.

- Servicio de integración de PowerCenter
- Servicio de integración de datos

6. Configure las propiedades del perfil de sistema operativo para los servicios de integración.

7. Si el servicio de integración de datos ejecuta asignaciones, perfiles y flujos de trabajo en un entorno de Hadoop, configure las propiedades de suplantación de Hadoop como se explica a continuación:

- Seleccione **Habilitar propiedades de suplantación de Hadoop**.
- Puede usar el usuario que ha iniciado sesión o especificar un usuario de suplantación de Hadoop para ejecutar las tareas de Hadoop.

8. Opcionalmente, configure las variables del entorno.

9. Si el servicio del analista se conecta a un servicio de integración de datos que utiliza perfiles de sistema operativo, configure las propiedades del servicio del analista.

10. Haga clic en **Siguiente**.

El cuadro de diálogo **Asignar grupos y usuarios al perfil de sistema operativo: paso 3 de 3** aparece.

11. En la ficha **Grupos**, asigne grupos al perfil de sistema operativo de la siguiente manera:

- Para asignar grupos específicos al perfil de sistema operativo, seleccione uno o varios grupos y haga clic en **Añadir**.
- Para asignar todos los grupos disponibles al perfil de sistema operativo, haga clic en **Añadir todos**.

12. Opcionalmente, asigne el perfil de sistema operativo como perfil predeterminado para uno o varios grupos. Para asignar un perfil predeterminado, seleccione **Perfil predeterminado** para el grupo en la lista Grupos seleccionados.

13. En la ficha **Usuarios**, asigne usuarios al perfil de sistema operativo de la siguiente manera:

- Para asignar usuarios específicos al perfil de sistema operativo, seleccione uno o varios usuarios y haga clic en **Añadir**.
- Para asignar todos los usuarios disponibles al perfil de sistema operativo, haga clic en **Añadir todos**.

14. Opcionalmente, asigne el perfil de sistema operativo como perfil predeterminado para uno o varios usuarios. Para asignar un perfil predeterminado, seleccione **Perfil predeterminado** para el usuario en la lista Usuarios seleccionados.
15. Haga clic en **Finalizar**.  
Después de crear el perfil de sistema operativo, el panel de detalles muestra las propiedades del perfil de sistema operativo y los grupos y usuarios a los que se ha asignado el perfil.

## Editar un perfil de sistema operativo

Puede editar un perfil de sistema operativo para cambiar las propiedades del mismo.

No se puede editar el nombre o el nombre del usuario del sistema después de crear un perfil de sistema operativo. Si no desea usar el usuario del sistema operativo especificado en el perfil de sistema operativo, elimine el perfil de sistema operativo.

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Seleccione la vista **Perfiles de sistema operativo**.
3. Seleccione el perfil de sistema operativo.
4. En la ficha **Propiedades**, haga clic en **Editar**.  
Se abrirá el cuadro de diálogo **Editar propiedades**.
5. Seleccione el **servicio de integración de datos** o el **servicio de integración de PowerCenter** que desea configurar.
6. Edite las propiedades del servicio de integración.
7. Haga clic en **Aceptar**.

## Asigne un perfil del sistema operativo predeterminado a un usuario o grupo

Cuando un usuario o grupo tiene acceso a más de un perfil de sistema operativo, asigne un perfil predeterminado que el servicio de integración pueda utilizar para ejecutar las tareas y los flujos de trabajo. Puede asignar cualquier perfil de sistema operativo con permiso directo como perfil predeterminado para un usuario o grupo. Un usuario o grupo solo puede tener un perfil de sistema operativo predeterminado. Sin embargo, puede asignar el mismo perfil de sistema operativo como perfil predeterminado a más de un usuario o grupo.

1. En la ficha Seguridad, seleccione la vista **Usuarios o Grupos**.
2. En el navegador, seleccione el usuario o grupo.
3. En el panel de contenido, seleccione la vista **Permisos**.
4. Haga clic en la ficha **Perfiles del sistema operativo**.
5. Haga clic en el botón **Asignar o cambiar el perfil del sistema operativo predeterminado**.  
Aparecerá el cuadro de diálogo **Asignar o cambiar el perfil del sistema operativo predeterminado**.
6. Seleccione un perfil desde la lista **Perfil del sistema operativo predeterminado**. O bien seleccione **No asignar un perfil del sistema operativo predeterminado** en la lista para eliminar el perfil predeterminado que se ha asignado a un usuario o un grupo.
7. Haga clic en **Aceptar**.  
En el panel de detalles, la columna **Perfil predeterminado** muestra **Sí (directo)** para el perfil del sistema operativo.

## Eliminar un perfil de sistema operativo

Para eliminar un perfil de sistema operativo, haga clic con el botón derecho en el nombre del perfil de sistema operativo en la sección del navegador del mismo nombre y seleccione **Eliminar perfil**.

Después de eliminar un perfil de sistema operativo, asigne otro a los usuarios y grupos a los que se había asignado dicho perfil como perfil predeterminado. Si el servicio de integración de PowerCenter utiliza perfiles de sistema operativo, asigne otro perfil de sistema operativo a las carpetas del repositorio y a los flujos de trabajo a los que se había asignado este perfil.

## Trabajar con perfiles del sistema operativo en un dominio seguro

Puede utilizar perfiles de sistema operativo en un dominio de Informática que tiene la comunicación segura habilitada.

Tenga en cuenta las siguientes reglas y directrices cuando utilice perfiles de sistema operativo en un dominio que tiene la comunicación segura habilitada:

- Debe establecer la siguiente variable de entorno para el perfil del sistema operativo:

### **INFA\_TRUSTSTORE**

Establezca el valor en el directorio que contiene los archivos de truststore de los certificados SSL del dominio de seguridad. El directorio debe contener un archivo truststore llamado `infa_truststore.pem`.

### **INFA\_TRUSTSTORE\_PASSWORD**

Si utiliza un truststore personalizado, establezca el valor de la contraseña del `infa_truststore.pem` que contiene el certificado SSL del dominio seguro. La contraseña debe estar cifrada. Use el programa de la línea de comandos `pmpasswd` para cifrar la contraseña.

- Asimismo, si el servicio de integración de PowerCenter utiliza la opción Sesión en malla, debe establecer la siguiente variable de entorno para el perfil del sistema operativo:

### **INFA\_KEYSTORE**

Establezca el valor en el directorio que contiene los archivos de almacén de claves de los certificados SSL del dominio de seguridad. El directorio debe contener un archivo de almacén de claves llamado `infa_keystore.pem`.

Puede configurar las variables de entorno del perfil del sistema operativo en la Herramienta del administrador. Para establecer las variables de entorno para el perfil del sistema operativo, haga clic en **Seguridad > Perfil del sistema operativo**. Edite las propiedades del perfil del sistema operativo y configure las variables de entorno.

## Cómo trabajar con perfiles del sistema operativo en un dominio con autenticación Kerberos

Puede utilizar perfiles de sistema operativo en un dominio de Informática que se ejecuta en una red con autenticación Kerberos.

Tenga en cuenta las siguientes reglas y directrices cuando utilice perfiles de sistema operativo en un dominio que se ejecuta en una red con autenticación Kerberos:

- La cuenta de usuario del perfil del sistema operativo debe ser un nombre principal en el servicio Active Directory utilizada para la autenticación Kerberos e importada en un dominio de seguridad de LDAP del dominio de Informática.
- La cuenta de usuario debe tener un archivo de memoria caché de credenciales de Kerberos accesible para cuenta de usuario del perfil del sistema operativo. Cada cuenta de usuario del perfil del sistema operativo debe tener un archivo de memoria caché de credenciales independiente.

- El archivo de memoria caché de credenciales de la cuenta de usuario del perfil del sistema operativo debe ser reenviable. Por ejemplo, si usa la utilidad *kinit* para crear el archivo de memoria caché de credenciales, debe incluir la opción *-f*.
- El archivo de memoria caché de credenciales para la cuenta de usuario del perfil del sistema operativo debe estar disponible al ejecutar un flujo de trabajo que utiliza un perfil del sistema operativo.
- El archivo de memoria caché de credenciales para la cuenta de usuario del perfil del sistema operativo siempre debe tener las credenciales más actualizadas. Puede ejecutar la utilidad del programador de trabajos, tales como *cron*, para actualizar las credenciales de usuario en el archivo de memoria caché de credenciales de forma regular.
- Debe establecer las siguientes variables de entorno para el perfil del sistema operativo:

#### **INFA\_OSPI\_SECURITY\_DOMAIN**

Establezca el valor para el nombre del dominio de seguridad que contiene la cuenta de usuario del perfil del sistema operativo. Si la cuenta de usuario está en el dominio de seguridad del dominio de usuario de Kerberos, no necesita configurar esta variable. El dominio de seguridad del dominio de usuario de Kerberos es el dominio de seguridad creado durante la instalación, el cual tiene el mismo nombre que el del dominio del usuario Kerberos.

#### **KRB5\_CONFIG**

Establezca el valor en la ruta y nombre del archivo de configuración de Kerberos. El nombre del archivo de configuración de Kerberos es *krb5.conf*.

#### **KRB5CCNAME**

Establezca el valor en la ruta y nombre del archivo de memoria caché de credenciales de Kerberos para la cuenta de usuario del perfil del sistema operativo.

Puede configurar las variables de entorno del perfil del sistema operativo en la Herramienta del administrador. Para establecer las variables de entorno para el perfil del sistema operativo, haga clic en **Seguridad > Perfil del sistema operativo**. Edite las propiedades del perfil del sistema operativo y configure las variables de entorno.

## Bloqueo de cuenta

Para mejorar la seguridad en el dominio de Informatica, un administrador puede aplicar el bloqueo de cuentas de usuario del dominio, incluidas otras de usuario de administrador, después de varios inicios de sesión fallidos.

El administrador puede especificar el número de intentos de inicio de sesión fallidos que un usuario puede tener antes de que se bloquee la cuenta de usuario. Si una cuenta se bloquea, el administrador puede desbloquear la cuenta en el dominio de Informatica.

Si el administrador desbloquea una cuenta de usuario, este puede seleccionar la opción "Desbloquear el usuario y restablecer la contraseña" para restablecer la contraseña de usuario. El administrador puede enviar un correo electrónico al usuario para pedirle que cambie la contraseña antes de volver a iniciar sesión en el dominio. Para habilitar el dominio para enviar correos electrónicos a los usuarios cuando se restablecen las contraseñas, establezca la configuración del servidor de correo electrónico del dominio.

Si el usuario está bloqueado en el dominio de Informatica y el servidor de LDAP, el administrador de Informatica puede desbloquear la cuenta de usuario en el dominio de Informatica. El usuario no puede iniciar sesión en el dominio de Informatica hasta que el administrador de LDAP también desbloquee la cuenta de usuario en el servidor de LDAP.

**Nota:** Si el dominio de Informatica utiliza la autenticación de red de Kerberos, no se podrá configurar el bloqueo de cuentas de usuario. La vista **Administración de cuentas** no está disponible en la ficha **Seguridad** de la herramienta Administrator.

## Cómo configurar el bloqueo de cuenta

Seleccione las opciones de bloqueo de cuenta para bloquear cuentas de usuario del dominio de Informatica tras varios inicios de sesión fallidos.

1. En la herramienta Administrator, haga clic en **Seguridad > Administración de cuentas**.
2. En la sección **Configuración de bloqueo de cuenta**, haga clic en **Editar**.
3. Establezca las propiedades siguientes:

Propiedad	Descripción
Habilitar bloqueo de cuenta	Bloquea una cuenta de usuario del dominio de Informatica después de un número determinado de inicios de sesión fallidos. De forma predeterminada, esta opción no bloquea cuentas de usuario de administrador. Debe seleccionar la opción <b>Habilitar el bloqueo de cuentas de administrador</b> para aplicar el bloqueo en cuentas de usuario de administrador.
Habilitar el bloqueo de cuentas de administrador	Bloquea una cuenta de usuario de administrador del dominio de Informatica después de un número determinado de inicios de sesión fallidos. Debe seleccionar la opción <b>Habilitar bloqueo de cuenta</b> antes de poder aplicar el bloqueo en cuentas de usuario de administrador.
Número máximo de intentos de inicio de sesión	Especifica el número máximo de inicios de sesión fallidos que se permiten de forma consecutiva antes de que una cuenta de usuario se bloquee del dominio de Informatica.

## Reglas y directrices para el bloqueo de cuenta

Tenga en cuenta las siguientes reglas y directrices al aplicar el bloqueo de cuenta para usuarios de Informatica:

- Si se ejecuta un servicio de aplicación bajo una cuenta de usuario y la contraseña es incorrecta para el servicio de aplicación, la cuenta de usuario puede bloquearse cuando el servicio de aplicación intente iniciarse. El servicio de integración de datos, el servicio del concentrador de servicios web y el servicio de integración de PowerCenter son servicios de aplicaciones fiables que utilizan un nombre de usuario y una contraseña para autenticarse con el servicio de repositorio de modelos o el servicio de repositorio de PowerCenter. Si el servicio de integración de datos, el servicio de concentrador de servicios web o el servicio de integración de PowerCenter intentan reiniciar continuamente después de un inicio de sesión fallido, el dominio bloquea finalmente la cuenta de usuario asociada.
- Si una cuenta de usuario de LDAP está bloqueada del dominio de Informatica y el servidor de autenticación de LDAP, el administrador del dominio de Informatica puede desbloquear la cuenta en el dominio de Informatica. El administrador de LDAP puede desbloquear la cuenta de usuario en el servidor de LDAP.
- Si se habilita el bloqueo de cuenta en el dominio de Informatica y en el servidor de LDAP, configure el mismo umbral de fallos en el inicio de sesión en el dominio de Informatica y en el servidor de LDAP para evitar confusiones sobre la política de bloqueo de la cuenta.
- Si el bloqueo de cuenta no está habilitado en el dominio de Informatica pero un usuario está bloqueado, verifique que el usuario no esté bloqueado en el servidor de LDAP.

## CAPÍTULO 9

# Privilegios y funciones

Este capítulo incluye los siguientes temas:

- [Introducción a los privilegios y funciones, 135](#)
- [Privilegios del dominio, 138](#)
- [Privilegios del servicio del analista, 146](#)
- [Privilegios del servicio de administración de contenido, 148](#)
- [Privilegios del servicio de integración de datos., 148](#)
- [Privilegios del servicio de Metadata Manager, 149](#)
- [Privilegios del Servicio de repositorio de modelos, 152](#)
- [Privilegios del servicio de repositorio de PowerCenter, 154](#)
- [Privilegios del Servicio de escucha PowerExchange, 169](#)
- [Privilegios del Servicio de registrador PowerExchange, 169](#)
- [Privilegios del servicio de programador, 170](#)
- [Privilegios del servicio de Test Data Manager, 171](#)
- [Cómo administrar funciones, 180](#)
- [Cómo asignar privilegios y funciones a usuarios y grupos, 185](#)
- [Visualización de usuarios con privilegios para un servicio, 187](#)
- [Solucionar problemas de privilegios y funciones, 187](#)

## Introducción a los privilegios y funciones

La seguridad de los usuarios se administra mediante privilegios y funciones.

Puede modificar los privilegios y las funciones según el tipo de licencia de PowerCenter Express.

### Privilegios

Los privilegios determinan las acciones que los usuarios pueden realizar en aplicaciones cliente. Informatica incluye los siguientes privilegios:

- Privilegios del dominio. Determine las acciones que los usuarios pueden realizar en el dominio de Informatica mediante la Herramienta del administrador y los programas de la línea de comandos infacmd y pmrep.

- Privilegios del dominio. Determinan las acciones sobre el dominio de Informatica que los usuarios pueden realizar mediante la Herramienta del administrador.
- Privilegio del Servicio del analista. Determina las acciones que los usuarios pueden realizar mediante Informatica Analyst.
- Privilegio del servicio de administración de contenido. Determina las acciones que los usuarios pueden realizar con las tablas de referencia de la Informatica Developer tool y la herramienta Informatica Analyst.
- Privilegio del servicio de integración de datos. Determina las acciones sobre las aplicaciones que los usuarios pueden realizar mediante la Herramienta del administrador y el programa de línea de comandos infacmd. Este privilegio también determina si los usuarios pueden obtener detalles y exportar resultados de perfiles.
- Privilegio del servicio de integración de datos. Determina las acciones sobre las aplicaciones que los usuarios pueden realizar mediante la Herramienta del administrador. Este privilegio también determina si los usuarios pueden obtener detalles y exportar resultados de perfiles.
- Privilegios del servicio de Metadata Manager. Determinan las acciones que los usuarios pueden realizar mediante Metadata Manager.
- Privilegio del servicio de repositorio de modelos. Determina las acciones que los usuarios pueden realizar mediante Informatica Analyst e Informatica Developer.
- Privilegio del servicio de repositorio de modelos. Determina las acciones que los usuarios pueden realizar con Informatica Developer.
- Privilegios del servicio de repositorio de PowerCenter. Determinan las acciones del repositorio de PowerCenter que los usuarios pueden realizar mediante el administrador de repositorios, Designer, el administrador de flujos de trabajo, el supervisor de flujos de trabajo y los programas de línea de comandos pmrep y pmcmd.
- Privilegios del servicio de aplicaciones de PowerExchange. Determinan las acciones que los usuarios pueden realizar sobre el servicio de escucha de PowerExchange y el servicio de registrador de PowerExchange mediante comandos infacmd pwx.
- Privilegios del servicio de programador. Determine las acciones que los usuarios pueden realizar con el Servicio de programador.
- Privilegios del servicio de Test Data Manager. Determinan las tareas de obtención de datos, enmascaramiento de datos, subconjunto de datos y generación de datos de prueba que los usuarios pueden realizar mediante Test Data Manager.

Los privilegios determinan las acciones que los usuarios pueden realizar en aplicaciones cliente. Informatica incluye privilegios de dominio, que determinan las acciones que pueden realizar los usuarios mediante la Herramienta del administrador.

Puede asignar privilegios a usuarios y grupos para los servicios de aplicación. Puede asignar diferentes privilegios a un usuario para cada servicio de aplicación del mismo tipo de servicio.

También puede asignar privilegios a usuarios y grupos en la **ficha Seguridad** de la Herramienta del administrador.

La Herramienta del administrador organiza los privilegios por niveles. Un privilegio se lista debajo del privilegio que incluye. Algunos privilegios incluyen otros privilegios. Cuando asigne un privilegio a usuarios y grupos, la Herramienta del administrador también asignará cualquier privilegio incluido.



## Grupos de privilegios

Los privilegios del dominio y servicio de aplicación se organizan en grupos de privilegios. Un grupo de privilegios es una organización de privilegios que definen acciones de usuario habituales. Por ejemplo, los privilegios del dominio incluyen los siguientes grupos de privilegios:

- Herramientas. Incluye los privilegios para iniciar sesión en la herramienta Administrator.
- Administración de seguridad. Incluye los privilegios para administrar los usuarios, los grupos, las funciones y los privilegios.
- Administración de dominios. Incluye los privilegios para administrar el dominio, las carpetas, los nodos, las mallas, las licencias y los servicios de aplicación.
- Administración de dominios. Incluye los privilegios para administrar el dominio, las carpetas y los servicios de aplicación.
- Administración de seguridad. Incluye los privilegios para administrar los usuarios, los grupos, las funciones y los privilegios.
- Administración de dominios. Incluye los privilegios para administrar el dominio, las carpetas, los nodos, las mallas, las licencias y los servicios de aplicación.
- Herramientas. Incluye los privilegios para iniciar sesión en la herramienta Administrator.
- Supervisión. Incluye los privilegios para supervisar las implementaciones de Ultra Messaging y ver las estadísticas.

**Sugerencia:** Cuando asigne privilegios a usuarios y grupos de usuarios, puede seleccionar un grupo de privilegios para asignar todos los privilegios del grupo.

## Funciones

Una función es una recopilación de privilegios que se asignan a un usuario o grupo. Dentro de una organización, cada usuario tiene una función específica, ya sea un desarrollador, administrador, usuario básico o usuario avanzado.

Por ejemplo, la función Desarrollador de PowerCenter incluye todos los privilegios o acciones del servicio de repositorio de PowerCenter que realiza un desarrollador.

Las funciones se asignan a usuarios y grupos para el dominio y para servicios de aplicación del dominio.

**Sugerencia:** Si organiza a los usuarios en grupos y, a continuación, asigna funciones y permisos a los grupos, puede simplificar las tareas de administración del usuario. Por ejemplo, si un usuario cambia posiciones dentro de la organización, mueva el usuario a otro grupo. Si un nuevo usuario se une a la organización, agregue el usuario al grupo. El usuario hereda las funciones y permisos asignados al grupo. No necesita volver a asignar privilegios, funciones y permisos. Para obtener más información, consulte el siguiente artículo de la biblioteca de asistencia de Informatica:

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

**Sugerencia:** Si organiza a los usuarios en grupos y, a continuación, asigna funciones y permisos a los grupos, puede simplificar las tareas de administración del usuario. Por ejemplo, si un usuario cambia posiciones dentro de la organización, mueva el usuario a otro grupo. Si un nuevo usuario se une a la organización, agregue el usuario al grupo. El usuario hereda las funciones y permisos asignados al grupo. No necesita volver a asignar privilegios, funciones y permisos.

# Privilegios del dominio

Los privilegios del dominio determinan las acciones que pueden realizar los usuarios con la herramienta Administrator y los programas de la línea de comandos infacmd y pmrep.

Los privilegios de dominio determinan las acciones que pueden realizar los usuarios mediante la herramienta Administrator.

La siguiente tabla describe cada uno de los grupos de privilegios del dominio:

Grupo de privilegios	Descripción
Administración de seguridad	Incluye los privilegios para administrar los usuarios, los grupos, las funciones y los privilegios.
Administración de dominios	Incluye los privilegios para administrar el dominio, las carpetas, los nodos, las mallas, las licencias, los servicios de aplicación y las conexiones.
Supervisión	Incluye privilegios para configurar estadísticas e informes de supervisión, ver la supervisión de los objetos de integración y acceder a la supervisión.
Herramientas	Incluye los privilegios para iniciar sesión en la herramienta Administrator.
Administración en la nube	Incluye privilegios para añadir y ver organizaciones de Informatica Cloud en la herramienta del administrador.

Grupo de privilegios	Descripción
Administración de seguridad	Incluye los privilegios para administrar los usuarios, los grupos, las funciones y los privilegios.
Administración de dominios	Incluye los privilegios para administrar el dominio, los servicios de aplicación y las conexiones.
Supervisión	Incluye privilegios para configurar estadísticas e informes de supervisión, ver la supervisión de los objetos de integración y acceder a la supervisión.
Herramientas	Incluye los privilegios para iniciar sesión en la herramienta Administrator.

Grupo de privilegios	Descripción
Administración de seguridad	Incluye los privilegios para administrar los usuarios, los grupos, las funciones y los privilegios.
Administración de dominios	Incluye los privilegios para administrar el dominio, los servicios de aplicación y las conexiones.
Supervisión	Incluye los privilegios para supervisar las implementaciones de UM y ver las estadísticas.
Herramientas	Incluye los privilegios para iniciar sesión en la herramienta Administrator.

## Grupo de privilegios Administración de seguridad

Los privilegios del grupo de privilegios Administración de seguridad y los permisos del objeto de dominio determinan las acciones de administración de seguridad que los usuarios pueden realizar.

Algunas tareas de administración de seguridad están determinadas por la función de administrador, no por los privilegios o permisos.

Algunas tareas de administración de seguridad están determinadas por la función de administrador, no por los privilegios o permisos. Un usuario que tenga asignada la función de administrador para el dominio puede realizar las siguientes tareas:

- Cree, edite y elimine perfiles de sistema operativo.
- Conceder permisos para perfiles de sistema operativo.

**Nota:** Para completar las tareas de administración de seguridad en la Herramienta del administrador, los usuarios también tienen el privilegio de acceso a Informatica Administrator.

### Privilegio Conceder privilegios y funciones

Los usuarios a los que se les ha asignado el privilegio Conceder privilegios y funciones pueden asignar privilegios y funciones a usuarios y a grupos.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Conceder privilegios y funciones:

Permiso de	Descripción
Servicio de aplicación o dominio	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Asignar privilegios y funciones a usuarios y grupos para el dominio y servicio de aplicaciones.</li><li>- Editar y quitar los privilegios y funciones asignados a usuarios y grupos.</li></ul>

### Privilegio Administrar usuarios, grupos y funciones

Los usuarios a los que se les ha asignado el privilegio Administrar usuarios, grupos y funciones pueden configurar la autenticación de LDAP y administrar usuarios, grupos y funciones.

El privilegio Administrar usuarios, grupos y funciones incluye el privilegio Conceder privilegios y funciones.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar usuarios, grupos y funciones:

Permiso de	Descripción
-	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Configurar la autenticación de LDAP para el dominio.</li><li>- Crear, editar y eliminar usuarios, grupos y funciones.</li><li>- Importar usuarios y grupos de LDAP.</li></ul>
Perfiles de sistema operativo	El usuario puede editar propiedades de perfil del sistema operativo.

## Grupo de privilegios Administración de dominios

Las acciones de administración de dominios que los usuarios pueden realizar dependen de los privilegios del grupo Administración de dominios y los permisos para los objetos de dominios.

Algunas tareas de administración de dominios se determinan mediante el rol de administrador y no mediante privilegios o permisos. Un usuario que tenga asignada la función de administrador para el dominio puede realizar las siguientes tareas:

- Configurar las propiedades del dominio.
- Conceder permiso para el dominio..
- Administrar y purgar eventos de registro.
- Recibir alertas del dominio.
- Ejecutar el informe de licencia.
- Ver los eventos de registro de actividad del usuario.
- Cerrar el dominio.
- Acceder al asistente para actualización de servicios.

Los usuarios a los que se le asignan permisos de objetos de dominio, pero no privilegios, pueden realizar algunas tareas de administración de dominio. La siguiente tabla muestra las acciones que pueden realizar los usuarios cuando solo se les asigna permisos del objeto de dominio:

Permiso en	Descripción
Dominio	El usuario puede realizar las acciones siguientes: <ul style="list-style-type: none"><li>- Ver las propiedades y los eventos de registro del dominio.</li><li>- Definir la configuración de supervisión.</li></ul>
Carpeta	El usuario puede ver propiedades de carpeta.
Servicio de aplicación	El usuario puede ver las propiedades del servicio de aplicación y eventos de registro.
Objeto de licencia	El usuario puede ver las propiedades del objeto de licencia.
Malla	El usuario puede ver las propiedades de malla.
Nodo	El usuario puede ver las propiedades del nodo.
Concentrador de servicios web	El usuario puede ejecutar el informe de servicios web.

**Nota:** Para completar las tareas de administración de dominios en la herramienta Administrator, los usuarios deben tener además el privilegio de acceso para Informatica Administrator.

## Privilegio Administrar ejecución de servicios

Los usuarios a los que se les ha asignado el privilegio Administrar ejecución de servicios pueden habilitar y deshabilitar servicios de aplicación y recibir alertas de servicios de aplicación.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar ejecución de servicios:

Permiso de	Descripción
Servicio de aplicación	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Habilitar y deshabilitar servicios de aplicación y procesos de servicio. Para habilitar y deshabilitar un servicio de Metadata Manager, los usuarios deben tener además permiso para el servicio de integración de PowerCenter y el servicio de repositorio de PowerCenter asociados.</li><li>- Recibir alertas de servicio de aplicación.</li></ul>

Permiso de	Descripción
Servicio de aplicación	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Habilitar y deshabilitar servicios de aplicación y procesos de servicio.</li><li>- Recibir alertas de servicio de aplicación.</li></ul>

## Privilegio Administrar servicios

Los usuarios a los que se les ha asignado el privilegio Administrar servicios pueden crear, configurar, mover, eliminar y otorgar permisos sobre servicios de aplicación y objetos con licencia.

El privilegio Administrar servicios incluye el privilegio Administrar ejecución de servicios.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar servicios:

Permiso en	Descripción
Dominio o carpeta principal	El usuario puede crear objetos de licencia.
Dominio o carpeta principal, nodo o malla en los que se ejecuta el servicio de aplicación, objeto de licencia y cualquier servicio de aplicación asociado	El usuario puede crear servicios de aplicación.
Servicio de aplicación	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Configurar servicios de aplicación.</li><li>- Conceder permiso para los servicios de aplicación.</li></ul>
Carpetas originales y de destino	El usuario puede mover servicios de aplicación u objetos de licencia de una carpeta a otra.
Dominio o carpeta principal y servicio de aplicación	El usuario puede quitar servicios de aplicación.
Servicio del analista	El usuario puede crear y eliminar tablas de traza de auditoría.

Permiso en	Descripción
Servicio de Metadata Manager	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Realizar una copia de seguridad del contenido del repositorio de Metadata Manager.</li> <li>- Eliminar contenido del repositorio de Metadata Manager.</li> <li>- Actualizar el contenido del Servicio de Metadata Manager.</li> </ul> <p><b>Nota:</b> Para crear o restaurar el contenido del repositorio de Metadata Manager, el usuario debe pertenecer al grupo Administrador predeterminado.</p>
Servicio de Metadata Manager Servicio de repositorio de PowerCenter	El usuario puede restaurar el repositorio de PowerCenter para Metadata Manager.
Servicio de repositorio de modelos	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Crear y eliminar contenido del repositorio de modelos.</li> <li>- Crear, eliminar y volver a indizar el índice de búsqueda.</li> <li>- Actualizar el contenido del servicio de repositorio de modelos mediante el menú <b>Acciones</b> o la línea de comandos. El usuario también debe contar con los privilegios Crear, Editar y Eliminar proyectos en el servicio de repositorio de modelos, así como permisos de escritura en los proyectos.</li> </ul>
Servicio de integración de PowerCenter	El usuario puede ejecutar el servicio de integración de PowerCenter en modo seguro.
Servicio de repositorio de PowerCenter	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Hacer copias de seguridad, restaurar y actualizar el repositorio de PowerCenter.</li> <li>- Configurar el linaje de datos para el repositorio de PowerCenter.</li> <li>- Copiar contenido desde otro repositorio de PowerCenter.</li> <li>- Cerrar conexiones de usuario y liberar bloqueos del repositorio de PowerCenter.</li> <li>- Crear y eliminar contenido del repositorio de PowerCenter.</li> <li>- Crear, editar y eliminar extensiones de metadatos reutilizables en el PowerCenter Repository Manager.</li> <li>- Habilitar el control de versiones para el repositorio de PowerCenter.</li> <li>- Administrar un dominio del repositorio de PowerCenter.</li> <li>- Realizar una purga avanzada de las versiones de objetos en el nivel de repositorio en el PowerCenter Repository Manager.</li> <li>- Registrar y cancelar el registro de complementos del repositorio de PowerCenter.</li> <li>- Ejecutar el repositorio de PowerCenter en modo exclusivo.</li> <li>- Enviar notificaciones del repositorio de PowerCenter a los usuarios.</li> <li>- Actualizar las estadísticas del repositorio de PowerCenter.</li> <li>- Actualizar el contenido del servicio de repositorio de PowerCenter.</li> </ul>
Servicio de Test Data Manager	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Crear y eliminar el contenido del repositorio de Test Data Manager.</li> <li>- Actualizar el contenido del servicio de Test Data Manager.</li> </ul>
Objeto de licencia	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Editar objetos de licencia.</li> <li>- Conceder permiso para los objetos de licencia.</li> </ul>

Permiso en	Descripción
Objeto de licencia y servicio de aplicación	El usuario puede asignar una licencia a un servicio de aplicación.
Dominio o carpeta principal y objeto de licencia	El usuario puede quitar objetos de licencia.

Permiso en	Descripción
Dominio en el que se ejecuta el servicio de aplicación, así como cualquier servicio de aplicación asociado	El usuario puede crear servicios de aplicación.
Servicio de aplicación	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Configurar servicios de aplicación.</li> <li>- Conceder permiso para los servicios de aplicación.</li> </ul>
Servicio de repositorio de modelos	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Crear y eliminar contenido del repositorio de modelos.</li> <li>- Crear, eliminar y volver a indexar el índice de búsqueda.</li> </ul>

## Privilegio Administrador nodos y cuadrículas

Los usuarios a los que se les ha asignado el privilegio Administrar nodos y cuadrículas pueden crear, configurar, mover, cambiar el nombre, apagar y otorgar permisos sobre nodos y cuadrículas.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar nodos y cuadrículas:

Permiso de	Descripción
Dominio o carpeta primaria	El usuario puede crear nodos.
Dominio o carpeta primaria y nodos asignados a la malla	El usuario puede crear mallas.
Nodo o malla	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Configurar y cerrar nodos y cuadrículas.</li> <li>- Conceder permiso para nodos y cuadrículas.</li> </ul>
Carpetas de origen y destino	El usuario puede mover los nodos y mallas de una carpeta a otra.
Dominio o carpeta primaria y nodo o malla	El usuario puede quitar nodos y mallas.

## Privilegio Administrar carpetas de dominio

Los usuarios a los que se les ha asignado el privilegio de Administrar carpetas de dominio pueden crear, editar, mover, cambiar el nombre y otorgar permisos de carpetas de dominio.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar carpetas de dominio:

Permiso de	Descripción
Dominio o carpeta primaria	El usuario puede crear carpetas.
Carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Editar carpetas.</li><li>- Conceder permiso para carpetas.</li></ul>
Carpetas originales y de destino	El usuario puede mover carpetas de una carpeta principal a otra.
Dominio o carpeta primaria y carpeta que se va a quitar	El usuario puede quitar carpetas.

## Privilegio Administrar conexiones

Los usuarios a los que se les ha asignado el privilegio Administrar conexiones pueden crear, editar y eliminar conexiones en las herramientas Administrator, Analyst, Developer y en el programa de la línea de comandos infacmd. Los usuarios también pueden copiar conexiones en la herramienta Developer y pueden conceder permisos sobre las conexiones en la herramienta Administrator y el programa de línea de comandos infacmd.

Los usuarios a los que se les ha asignado el privilegio Administrar conexiones pueden crear, editar y eliminar conexiones en las herramientas Administrator y Developer y en el programa de la línea de comandos infacmd. Los usuarios también pueden copiar conexiones en la herramienta Developer y pueden conceder permisos sobre las conexiones en la herramienta Administrator y el programa de línea de comandos infacmd.

Los usuarios a los que se les ha asignado permisos de conexión pero no el privilegio de Administrar conexiones pueden realizar las siguientes acciones de administración de conexiones:

- Ver todos los metadatos de conexiones, excepto contraseñas. Requiere permisos de lectura de conexiones.
- Obtener una vista previa de los datos o ejecutar una asignación, un cuadro de mando o un perfil. Requiere ejecutar permisos de conexiones.
- Obtener una vista previa de los datos o ejecutar una asignación o un perfil. Requiere ejecutar permisos de conexiones.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar conexiones:

Permiso	Descripción
-	El usuario puede crear conexiones.
Escribir al conectar	El usuario puede copiar, editar y eliminar conexiones.
Conceder al conectar	El usuario puede conceder y revocar permisos en las conexiones.



## Grupo de privilegios Supervisión

Los privilegios del grupo de privilegios Supervisión determinan qué usuarios pueden ver y configurar la supervisión.

La siguiente tabla muestra los permisos necesarios y las acciones que pueden realizar los usuarios con los privilegios del grupo Administrar supervisión:

Privilegio principal	Privilegio	Permiso en	Descripción
Administrar supervisión	Configuración de supervisión	Dominio	El usuario puede configurar valores de supervisión.
Administrar supervisión	Configuración de informes y estadísticas	Dominio	El usuario puede configurar estadísticas e informes de supervisión.
Ver	Vea tareas de todos los usuarios de los grupos a los que pertenece el usuario	Dominio	Un usuario de un grupo puede supervisar las tareas ejecutadas por otros usuarios del grupo. Si el usuario pertenece a varios grupos, puede ver las tareas de todos ellos.
Vea tareas de todos los usuarios de los grupos a los que pertenece el usuario	Ver trabajos de otros usuarios	Dominio	El usuario puede ver los trabajos de otros usuarios.
Ver	Ver estadísticas	Dominio	El usuario puede acceder a la vista Estadísticas de resumen y a estadísticas de objetos de dominio. <b>Nota:</b> En un dominio que utiliza la autenticación Kerberos, los usuarios deben tener también la función de administrador del servicio de repositorio de modelos que se ha configurado para supervisar.
Ver	Ver informes	Dominio	El usuario puede ver informes de objetos de dominio.
Acceder a la supervisión	Acceder desde la Herramienta del analista	Dominio	El usuario puede acceder al espacio de trabajo Estado de trabajo en la Herramienta del analista.
Acceder a la supervisión	Acceder desde Developer tool	Dominio	El usuario puede acceder a la herramienta Monitoring desde Developer tool.
Acceder a la supervisión	Acceder desde la Herramienta del administrador	Dominio	El usuario puede acceder a la ficha Supervisión en la Herramienta del administrador.
N/A	Realizar acciones en trabajos	Dominio	El usuario puede realizar las acciones siguientes: <ul style="list-style-type: none"><li>- Anular trabajos.</li><li>- Emitir de nuevo trabajos de asignación.</li><li>- Ver registros de trabajos.</li></ul>

Los usuarios no necesitan tener el privilegio Acceder a Informática Administrator para poder acceder a la Herramienta del administrador.

## Grupo de privilegios Herramientas

El privilegio en el grupo Herramientas del dominio determina qué usuarios pueden acceder a la herramienta Administrator.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con privilegios en el grupo de herramientas.

Privilegio	Descripción
Acceder a Informatica Administrator	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Iniciar sesión en Administrator Tool.</li><li>- Administrar su propia cuenta de usuario en Administrator Tool.</li><li>- Exportar eventos de registro.</li></ul>

Para realizar tareas en la Herramienta del administrador, los usuarios deben tener el privilegio de acceso a Informatica Administrator. Los usuarios no necesitan el privilegio de acceso a Informatica Administrator para ejecutar comandos infacmd ni acceder a la Herramienta de supervisión.

## Grupo de privilegios Administración en la nube

Los privilegios del grupo Administración en la nube determinan qué usuarios pueden ver y configurar organizaciones de Informatica Cloud.

La siguiente tabla enumera los permisos requeridos y las acciones que pueden realizar los usuarios con privilegios en el grupo Administración en la nube:

Privilegio	Permiso en	Descripción
Ver organización	Dominio	El usuario puede ver organizaciones de Informatica Cloud y los agentes seguros y las conexiones en la nube asociados.
Administrar organización	Dominio	Puede añadir organizaciones de Informatica Cloud en la herramienta del administrador.

## Privilegios del servicio del analista

El privilegio del servicio del analista determina las acciones que los usuarios con la licencia correspondiente pueden realizar en los proyectos empleando la Herramienta del analista.

La tabla siguiente detalla los privilegios y permisos necesarios para administrar proyectos y objetos de los proyectos:

Privilegio	Permiso	Descripción
Ejecutar perfiles y cuadros de mando	Lectura en proyectos. Ejecución en la conexión de origen de datos relacionales.	El usuario puede ejecutar perfiles y cuadros de mando para los usuarios con la licencia correspondiente en la Herramienta del analista.
Acceder a especificaciones de asignación	Lectura en proyectos.	El usuario puede acceder a especificaciones de asignación para los usuarios con la licencia correspondiente en la Herramienta del analista.
Cargar resultados de especificación de asignación	Escritura en proyectos.	El usuario puede cargar los resultados de una especificación de asignación para los usuarios con la licencia correspondiente en una tabla o archivo sin formato. <b>Nota:</b> Al seleccionar este privilegio también se concede el privilegio <b>Acceder a especificaciones de asignación</b> de forma predeterminada.
Administrar glosarios	-	El usuario puede administrar el glosario empresarial.
Ver glosarios	-	El usuario puede ver activos de Business Glossary publicados en el espacio de trabajo Biblioteca. Es equivalente a proporcionar permiso de lectura para los glosarios y los activos del glosario en el espacio de trabajo Seguridad del glosario.
Acceso al espacio de trabajo	-	El usuario puede acceder a los siguientes espacios de trabajo en la Herramienta del analista: - Espacio de trabajo <b>Diseño</b> . - Espacio de trabajo <b>Detección</b> . - Espacio de trabajo <b>Glosario</b> . - Espacio de trabajo <b>Cuadros de mando</b> . <b>Nota:</b> Al seleccionar este privilegio también se concede acceso a los proyectos de la Herramienta del analista. Si el usuario no tiene este privilegio, el usuario debe tener el privilegio <b>Espacio de trabajo de diseño, Espacio de trabajo de detección, Espacio de trabajo del glosario o Espacio de trabajo de cuadros de mando</b> para acceder a los proyectos.
Espacio de trabajo Diseño	-	El usuario puede acceder al espacio de trabajo <b>Diseño</b> .
Espacio de trabajo Detección	-	El usuario puede acceder al espacio de trabajo <b>Detección</b> .
Espacio de trabajo Glosario	-	El usuario puede acceder al espacio de trabajo <b>Glosario</b> .
Espacio de trabajo Cuadros de mando	-	El usuario puede acceder al espacio de trabajo <b>Cuadros de mando</b> .

## Privilegios del servicio de administración de contenido

Los privilegios del servicio de administración del contenido determinan las acciones que los usuarios con licencia pueden realizar en las tablas de referencia.

En la siguiente tabla se indican los privilegios y permisos requeridos para administrar las tablas de referencia:

Privilegio	Permiso	Descripción
Crear tablas de referencia	Escritura en proyecto	<ul style="list-style-type: none"><li>- Cree una tabla de referencia en las herramientas Analyst y Developer.</li><li>- Cree una tabla de referencia con el comando <code>infacmd rtm import</code>.</li><li>- Importe un objeto de la tabla de referencia en el repositorio de modelos.</li><li>- Copie una tabla de referencia en las herramientas Analyst y Developer.</li><li>- Cree una tabla de referencia a partir de datos de perfil.</li></ul> <b>Nota:</b> El privilegio Crear también concede el privilegio Editar de forma predeterminada.
Editar los datos y metadatos de la tabla de referencia	Lectura en proyecto	<ul style="list-style-type: none"><li>- Edite los valores de los datos en las herramientas Developer y Analyst.</li><li>- Añada los datos de perfil en una tabla de referencia.</li><li>- Añada columnas a una tabla de referencia o elimínelas. Los metadatos de la tabla de referencia tales como nombres de columna, descripciones y valores predeterminados se pueden cambiar.</li></ul>

## Privilegios del servicio de integración de datos.

Los privilegios del servicio de integración de datos determinan las acciones que los usuarios pueden realizar en las aplicaciones que utilicen la herramienta Administrator y el programa de línea de comandos `infacmd`. También determinan si los usuarios pueden recopilar y exportar resultados del perfil utilizando las herramientas Analyst y Developer.

Los privilegios del servicio de integración de datos determinan las acciones que los usuarios pueden realizar en las aplicaciones que utilicen la herramienta Administrator y el programa de línea de comandos `infacmd`. También determinan si los usuarios pueden recopilar y exportar resultados del perfil utilizando la herramienta Developer.

En la siguiente tabla se muestran las acciones que pueden realizar los usuarios con el privilegio en el grupo de privilegios de administración de la aplicación:

Nombre del privilegio	Descripción
Administrar aplicaciones	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"><li>- Realizar copias de seguridad y restaurar una aplicación en un archivo.</li><li>- Implementar una aplicación en un servicio de integración de datos y resolver conflictos de nombres.</li><li>- Iniciar una aplicación después de la implementación.</li><li>- Buscar una aplicación.</li><li>- Inicie o detenga objetos en una aplicación.</li><li>- Configurar las propiedades de la aplicación.</li></ul>

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio en grupo de privilegios de administración de creación de perfiles:

Nombre del privilegio	Permiso en	Descripción
Resultados de obtención de detalles y exportación	Leer proyecto Ejecutar en la conexión de origen de datos relacional para obtener detalles de datos activos	El usuario puede realizar las siguientes acciones: - Recopilar resultados de creación de perfiles - Exportar resultados de creación de perfiles.

## Privilegios del servicio de Metadata Manager

Los privilegios del servicio de Metadata Manager determinan las acciones de Metadata Manager que los usuarios pueden realizar empleando Metadata Manager.

La tabla siguiente describe cada grupos de privilegios de Metadata Manager:

Grupos de privilegios	Descripción
Catálogo	Incluye privilegios para administrar objetos en la página del navegador de la interfaz de Metadata Manager.
Cargar	Incluye privilegios para administrar objetos en la página de carga de la interfaz de Metadata Manager.
Modelo	Incluye privilegios para administrar objetos en la página de modelos de la interfaz de Metadata Manager.
Seguridad	Incluye privilegios para administrar objetos en la página de seguridad de la interfaz de Metadata Manager.

### Grupo de privilegios Catálogo

Los privilegios del grupo de privilegios Catálogo determinan las tareas que los usuarios pueden realizar en la ficha **Examinar** de la aplicación Metadata Manager. Un usuario con el privilegio para realizar una acción

determinada también necesita permisos para realizar la acción en un objeto concreto. Configure los permisos en la ficha **Seguridad** de la aplicación Metadata Manager.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Catálogo y los permisos requeridos para realizar una tarea en un objeto:

Privilegio	Privilegios incluidos	Permiso	Descripción
Compartir accesos directos	n/d	Escritura	El usuario puede compartir una carpeta que contiene un acceso directo con otros usuarios y grupos.
Ver linaje	n/d	Lectura	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Ejecutar análisis de linaje de datos en objetos de metadatos, categorías y términos de negocio.</li> <li>- Ejecutar análisis de linaje de datos en PowerCenter Designer. Además, los usuarios deben tener permiso de lectura en la carpeta del repositorio de PowerCenter.</li> </ul>
Ver catálogos relacionados	n/d	Lectura	El usuario puede ver catálogos relacionados.
Ver resultados de perfil	n/d	Lectura	El usuario puede ver información de creación de perfiles para objetos de metadatos en el catálogo de un origen relacional.
Ver catálogo	n/d	Lectura	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Ver recursos y objetos de metadatos en el catálogo de metadatos.</li> <li>- Realizar búsquedas en el catálogo de metadatos.</li> </ul>
Ver relaciones	n/d	Lectura	El usuario puede ver relaciones para objetos de metadatos, categorías y términos empresariales.
Administrar relaciones	Ver relaciones	Escritura	El usuario puede crear, editar y eliminar relaciones para objetos de metadatos personalizados, categorías y términos empresariales.
Ver comentarios	n/d	Lectura	El usuario puede ver comentarios para objetos de metadatos, categorías y términos empresariales.
Insertar comentarios	Ver comentarios	Escritura	El usuario puede añadir comentarios para objetos de metadatos, categorías y términos empresariales.
Eliminar comentarios	<ul style="list-style-type: none"> <li>- Insertar comentarios</li> <li>- Ver comentarios</li> </ul>	Escritura	El usuario puede eliminar comentarios para objetos de metadatos, categorías y términos empresariales.
Ver vínculos	n/d	Lectura	El usuario puede ver vínculos para objetos de metadatos, categorías y términos empresariales.
Administrar vínculos	Ver vínculos	Escritura	El usuario puede crear, editar y eliminar vínculos para objetos de metadatos, categorías y términos empresariales.

Privilegio	Privilegios incluidos	Permiso	Descripción
Ver glosario	n/d	Lectura	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Ver glosarios empresariales en la vista <b>Glosario</b>.</li> <li>- Realizar búsquedas en glosarios de negocio.</li> </ul>
Administrar objetos	n/d	Escritura	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Editar objetos de metadatos del catálogo.</li> <li>- Crear, editar y eliminar objetos de metadatos personalizados. Los usuarios deben tener además el privilegio Ver modelo.</li> <li>- Crear, editar y eliminar recursos de metadatos personalizados. Los usuarios deben tener además el privilegio Administrar recurso.</li> </ul>

## Grupo de privilegios Carga

Los privilegios del grupo de privilegios Carga determinan las tareas que los usuarios pueden realizar en la ficha **Carga** de la aplicación Metadata Manager. Un usuario con el privilegio para realizar una acción determinada también necesita permisos para realizar la acción en un objeto concreto. Configure los permisos en la ficha **Seguridad** de la aplicación Metadata Manager.

La tabla siguiente enumera los privilegios y los permisos necesarios para administrar una instancia de un recurso en el almacén de Metadata Manager:

Privilegio	Privilegios incluidos	Permiso	Descripción
Ver recursos	-	Lectura	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Ver recursos y sus propiedades en el almacén de Metadata Manager.</li> <li>- Exportar configuraciones de recursos.</li> <li>- Descargar el programa de instalación del Agente de Metadata Manager.</li> </ul>
Cargar recurso	Ver recursos	Escritura	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Cargar metadatos para un recurso en el almacén de Metadata Manager.*</li> <li>- Crear vínculos entre objetos en recursos conectados para linaje de datos.</li> <li>- Configurar indexación de búsqueda para recursos.</li> <li>- Importar configuraciones de recursos.</li> </ul>
Administrar programas	Ver recursos	Escritura	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Crear y editar programas.</li> <li>- Añadir programas a los recursos.</li> </ul>
Purgar metadatos	Ver recursos	Escritura	El usuario puede quitar metadatos para un recurso desde el almacén de Metadata Manager.
Administrar recursos	<ul style="list-style-type: none"> <li>- Purgar metadatos</li> <li>- Ver recursos</li> </ul>	Escritura	El usuario puede crear, editar y eliminar recursos.
* Para cargar metadatos de los recursos de Business Glossary, son necesarios los privilegios Cargar recurso, Administrar recursos y Ver modelo.			

## Grupo de privilegios Modelo

Los privilegios del grupo de privilegios Modelo determinan las tareas que los usuarios pueden realizar en la ficha **Modelo** de la aplicación Metadata Manager. No se pueden configurar permisos en un modelo.

En la siguiente tabla, se enumeran los privilegios necesarios para administrar modelos:

Privilegio	Privilegios incluidos	Permiso	Descripción
Ver modelo	-	-	El usuario puede abrir modelos y clases y ver propiedades de modelos y clases. Ver relaciones y atributos para las clases.
Administrar modelo	Ver modelo	-	El usuario puede crear, editar y eliminar modelos personalizados. Añade atributos a modelos empaquetados y universales.
Exportar/Importar modelos	Ver modelo	-	El usuario puede importar y exportar modelos personalizados. Importe y exporte modelos empaquetados modificados y universales.

## Grupo de privilegios Seguridad

Los privilegios del grupo de privilegios Seguridad determinan las tareas que los usuarios pueden realizar en la ficha **Seguridad** de la aplicación Metadata Manager.

De manera predeterminada, el privilegio Administrar permisos de catálogo del grupo de privilegios Seguridad se asigna al administrador o a un usuario con función de administrador en el servicio de Metadata Manager. Puede asignar el privilegio Administrar permisos de catálogo a otros usuarios.

En la siguiente tabla, se enumeran los privilegios y los permisos necesarios para administrar la seguridad de Metadata Manager:

Privilegio	Privilegios incluidos	Permiso	Descripción
Administrar permisos de catálogo	-	Control total	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Asignar usuarios y permisos del grupo en recursos, objetos de metadatos, categorías y términos empresariales.</li><li>- Editar permisos en recursos, objetos de metadatos, categorías y términos empresariales.</li></ul>

## Privilegios del Servicio de repositorio de modelos

Los privilegios del Servicio de repositorio de modelos determinan las acciones que pueden realizar los usuarios en los proyectos mediante Informatica Analyst e Informatica Developer.

Los privilegios del Servicio de repositorio de modelos determinan las acciones que los usuarios pueden realizar en los proyectos mediante Informatica Developer.

Los permisos del objeto del repositorio de modelos determinan las tareas que los usuarios pueden realizar en los objetos de los proyectos.



En la siguiente tabla se muestran los permisos necesarios y las acciones que los usuarios pueden realizar con los privilegios del Servicio de repositorio de modelos:

Privilegio	Permiso	Descripción
N/A	Lectura en proyecto	El usuario puede ver proyectos y los objetos de los proyectos.
N/A	Escritura en proyecto	El usuario puede crear, editar y eliminar objetos de los proyectos.
N/A	Conceder en proyecto	El usuario puede conceder y revocar permisos para los proyectos a usuarios y grupos.
Acceder con el analista	N/A	El usuario puede acceder al repositorio de modelos desde la Herramienta del analista.
Acceder con el desarrollador	N/A	El usuario puede acceder al repositorio de modelos desde Developer tool.
Crear, editar y eliminar proyectos	N/A	El usuario puede crear proyectos.
Crear, editar y eliminar proyectos	Escritura en proyectos	El usuario puede realizar las acciones siguientes: <ul style="list-style-type: none"> <li>- Editar proyectos.</li> <li>- Eliminar proyectos si los ha creado el usuario.</li> <li>- Actualizar el contenido del Servicio de repositorio de modelos. Para actualizar el servicio mediante el menú <b>Acciones</b> o la línea de comandos, el usuario también debe contar con el privilegio Administrar servicios en el dominio, así como con permisos en el Servicio de repositorio de modelos. Para actualizar el servicio mediante el asistente para actualización de servicios, es necesario que el usuario también tenga asignada la función de administrador para el dominio.</li> </ul>
Administrar dominios de datos	N/A	El usuario puede crear, editar y eliminar dominios de datos en el glosario de dominio de datos. Este privilegio forma parte del grupo de privilegios <b>Administración de dominio de datos</b> .
Administrar notificaciones	N/A	El usuario puede configurar notificaciones de cuadro de mandos. Este privilegio forma parte del grupo de privilegios <b>Administración de creación de perfiles</b> .

Privilegio	Permiso	Descripción
Administrar desarrollo basado en equipos	N/A	El usuario puede administrar los estados de bloqueo o desbloqueo de los objetos del repositorio de modelos. Si el repositorio de modelos está integrado con un sistema de control de versiones, el usuario puede administrar los estados protegido o desprotegido de los objetos. El usuario también puede administrar la propiedad de los objetos desprotegidos.
Mostrar detalles de seguridad	N/A	El usuario puede ver los siguientes detalles: <ul style="list-style-type: none"> <li>- Nombre de los proyectos para los que los usuarios no tienen permiso de lectura.</li> <li>- Detalles de los mensajes de error y de advertencia.</li> </ul>

Privilegio	Permiso	Descripción
N/A	Lectura en proyecto	El usuario puede ver proyectos y los objetos de los proyectos.
N/A	Escritura en proyecto	El usuario puede crear, editar y eliminar objetos de los proyectos.
N/A	Conceder en proyecto	El usuario puede conceder y revocar permisos para los proyectos a usuarios y grupos.
Acceder con el desarrollador	N/A	El usuario puede acceder al repositorio de modelos desde Developer tool.
Crear, editar y eliminar proyectos	N/A	El usuario puede realizar las acciones siguientes: <ul style="list-style-type: none"> <li>- Crear proyectos.</li> <li>- Actualizar el Servicio de repositorio de modelos.</li> </ul>
Crear, editar y eliminar proyectos	Escritura en proyecto	El usuario puede realizar las acciones siguientes: <ul style="list-style-type: none"> <li>- Editar proyectos.</li> <li>- Eliminar proyectos si los ha creado el usuario.</li> </ul>
Mostrar detalles de seguridad	N/A	El usuario puede ver los siguientes detalles: <ul style="list-style-type: none"> <li>- Nombre de los proyectos para los que los usuarios no tienen permiso de lectura.</li> <li>- Detalles de los mensajes de error y de advertencia.</li> </ul>

## Privilegios del servicio de repositorio de PowerCenter

Los privilegios del servicio de repositorio de PowerCenter determinan las acciones del repositorio de PowerCenter que los usuarios pueden efectuar con el administrador de repositorios de PowerCenter, Designer, el administrador del flujo de trabajo, el supervisor de flujo de trabajo y los programas de la línea de comandos pmrep y pmcmd.

La tabla siguiente describe cada grupo de privilegios para el servicio del repositorio de PowerCenter:

Grupos de privilegios	Descripción
Herramientas	Incluye privilegios para acceder a las herramientas cliente de PowerCenter y a los programas de la línea de comandos.
Carpetas	Incluye privilegios para administrar las carpetas del repositorio.
Objetos de diseño	Incluye privilegios para administrar los componentes de negocio, los parámetros y variables de asignación, las asignaciones, los mapplets, las transformaciones y las funciones definidas por el usuario.
Orígenes y destinos	Incluye privilegios para administrar cubos, dimensiones, definiciones de origen y definiciones de destino.
Objetos en tiempo de ejecución	Incluye privilegios para administrar objetos de configuración de sesión, tareas, flujos de trabajos y worklets.
Objetos globales	Incluye privilegios para administrar objetos de conexiones, grupos de implementación, etiquetas y consultas.

Los usuarios deben tener el privilegio de dominio Administrar servicios y el permiso en el servicio de repositorio de PowerCenter para efectuar las siguientes acciones en el administrador del repositorio:

- Efectuar una purga avanzada de las versiones de objeto en el nivel del repositorio de PowerCenter.
- Crear, editar y eliminar extensiones de metadatos reutilizables.

## Grupo de privilegios Herramientas

Los privilegios del grupo de privilegios Herramientas del servicio de repositorio de PowerCenter determinan las herramientas y programas de línea de comandos del cliente de PowerCenter a los que los usuarios pueden acceder.

La siguiente tabla enumera las acciones que los usuarios pueden realizar para los privilegios del grupo Herramientas:

Privilegio	Permiso	Descripción
Acceso a Designer	-	El usuario puede conectar con el repositorio de PowerCenter mediante Designer.
Acceso al administrador de repositorios	-	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Conectar con el repositorio de PowerCenter mediante el administrador de repositorios.</li> <li>- Ejecutar comandos <i>pmrep</i>.</li> </ul>

Privilegio	Permiso	Descripción
Acceso al administrador de flujos de trabajo	-	El usuario puede realizar las siguientes acciones: - Permite conectarse con el repositorio de PowerCenter mediante el administrador de flujos de trabajo. - Quitar un servicio de integración de PowerCenter del administrador de flujos de trabajo.
Acceso al supervisor de flujos de trabajo	-	El usuario puede realizar las siguientes acciones: - Conectar con el repositorio de PowerCenter mediante el supervisor de flujo de trabajo. - Conectar con el servicio de integración de PowerCenter mediante el supervisor de flujo de trabajo.

**Nota:** Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.

Se necesita el privilegio adecuado del grupo de privilegios Herramienta para todos los usuarios que realicen tareas con las herramientas y programas de línea de comandos del cliente de PowerCenter. Por ejemplo, para crear carpetas en el administrador de repositorios, un usuario debe tener los privilegios Crear carpetas y Acceso al administrador de repositorio.

Si los usuarios tienen un privilegio del grupo de privilegios Herramientas y permiso sobre un objeto de repositorio de PowerCenter pero no el privilegio para modificar el tipo de objeto, pueden realizar algunas acciones sobre el objeto. Por ejemplo, un usuario tiene el privilegio de acceso al administrador de repositorio y de lectura sobre algunas carpetas. El usuario no tiene ningún privilegio del grupo de privilegios Carpetas. El usuario puede visualizar objetos en las carpetas y comparar carpetas.

## Grupo de privilegios Carpetas

Las acciones de administración de carpetas vienen determinadas por los privilegios del grupo de privilegios Carpetas, los permisos de objeto de repositorio de PowerCenter y los permisos de objeto de dominio. Los usuarios realizan las acciones de administración de carpetas en el administrador del repositorio y con el programa de la línea de comandos pmrep.

Algunas tareas de administración de carpetas vienen determinadas por la propiedad de la carpeta y la función de administrador, no por privilegios o permisos. El propietario de la carpeta o un usuario que tenga asignada la función de administrador para el servicio de repositorio de PowerCenter puede llevar a cabo las siguientes tareas de administración de carpetas:

- Asignar perfiles de sistema operativo si el servicio de integración de PowerCenter usa perfiles de sistema operativo. Requiere permiso en el perfil de sistema operativo.
- Cambiar el propietario de la carpeta.
- Configurar permisos de carpeta.
- Eliminar la carpeta.
- Designar la carpeta que se va a compartir.
- Editar el nombre y la descripción de la carpeta.

Los usuarios a los que se les ha asignado permisos de carpetas pero no privilegios pueden realizar algunas de las acciones de administración de carpetas. La siguiente tabla muestra las acciones que pueden realizar los usuarios cuando solo se les asignan permisos de carpetas:

Permiso	Descripción
Lectura en carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Comparar carpetas.</li><li>- Ver los objetos de las carpetas.</li></ul>

**Nota:** Para realizar acciones en las carpetas, los usuarios también deben tener el privilegio de acceso al administrador del repositorio.

### Privilegio Crear carpetas

Los usuarios a los que se les ha asignado el privilegio Crear carpetas pueden crear carpetas del repositorio de PowerCenter.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Crear carpetas:

Permiso	Descripción
-	El usuario puede crear carpetas.

### Privilegio Copiar carpetas

Los usuarios a los que se les ha asignado el privilegio Copiar carpetas pueden copiar carpetas dentro de un repositorio de PowerCenter o en otro repositorio de PowerCenter.

Las siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Copiar carpetas:

Permiso	Descripción
Lectura en carpeta	El usuario puede copiar carpetas dentro del mismo repositorio de PowerCenter o a otro repositorio de PowerCenter. Los usuarios también deben tener el privilegio Crear carpetas en el repositorio de destino.

## Gestionar versiones de carpetas

Si tiene una opción de desarrollo basado en equipos, asigne a los usuarios el privilegio Administrar versiones de carpetas en un repositorio con versión de PowerCenter. Los usuarios pueden cambiar el estado de las carpetas y efectuar una purga avanzada de las versiones del objeto en el nivel de la carpeta.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar versiones de carpeta:

Permiso	Descripción
Lectura y escritura en carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Cambiar el estado de las carpetas.</li><li>- Realizar un purgado avanzado de versiones de objetos en el nivel de carpeta.</li></ul>

## Grupo de privilegios Objetos de diseño

Los privilegios del grupo de privilegios Objetos de diseño y los permisos para los objetos del repositorio de PowerCenter determinan las acciones que los usuarios pueden realizar en los siguientes objetos de diseño:

- Componentes de negocio
- Parámetros y variables de asignación
- Asignaciones
- Mapplets
- Transformaciones
- Funciones definidas por el usuario

Los usuarios a los que se les han asignado permisos pero no privilegios pueden realizar algunas acciones para los objetos de diseño. La siguiente tabla muestra las acciones que pueden realizar los usuarios cuando solo se les asignan permisos:

Permiso	Descripción
Lectura en carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Comparar objetos de diseño.</li><li>- Copiar objetos de diseño como imágenes.</li><li>- Exportar objetos de diseño.</li><li>- Generar código para la transformación personalizada y los procedimientos externos.</li><li>- Recibir mensajes de notificación del repositorio de PowerCenter.</li><li>- Ejecutar el linaje de datos en los objetos de diseño. Los usuarios deben tener además el privilegio Ver linaje para el servicio de Metadata Manager y permiso de lectura en los objetos de metadatos del catálogo de Metadata Manager.</li><li>- Buscar objetos de diseño.</li><li>- Ver los objetos de diseño, las dependencias de los objetos de diseño y el historial de los objetos de diseño.</li></ul>
Lectura en carpeta compartida Lectura y escritura en carpeta de destino	El usuario puede crear accesos directos.

**Nota:** Para realizar acciones en los objetos de diseño, los usuarios deben tener además el privilegio correspondiente en el grupo de privilegio Herramientas.

## Privilegio de Crear, editar y eliminar objetos de diseño

Los usuarios a los que se les ha asignado el privilegio de Crear, editar y eliminar objetos de diseño pueden crear, editar y eliminar componentes de negocio, los parámetros y variables de asignación, las asignaciones, los mapplets, las transformaciones y las funciones definidas por el usuario.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio de Crear, editar y eliminar objetos de diseño:

Permiso	Descripción
Lectura en carpeta original Lectura y escritura en carpeta de destino	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Copiar objetos de diseño de una carpeta a otra.</li> <li>- Copiar objetos de diseño a otro repositorio de PowerCenter. Los usuarios deben tener además el privilegio Crear, editar y eliminar objetos de diseño en el repositorio de destino.</li> </ul>
Lectura y escritura en carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Cambiar comentarios para un objeto de diseño con versión.</li> <li>- Proteger y deshacer desprotección de objetos de diseño desprotegidos por su propia cuenta de usuario.</li> <li>- Desproteger objetos de diseño.</li> <li>- Copiar y pegar objetos de diseño en la misma carpeta.</li> <li>- Crear, editar y eliminar perfiles de datos e iniciar Profile Manager. Los usuarios deben tener además el privilegio Crear, editar y eliminar objetos en tiempo de ejecución.</li> <li>- Crear, editar y eliminar objetos de diseño.</li> <li>- Generar y limpiar programas SAP ABAP.</li> <li>- Generar asignaciones de integración de contenido de negocio. Los usuarios deben tener además el privilegio Crear, editar y eliminar orígenes y destinos.</li> <li>- Importar objetos de diseño mediante Designer. Los usuarios deben tener además el privilegio Crear, editar y eliminar orígenes y destinos.</li> <li>- Importar objetos de diseño mediante Repository Manager. Los usuarios deben tener además los privilegios Crear, editar y eliminar objetos en tiempo de ejecución y Crear, editar y eliminar orígenes y destinos.</li> <li>- Revertir a una versión anterior de los objetos de diseño.</li> <li>- Validar asignaciones, mapplets y funciones definidas por el usuario.</li> </ul>

## Gestionar versiones de objetos de diseño

Si tiene una opción de desarrollo basado en equipos, asigne a los usuarios el privilegio Administrar versiones de objetos de diseño en un repositorio con versión de PowerCenter. Los usuarios pueden cambiar el estado, recuperar y purgar versiones de objetos de diseño. Los usuarios también pueden proteger y deshacer la protección realizada por otros usuarios.

El privilegio Administrar versiones de objetos de diseño incluye el privilegio de Crear, editar y eliminar objetos de diseño.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar versiones de objetos de diseño:

Permiso	Descripción
Lectura y escritura en carpeta	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Cambiar el estado de los objetos de diseño.</li> <li>- Proteger y deshacer desprotección de objetos de diseño desprotegidos por otros usuarios.</li> <li>- Purgar versiones de objetos de diseño.</li> <li>- Recuperar objetos de diseño eliminados.</li> </ul>

## Grupo de privilegios Orígenes y destinos

Los privilegios del grupo de privilegios Orígenes y destinos y los permisos de los objetos del repositorio de PowerCenter determinan las acciones que pueden completar los usuarios en los siguientes objetos de origen y destino:

- Cubos
- Dimensiones
- Definiciones de origen
- Definiciones de destino

Los usuarios a los que se les han asignado permisos pero no privilegios pueden realizar algunas acciones para objetos de origen y destino. La siguiente tabla muestra las acciones que pueden realizar los usuarios cuando solo se les asignan permisos:

Permiso	Descripción
Lectura en carpeta	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Comparar objetos de origen y destino.</li> <li>- Exportar objetos de origen y destino.</li> <li>- Obtener una vista previa de datos de origen y destino.</li> <li>- Recibir mensajes de notificación del repositorio de PowerCenter.</li> <li>- Ejecutar linaje de datos en objetos de origen y destino. Los usuarios también deben contar con el privilegio Ver linaje para el servicio de Metadata Manager y permiso de lectura en los objetos de metadatos en el catálogo de Metadata Manager.</li> <li>- Buscar objetos de origen y destino.</li> <li>- Ver objetos de origen y destino, dependencias de objetos de origen y destino e historial de objetos de origen y destino.</li> </ul>
Lectura en carpeta compartida Lectura y escritura en carpeta de destino	Crear accesos directos

**Nota:** Para realizar acciones en objetos de origen y destino, los usuarios deben contar también con el privilegio apropiado en el grupo de privilegios Herramientas.



## Privilegio de Crear, editar y eliminar orígenes y destinos

Los usuarios a los que se les ha asignado el privilegio Crear, editar y eliminar orígenes y destinos pueden crear, editar y eliminar cubos, dimensiones, definiciones de origen y definiciones de destino.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Crear, editar y eliminar orígenes y destinos:

Permiso	Descripción
Lectura en carpeta original Lectura y escritura en carpeta de destino	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Copiar objetos de origen y destino en otra carpeta.</li><li>- Copiar objetos de origen y destino en otro repositorio de PowerCenter. Los usuarios también deben contar con el privilegio Crear, editar y eliminar orígenes y destinos en el repositorio de destino.</li></ul>
Lectura y escritura en carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Cambiar comentarios para un objeto de origen o de destino con versión.</li><li>- Proteger y deshacer una desprotección de objetos de origen y destino protegidos por sus correspondientes cuentas de usuario.</li><li>- Desproteger objetos de origen y destino.</li><li>- Copiar y pegar objetos de origen y destino en la misma carpeta.</li><li>- Crear, editar y eliminar objetos de origen y destino.</li><li>- Importar funciones SAP.</li><li>- Importar objetos de origen y destino mediante Designer. Los usuarios también deben contar con el privilegio Crear, editar y eliminar objetos de diseño.</li><li>- Importar objetos de origen y destino mediante el administrador de repositorios. Los usuarios también deben contar con los privilegios Crear, editar y eliminar objetos de diseño y Eliminar objetos de tiempo de ejecución.</li><li>- Generar y ejecutar SQL para crear destinos en una base de datos relacional.</li><li>- Revertir a una versión anterior de un objeto de origen o de destino.</li></ul>

## Privilegio Administrar versiones de origen y destino

Si tiene una opción de desarrollo basado en equipos, asigne a los usuarios el privilegio Administrar versiones de origen y destino en un repositorio con versión de PowerCenter. Los usuarios pueden cambiar el estado, recuperar y purgar versiones de objetos de origen y destino. Los usuarios también pueden proteger y deshacer la protección realizada por otros usuarios.

El privilegio Administrar versiones de origen y destino incluye el privilegio Crear, editar y eliminar orígenes y destinos.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar versiones de origen y destino:

Permiso	Descripción
Lectura y escritura en carpeta	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Cambiar el estado de objetos de origen y destino.</li> <li>- Proteger y deshacer la protección de objetos de origen y destino desprotegidos por otros usuarios.</li> <li>- Purgar versiones de objetos de origen y destino.</li> <li>- Recuperar objetos de origen y destino.</li> </ul>

## Grupo de privilegios Objetos de tiempo de ejecución

Los privilegios del grupo de privilegios Objetos en tiempo de ejecución, los permisos del objeto del repositorio de PowerCenter y los permisos del objeto de dominio determinan las acciones que los usuarios pueden realizar en los siguientes objetos en tiempo de ejecución:

- Objetos de configuración de sesión
- Tareas
- Flujos de trabajo
- Worklets

Algunas tareas del objeto en tiempo de ejecución vienen determinadas por la función de administrador, no por los privilegios o los permisos. Un usuario con la función de administrador para el servicio de repositorio de PowerCenter puede eliminar un servicio de integración de PowerCenter desde el navegador del administrador de flujos de trabajo.

Los usuarios a los que se les ha asignado permisos pero no privilegios pueden realizar algunas acciones de objetos de tiempo de ejecución. La siguiente tabla muestra las acciones que pueden realizar los usuarios cuando solo se les asignan permisos:

Permiso	Descripción
Lectura en carpeta	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Comparar objetos en tiempo de ejecución.</li> <li>- Exportar objetos en tiempo de ejecución.</li> <li>- Recibir mensajes de notificación del repositorio de PowerCenter.</li> <li>- Buscar objetos en tiempo de ejecución.</li> <li>- Usar las variables y los parámetros de asignación en una sesión.</li> <li>- Ver objetos en tiempo de ejecución, las dependencias del objeto y el historial del objeto en tiempo de ejecución.</li> </ul>
Lectura y ejecución en carpeta	<p>Detener y anular tareas y flujos de trabajo iniciados por la cuenta de usuario propia.</p> <p>Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.</p>

**Nota:** Para efectuar acciones en objetos en tiempo de ejecución, los usuarios deben tener también el privilegio adecuado en el grupo de privilegio Herramientas.

## Privilegio de Crear, editar y eliminar objetos de tiempo de ejecución

Los usuarios a los que se les ha asignado el privilegio de Crear, editar y eliminar objetos de tiempo de ejecución pueden crear, editar y eliminar objetos de configuración de sesión, tareas, flujos de trabajo y worklets.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Crear, editar y eliminar objetos de tiempo de ejecución:

Permiso	Descripción
Lectura en carpeta original Lectura y escritura en carpeta de destino	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Copiar tareas, flujos de trabajo o worklets de una carpeta a otra.</li><li>- Copiar tareas, flujos de trabajo o worklets a otro repositorio de PowerCenter. Los usuarios deben tener también el privilegio Crear, editar y eliminar objetos en tiempo de ejecución en el repositorio de destino.</li></ul>
Lectura y escritura en carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Asignar un servicio de integración de PowerCenter a un flujo de trabajo en las propiedades del flujo de trabajo.</li><li>- Asignar un nivel de servicio a un flujo de trabajo.</li><li>- Cambiar comentarios para un objeto en tiempo de ejecución con versión.</li><li>- Proteger y anular la desprotección de los objetos en tiempo de ejecución desprotegidos por la cuenta de usuario propia.</li><li>- Desproteger los objetos en tiempo de ejecución.</li><li>- Copiar y pegar tareas, flujos de trabajo y worklets en la misma carpeta.</li><li>- Crear, editar y eliminar perfiles de datos e iniciar el administrador de perfiles. Los usuarios deben tener también el privilegio Crear, editar y eliminar objetos de diseño.</li><li>- Crear, editar y eliminar objetos de configuración de sesión.</li><li>- Eliminar y validar tareas, flujos de trabajo y worklets.</li><li>- Importar objetos en tiempo de ejecución con el administrador de repositorios. Los usuarios deben tener también los privilegios Crear, editar y eliminar objetos de diseño y Crear, editar y eliminar orígenes y destinos.</li><li>- Importar objetos en tiempo de ejecución con el administrador de flujos de trabajo.</li><li>- Revertir a una versión de objeto anterior.</li></ul>
Lectura y escritura en carpeta Lectura en objeto de conexión	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"><li>- Eliminar y editar tareas, flujos de trabajo y worklets.</li><li>- Reemplazar una conexión de base de datos relacional para todas las sesiones que usan la conexión.</li></ul>

## Privilegio Administrar versiones de objetos de tiempo de ejecución

Si tiene una opción de desarrollo basado en equipos, asigne a los usuarios el privilegio Administrar versiones de objetos de tiempo de ejecución en un repositorio con versión de PowerCenter. Los usuarios pueden cambiar el estado, recuperar y purgar versiones de objetos de tiempo de ejecución. Los usuarios también pueden proteger y deshacer la protección realizada por otros usuarios.

El privilegio Administrar versiones de objetos de tiempo de ejecución incluye el privilegio Crear, editar y eliminar objetos de tiempo de ejecución.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar versiones de objetos de tiempo de ejecución:

Permiso	Descripción
Lectura y escritura en carpeta	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Cambiar el estado de los objetos en tiempo de ejecución.</li> <li>- Proteger y anular la desprotección de los objetos en tiempo de ejecución desprotegidos por otros usuarios.</li> <li>- Purgar versiones de objetos en tiempo de ejecución.</li> <li>- Recuperar objetos eliminados en tiempo de ejecución.</li> </ul>

## Privilegio Supervisar objetos de tiempo de ejecución

Los usuarios a los que se les ha asignado el privilegio Supervisar objetos de tiempo de ejecución pueden supervisar flujos de trabajo y tareas en el supervisor de flujo de trabajo.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Supervisar objetos de tiempo de ejecución:

Permiso	Concede a los usuarios la capacidad de
Lectura en carpeta	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Ver propiedades de los objetos en tiempo de ejecución en el supervisor de flujo de trabajo.</li> <li>- Ver los registros de sesión y de flujo de trabajo en el supervisor de flujo de trabajo.</li> <li>- Ver los detalles del objeto en tiempo de ejecución y del rendimiento en el supervisor de flujo de trabajo.</li> </ul> <p>Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.</p>

## Privilegio Ejecutar objetos de tiempo de ejecución

Los usuarios a los que se les ha asignado el privilegio Ejecutar objetos de tiempo de ejecución pueden iniciar, iniciar en frío y recuperar tareas y flujos de trabajo.

El privilegio Ejecutar objetos de tiempo de ejecución incluye el privilegio de Supervisar objetos de tiempo de ejecución.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Ejecutar objetos de tiempo de ejecución:

Permiso	Descripción
Lectura y ejecución en carpeta	El usuario puede asignar un servicio de integración de PowerCenter a un flujo de trabajo mediante el menú Servicio o el navegador.
Lectura, escritura y ejecución en carpeta Lectura y ejecución en objeto de conexión	<p>El usuario puede depurar una asignación creando una instancia de sesión de depuración o mediante una sesión reutilizable existente. Los usuarios deben tener además el privilegio Crear, editar y eliminar objetos en tiempo de ejecución.</p> <p>Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.</p>

Permiso	Descripción
Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión	El usuario puede depurar una asignación utilizando una sesión no reutilizable existente. Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.
Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Iniciar, iniciar en frío y reiniciar tareas y flujos de trabajo.</li> <li>- Recuperar tareas y flujos de trabajo iniciados por la cuenta de usuario propia.</li> </ul> Si el servicio de integración de PowerCenter usa perfiles de sistema operativo, los usuarios deben tener también permiso en el perfil de sistema operativo. Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.

## Privilegio Administrar la ejecución de objetos de tiempo de ejecución

Los usuarios a los que se les ha asignado el privilegio Administrar la ejecución de objetos de tiempo de ejecución pueden programar y anular la programación de flujos de trabajo. Los usuarios también pueden detener, anular y recuperar tareas y flujos de trabajo iniciados por otros usuarios.

El privilegio Administrar la ejecución de objetos de tiempo de ejecución incluye el privilegio Ejecutar objetos de tiempo de ejecución y el privilegio Supervisar objetos de tiempo de ejecución.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar la ejecución de objetos de tiempo de ejecución:

Permiso	Descripción
Lectura y ejecución en carpeta	El usuario puede truncar entradas de registro de flujos de trabajo y de sesiones.
Lectura y ejecución en carpeta	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Detener y anular tareas y flujos de trabajo iniciados por otros usuarios.</li> <li>- Detener y anular tareas que se recuperaron automáticamente.</li> <li>- Anular la programación de flujos de trabajo.</li> </ul> Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.

Permiso	Descripción
Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Recuperar tareas y flujos de trabajo iniciados por otros usuarios.</li> <li>- Recuperar tareas que se recuperaron automáticamente.</li> </ul> <p>Si el servicio de integración de PowerCenter usa perfiles de sistema operativo, los usuarios deben tener también permiso en el perfil de sistema operativo.</p> <p>Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.</p>
Lectura, escritura y ejecución en carpeta Lectura y ejecución en objeto de conexión	<p>El usuario puede realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>- Crear y editar un programador reutilizable desde el menú Flujos de trabajo &gt; Programadores.</li> <li>- Editar un programador no reutilizable desde las propiedades del flujo de trabajo.</li> <li>- Editar un programador reutilizable desde las propiedades del flujo de trabajo.* Los usuarios deben tener además el privilegio Crear, editar y eliminar objetos en tiempo de ejecución.</li> </ul> <p>Si el servicio de integración de PowerCenter usa perfiles de sistema operativo, los usuarios deben tener también permiso en el perfil de sistema operativo.</p> <p>Cuando el servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el servicio de repositorio de PowerCenter asociado.</p>

## Grupo de privilegios Objetos globales

Los privilegios del grupo de privilegios Objetos globales y los permisos para los objetos del repositorio de PowerCenter determinan las acciones que los usuarios pueden realizar en los siguientes objetos globales:

- Objetos de conexión
- Grupos de implementación
- Etiquetas
- Consultas

Algunas tareas de objetos globales están determinadas por la propiedad de los objetos globales y la función de administrador, y no por los privilegios o permisos. El propietario de los objetos globales o un usuario con la función de administrador para el servicio de repositorio de PowerCenter pueden realizar las siguientes tareas para los objetos globales:

- Configurar permisos para los objetos globales.
- Cambiar el propietario de los objetos globales.
- Eliminar un objeto global.

Los usuarios a los que se les ha asignado permisos pero no privilegios pueden realizar algunas acciones para objetos globales. La siguiente tabla muestra las acciones que pueden realizar los usuarios cuando solo se les asignan permisos:

Permiso	Descripción
Lectura en objeto de conexión	El usuario puede ver objetos de conexión.
Lectura en grupo de implementación	El usuario puede ver grupos de implementación.
Lectura en etiqueta	El usuario puede ver etiquetas.

Permiso	Descripción
Lectura en consulta	El usuario puede ver consultas de objetos.
Lectura y escritura en objeto de conexión	El usuario puede editar objetos de conexión.
Lectura y escritura en etiqueta	El usuario puede editar y bloquear etiquetas.
Lectura y escritura en consulta	El usuario puede editar y validar consultas de objetos.
Lectura y ejecución en consulta	El usuario puede ejecutar consultas de objetos.
Lectura en carpeta Lectura y ejecución en etiqueta	El usuario puede aplicar etiquetas y quitar referencias de etiquetas.

**Nota:** Para realizar acciones en los objetos globales, los usuarios deben tener además el privilegio correspondiente en el grupo de privilegios Herramientas.

## Privilegio Crear conexiones

Los usuarios a los que se les ha asignado el privilegio Crear conexiones pueden crear objetos de conexión.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Crear conexiones:

Permiso	Descripción
-	El usuario puede crear y copiar objetos de conexión.

## Privilegio Administrar grupos de implementación

Si tiene una opción de desarrollo basado en equipos, los usuarios asignados con el privilegio Administrar grupos de implementación en un repositorio con versión de PowerCenter pueden crear, editar, copiar y revertir grupos de implementación. En un repositorio sin versión, los usuarios pueden crear, editar y copiar grupos de implementación.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Administrar grupos de implementación:

Permiso	Descripción
-	El usuario puede crear grupos de implementación.
Lectura y escritura en grupo de implementación	El usuario puede realizar las siguientes acciones: <ul style="list-style-type: none"> <li>- Editar grupos de implementación.</li> <li>- Quitar objetos de un grupo de implementación.</li> </ul>
Lectura en carpeta original Lectura y escritura en grupo de implementación	El usuario puede añadir objetos a un grupo de implementación.

Permiso	Descripción
Lectura en carpeta original Lectura y escritura en carpeta de destino Lectura y ejecución en grupo de implementación	El usuario puede copiar grupos de implementación.
Lectura y escritura en carpeta de destino	El usuario puede revertir grupos de implementación.

## Privilegio Ejecutar grupos de implementación

Los usuarios a los que se les ha asignado el privilegio Ejecutar grupos de implementación pueden copiar un grupo de implementación sin escribir permisos en las carpetas de destino.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Ejecutar grupos de implementación:

Permiso	Descripción
Lectura en carpeta original Ejecutar en grupo de implementación	El usuario puede copiar grupos de implementación.

## Privilegio Crear etiquetas

Si tiene una opción de desarrollo basado en equipos, los usuarios asignados al privilegio Crear etiquetas en un repositorio con versión de PowerCenter pueden crear etiquetas.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Crear etiquetas:

Permiso	Descripción
-	El usuario puede crear etiquetas.

## Privilegio Crear consultas

Los usuarios a los que se les ha asignado el privilegio Crear consultas pueden crear consultas de objetos.

La siguiente tabla muestra los permisos requeridos y las acciones que pueden realizar los usuarios con el privilegio Crear consultas:

Permiso	Descripción
-	El usuario puede crear consultas de objetos.



## Privilegios del Servicio de escucha PowerExchange

Los privilegios del servicio de escucha PowerExchange determina los comandos infacmd pwx que pueden ejecutar los usuarios.

La tabla siguiente describe el privilegio del Servicio de escucha de PowerExchange en el grupo de privilegios de comandos de información:

Nombre del privilegio	Descripción
listtask	Ejecute el comando infacmd pwx ListTaskListener.

La tabla siguiente describe cada privilegio del Servicio de escucha de PowerExchange en el grupo de privilegios de comandos de administración:

Nombre del privilegio	Descripción
cerrar	Ejecute el comando infacmd pwx CloseListener.
closeforce	Ejecute el comando infacmd pwx CloseForceListener.
stoptask	Ejecute el comando infacmd pwx StopTaskListener.

## Privilegios del Servicio de registrador PowerExchange

Los privilegios del servicio de registrador PowerExchange determinan los comandos infacmd pwx que pueden ejecutar los usuarios.

La tabla siguiente describe cada privilegio del servicio de registrador PowerExchange en el grupo de privilegios de comandos de información:

Nombre del privilegio	Descripción
displayall	Ejecute el comando infacmd pwx DisplayAllLogger.
displaycpu	Ejecute el comando infacmd pwx DisplayCPULogger.
displaycheckpoints	Ejecute el comando infacmd pwx DisplayCheckpointsLogger.
displayevents	Ejecute el comando infacmd pwx DisplayEventsLogger.
displaymemory	Ejecute el comando infacmd pwx DisplayMemoryLogger.
displayrecords	Ejecute el comando infacmd pwx DisplayRecordsLogger.
displaystatus	Ejecute el comando infacmd pwx DisplayStatusLogger.

La tabla siguiente describe cada privilegio del servicio de registrador PowerExchange en el grupo de privilegios de los comandos de administración.

Nombre del privilegio	Descripción
condensar	Ejecute el comando infacmd pwx CondenseLogger.
fileswitch	Ejecute el comando infacmd pwx FileSwitchLogger.
apagar	Ejecute el comando infacmd pwx ShutDownLogger.

## Privilegios del servicio de programador

Los privilegios del servicio de programador determinan las acciones que los usuarios pueden realizar en los programas y trabajos programados.

La siguiente tabla describe los privilegios y permisos requeridos del Servicio de programador:

Privilegio	Descripción	Requiere permiso en
Crear programa	El usuario puede crear programas. Para crear un programa, el usuario también debe tener el privilegio de administración de la aplicación en el servicio de integración de datos.	<ul style="list-style-type: none"> <li>- Servicio de programador</li> <li>- El servicio de integración de datos que ejecuta las tareas que el usuario desea programar</li> </ul>
Editar programa	El usuario puede editar, ver y reanudar programas. Para editar un programa, el usuario también debe tener el privilegio de administración de la aplicación en el servicio de integración de datos.	<ul style="list-style-type: none"> <li>- Servicio de programador</li> <li>- El servicio de integración de datos que ejecuta las tareas que el usuario desea programar</li> </ul>
Eliminar programa	El usuario puede eliminar programas.	Servicio de programador
Ver programas	El usuario puede acceder a la vista <b>Programaciones</b> y a los programas.	Servicio de programador

# Privilegios del servicio de Test Data Manager

Los privilegios del servicio de Test Data Manager determinan las acciones que los usuarios pueden realizar con Test Data Manager. Configure privilegios en la ficha **Seguridad** de la Herramienta del administrador.

En la siguiente tabla, se describe cada grupo de privilegios de Test Data Manager.

Grupo de privilegios	Descripción
Administración	Incluye los privilegios para crear y administrar conexiones y funciones, asignar privilegios a usuarios y grupos de usuarios de Informatica Administrator, administrar repositorios, añadir licencias y configurar atributos de flujo de trabajo y proyecto. <b>Nota:</b> Antes de crear usuarios y grupos, el usuario administrador de Informatica predeterminado debe asignar privilegios de administración de seguridad al usuario administrador de Test Data Manager.
Dominios de datos	Incluye los privilegios para ver y administrar dominios de datos en Test Data Manager.
Enmascaramiento de datos	Incluye los privilegios para ver y administrar reglas de enmascaramiento y asignaciones de directivas en Test Data Manager.
Subconjunto de datos	Incluye los privilegios para ver y administrar objetos de subconjunto como entidades, grupos y plantillas en Test Data Manager.
Directivas	Incluye los privilegios para ver y administrar directivas en Test Data Manager.
Proyectos	Incluye los privilegios para ver y administrar proyectos, auditar e importar metadatos y ejecutar planes y flujos de trabajo en Test Data Manager.
Reglas	Incluye los privilegios para ver y administrar reglas de enmascaramiento y de generación en Test Data Manager.
Generación de datos	Incluye los privilegios para ver y administrar la generación de datos de prueba en Test Data Manager.

## Grupo de privilegios Administración

Los privilegios del grupo de privilegios Administración determinan las tareas de administración que pueden realizar los administradores de Test Data.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Administración y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Privilegios incluidos	Permiso	Descripción
Administrar preferencias	-	Escritura	<p>El usuario puede realizar las siguientes acciones en Informatica Administrator y en Test Data Manager:</p> <ul style="list-style-type: none"><li>- Crear funciones.</li><li>- Editar funciones.</li><li>- Eliminar funciones.</li><li>- Ver funciones.</li><li>- Asociar funciones a usuarios.</li><li>- Asociar privilegios a usuarios.</li><li>- Asociar funciones a grupos de usuarios.</li><li>- Asociar privilegios a grupos de usuarios.</li><li>- Añadir licencias.</li><li>- Configurar el repositorio de TDM.</li><li>- Configurar el repositorio de PowerCenter.</li><li>- Configurar niveles de confidencialidad de dominio de datos.</li><li>- Configure un repositorio de Test Data Warehouse.</li><li>- Configure un Test Data Warehouse.</li><li>- Configurar atributos personalizados del proyecto.</li><li>- Configurar atributos de generación de flujo de trabajo.</li><li>- Habilitar la detección de datos.</li><li>- Configurar servicios de creación de perfiles.</li><li>- Ver objetos de administración.</li><li>- Configure las opciones de indexación de búsqueda de palabras claves.</li></ul>
Ver conexiones	-	Lectura	<p>El usuario puede realizar las siguientes acciones en la página Conexiones de Test Data Manager:</p> <ul style="list-style-type: none"><li>- Ver conexiones.</li><li>- Probar conexiones.</li></ul>
Administrar conexiones	Ver conexiones	Escritura	<p>El usuario puede realizar las siguientes acciones en la página Conexiones de Test Data Manager:</p> <ul style="list-style-type: none"><li>- Crear conexiones.</li><li>- Editar conexiones.</li><li>- Eliminar conexiones.</li><li>- Ver conexiones.</li><li>- Probar conexiones.</li><li>- Configure un repositorio de Test Data Warehouse.</li><li>- Configure un Test Data Warehouse.</li></ul>

## Grupo de privilegios Conexiones

Los privilegios del grupo de privilegios Conexiones determinan las tareas que los usuarios pueden realizar en la página Conexiones del entorno de trabajo de TDM. En la siguiente tabla se enumeran los privilegios del grupo de privilegios Conexiones y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver conexiones	-	Lectura	El usuario puede ver las conexiones y probar conexiones en el entorno de trabajo de TDM.
Administrar conexiones	Ver conexiones	Escritura	El usuario puede realizar las siguientes acciones en la página Conexiones en el entorno de trabajo de TDM: <ul style="list-style-type: none"><li>- Crear conexiones.</li><li>- Editar conexiones.</li><li>- Eliminar conexiones.</li><li>- Ver conexiones.</li><li>- Probar conexiones.</li></ul>

## Grupo de privilegios Dominios de datos

Los privilegios del grupo de privilegios Dominios de datos determinan las tareas que los usuarios pueden realizar en los dominios de datos en la página Directivas de Test Data Manager.

En la siguiente tabla se indican los privilegios del grupo de privilegios Dominios de datos y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver dominios de datos	-	Lectura	El usuario puede ver dominios de datos en Test Data Manager.
Administrar dominios de datos	Ver dominios de datos	Escritura	El usuario puede realizar las siguientes acciones en los dominios de datos en Test Data Manager: <ul style="list-style-type: none"><li>- Crear dominios de datos.</li><li>- Editar dominios de datos.</li><li>- Eliminar dominios de datos.</li><li>- Ver dominios de datos.</li></ul>

## Grupo de privilegios Enmascaramiento de datos

Los privilegios del grupo de privilegios Enmascaramiento de datos determinan las tareas que los usuarios pueden realizar en la vista Proyecto | Definir | Enmascaramiento de datos de Test Data Manager. Desde esta vista, puede asignar reglas y directivas a columnas de tablas.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Enmascaramiento de datos y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver enmascaramiento de datos	-	Lectura	El usuario puede ver asignaciones de reglas de enmascaramiento de datos en Test Data Manager.
Administrar enmascaramiento de datos	Ver enmascaramiento de datos	Escritura	El usuario puede realizar las siguientes acciones de asignación de enmascaramiento de datos en Test Data Manager: <ul style="list-style-type: none"><li>- Añadir asignaciones de reglas y directivas.</li><li>- Eliminar asignaciones de reglas y directivas.</li><li>- Reemplazar propiedades de reglas.</li><li>- Ver asignaciones de enmascaramiento de datos.</li></ul>

## Grupo de privilegios Subconjunto de datos

Los privilegios del grupo de privilegios Subconjunto de datos determinan las tareas que los usuarios pueden realizar en los objetos del subconjunto de datos en Test Data Manager.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Subconjunto de datos y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver subconjuntos de datos	-	Lectura	El usuario puede realizar las siguientes acciones de subconjunto de datos en Test Data Manager: <ul style="list-style-type: none"><li>- Ver grupos.</li><li>- Ver plantillas.</li><li>- Ver entidades.</li><li>- Ver objetos de proyectos recientes.</li></ul>
Administrar subconjuntos de datos	Ver subconjuntos de datos	Escritura	El usuario puede realizar las siguientes acciones de subconjunto de datos en Test Data Manager: <ul style="list-style-type: none"><li>- Crear grupos.</li><li>- Editar grupos.</li><li>- Eliminar grupos.</li><li>- Añadir parámetros de grupo.</li><li>- Crear plantillas.</li><li>- Editar plantillas.</li><li>- Eliminar plantillas.</li><li>- Añadir parámetros de plantilla.</li><li>- Crear entidades.</li><li>- Editar entidades.</li><li>- Eliminar entidades.</li><li>- Añadir criterios de entidad.</li><li>- Habilitar relaciones.</li><li>- Deshabilitar relaciones.</li><li>- Editar relaciones.</li><li>- Revisar cambios y actuar sobre ellos.</li><li>- Marcar la revisión de cambios como finalizada.</li></ul>

## Grupo de privilegios Directivas

Los privilegios del grupo de privilegios Directivas determinan las tareas que los usuarios pueden realizar en las directivas en Test Data Manager.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Directivas y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver directivas	-	Lectura	Los usuarios pueden ver las directivas en Test Data Manager.
Administrar directivas	Ver directivas	Escritura	El usuario puede realizar las siguientes acciones de directivas en Test Data Manager: <ul style="list-style-type: none"><li>- Crear directivas.</li><li>- Editar directivas.</li><li>- Eliminar directivas.</li><li>- Ver directivas.</li></ul>



## Grupo de privilegios Proyectos

Los privilegios del grupo de privilegios Proyectos determinan las tareas que los usuarios pueden realizar en los proyectos de Test Data Manager.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Proyectos y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Privilegios incluidos	Permiso	Descripción
Ver proyecto	-	Lectura	El usuario puede realizar las siguientes acciones en los proyectos de Test Data Manager: <ul style="list-style-type: none"><li>- Ver proyectos.</li><li>- Ver planes.</li><li>- Ver informes de detalles de planes.</li><li>- Ver informes de auditoría de planes.</li><li>- Ver proyectos recientes</li><li>- Crear planes de Test Data Warehouse</li><li>- Administrar planes de Test Data Warehouse</li><li>- Generar planes de Test Data Warehouse</li><li>- Ejecutar planes de Test Data Warehouse</li></ul>
Administrar proyecto	Ver proyecto	Escritura	El usuario puede realizar las siguientes acciones en los proyectos de Test Data Manager: <ul style="list-style-type: none"><li>- Crear proyectos.</li><li>- Editar proyectos.</li><li>- Eliminar proyectos.</li><li>- Ver proyectos.</li><li>- Asociar usuarios a proyectos.</li><li>- Asociar grupos de usuarios a proyectos.</li><li>- Asociar o eliminar reglas para los proyectos.</li><li>- Asociar o eliminar directivas para los proyectos.</li><li>- Crear planes.</li><li>- Editar planes.</li><li>- Eliminar planes.</li><li>- Generar planes.</li></ul>

Privilegio	Privilegios incluidos	Permiso	Descripción
Detectar proyecto	-	Escritura	<p>El usuario puede realizar las siguientes acciones de detección en los proyectos de Test Data Manager:</p> <ul style="list-style-type: none"> <li>- Clasificar tablas.</li> <li>- Marcar la detección como finalizada.</li> <li>- Asociar dominios de datos a columnas.</li> <li>- Marcar columnas como limitadas.</li> <li>- Marcar columnas como confidenciales.</li> <li>- Establecer columna de valor similar.</li> <li>- Quitar columnas de valor similar.</li> <li>- Añadir claves principales.</li> <li>- Eliminar claves principales.</li> <li>- Crear restricciones lógicas.</li> <li>- Ver restricciones lógicas.</li> <li>- Editar restricciones lógicas.</li> <li>- Eliminar restricciones lógicas.</li> <li>- Ver proyectos.</li> <li>- Ver dominios de datos de perfil.</li> <li>- Aprobar o rechazar dominios de datos de perfil.</li> <li>- Marcar clasificación de dominio de datos como finalizada.</li> <li>- Ver claves principales de perfil.</li> <li>- Aprobar o rechazar claves principales de perfil.</li> <li>- Marcar la detección de clave principal como finalizada.</li> <li>- Ver entidades de perfil.</li> <li>- Aprobar o rechazar entidades de perfil.</li> <li>- Marcar la detección de entidad como finalizada.</li> <li>- Ver análisis de riesgo de proyecto.</li> <li>- Ver distribución reciente de datos confidenciales del proyecto.</li> </ul>
Generar proyecto	-	Escritura	El usuario puede generar flujos de trabajo en Test Data Manager.
Ejecutar proyecto	-	Escritura	<p>El usuario puede realizar las siguientes acciones de ejecución en los proyectos de Test Data Manager:</p> <ul style="list-style-type: none"> <li>- Ejecutar planes.</li> <li>- Ejecutar flujos de trabajo.</li> <li>- Detener flujos de trabajo.</li> <li>- Anular flujos de trabajo.</li> <li>- Recuperar flujos de trabajo.</li> <li>- Visualizar la ejecución del plan.</li> </ul>
Supervisar proyecto	-	Lectura	<p>El usuario puede realizar las siguientes acciones de supervisión en los proyectos de Test Data Manager:</p> <ul style="list-style-type: none"> <li>- Supervisar tareas del proyecto.</li> <li>- Ver registros de tareas del proyecto.</li> <li>- Supervisar tareas de varios proyectos.</li> <li>- Ver registros de tareas de varios proyectos.</li> </ul>
Auditar proyecto	-	Lectura	El usuario puede ver la actividad reciente en los proyectos y planes de Test Data Manager.
Importar metadatos	-	Escritura	<p>El usuario puede realizar las siguientes acciones en los proyectos de Test Data Manager:</p> <ul style="list-style-type: none"> <li>- Importar orígenes.</li> <li>- Eliminar orígenes.</li> </ul>

**Nota:** Un usuario con el privilegio Administrar proyecto debe tener al menos los siguientes niveles de privilegios para poder crear un plan con cada componente.

- Ver conexión desde el grupo de privilegios Administración. Para crear un plan.
- Ver subconjuntos de datos desde el grupo de privilegios Subconjunto de datos. Para crear un plan con los componentes de subconjunto.
- Ver reglas de enmascaramiento desde el grupo de privilegios Reglas. Para crear un plan con los componentes de enmascaramiento.
- Ver reglas de generación desde el grupo de privilegios Reglas. Para crear un plan con la generación de componentes.

## Grupo de privilegios Reglas

Los privilegios del grupo de privilegios Reglas determinan las tareas que los usuarios pueden realizar en las reglas de enmascaramiento de datos y de generación de datos en Test Data Manager.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Enmascaramiento de datos y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver reglas de enmascaramiento	-	Lectura	El usuario puede ver las reglas de enmascaramiento en Test Data Manager.
Administrar reglas de enmascaramiento	Ver reglas de enmascaramiento	Escritura	El usuario puede realizar las siguientes acciones en las reglas de enmascaramiento de datos en Test Data Manager: <ul style="list-style-type: none"><li>- Crear reglas de enmascaramiento.</li><li>- Editar reglas de enmascaramiento.</li><li>- Eliminar reglas de enmascaramiento.</li><li>- Ver reglas de enmascaramiento.</li></ul>

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver reglas de generación	-	Lectura	El usuario puede ver reglas de generación de datos en Test Data Manager.
Administrar reglas de generación	Ver reglas de generación	Escritura	El usuario puede realizar las siguientes acciones en las reglas de generación de datos en Test Data Manager: <ul style="list-style-type: none"> <li>- Crear reglas de generación.</li> <li>- Editar reglas de generación.</li> <li>- Eliminar reglas de generación.</li> <li>- Ver reglas de generación.</li> </ul>

## Grupo de privilegios Generación de datos

Los privilegios del grupo de privilegios Generación de datos determinan las tareas de generación de datos de prueba que los usuarios pueden realizar en Test Data Manager.

En la siguiente tabla, se indican los privilegios del grupo de privilegios Generación de datos y los permisos necesarios para realizar una tarea en un objeto:

Privilegio	Incluye los privilegios	Permiso	Descripción
Ver la generación de datos	-	Lectura	El usuario puede ver asignaciones de reglas de generación de datos en Test Data Manager.
Administrar la generación de datos	Ver la generación de datos	Escritura	El usuario puede realizar las siguientes acciones en la generación de datos en Test Data Manager: <ul style="list-style-type: none"> <li>- Ver asignaciones de reglas de generación de datos.</li> <li>- Añadir asignaciones de reglas de generación de datos.</li> <li>- Eliminar asignaciones de reglas de generación de datos.</li> <li>- Reemplazar asignaciones de reglas de generación de datos.</li> </ul>

## Cómo administrar funciones

Una función es un conjunto de privilegios que se pueden asignar a usuarios y a grupos. Puede asignar los siguientes tipos de funciones:

- Definidas por el sistema. Funciones que puede editar o eliminar.
- Personalizadas. Funciones que puede crear, editar y eliminar.

Una función incluye privilegios para el dominio o un tipo de servicio de la aplicación. Asigne funciones a usuarios o grupos para el dominio o para cada servicio de aplicación del dominio. Por ejemplo, puede crear

una función de Developer que incluya privilegios para el servicio de repositorio de PowerCenter. Un dominio puede contener varios servicios de repositorio de PowerCenter. Puede asignar la función de Developer a un usuario para el servicio de repositorio de PowerCenter de desarrollo. Puede asignar una función diferente para ese usuario para el servicio de repositorio de PowerCenter de producción.

Una función incluye privilegios para el dominio o un tipo de servicio de la aplicación. Asigne funciones a usuarios o grupos para el dominio o para cada servicio de aplicación del dominio.

Una función incluye privilegios para el dominio o un tipo de servicio de la aplicación. Asigne funciones a usuarios o grupos para el dominio o para cada servicio de aplicación del dominio.

UMSM tiene los siguientes tipos de funciones:

- **Administrador.** Se trata de una función definida por el sistema que tiene privilegios para administrar la herramienta Administrator. Con esta función, puede crear y administrar cuentas de usuario, crear el servicio de Ultra Messaging y configurarlo, configurar los componentes de UMSM e implementaciones de UM.
- **Operador.** Se trata de una función personalizada que tiene privilegios para supervisar las implementaciones de UM.

Al seleccionar una función en la sección Funciones del navegador, puede ver todos los usuarios y grupos a quienes se les asignó directamente la función para los servicios del dominio y de la aplicación. Puede ver las funciones asignadas por usuarios y grupos o por servicios. Para desplazarse hasta un usuario o grupo de la sección Asignaciones, haga clic con el botón derecho en un usuario o grupo y seleccione Desplazarse hasta el elemento.

Puede buscar funciones definidas por el sistema y personalizadas.

## Funciones definidas por el sistema

Una función definida por el sistema es aquella que no se puede editar ni eliminar. La función de administrador es una función definida por el sistema.

Cuando se asigna la función de administrador a un usuario o grupo para el dominio, el servicio del analista, el servicio de integración de datos, el servicio de Metadata Manager, el servicio de repositorio de modelos o el servicio de repositorio de PowerCenter, al usuario o grupo en cuestión se le conceden todos los privilegios para el servicio. La función de administrador omite la comprobación de permisos. Los usuarios con la función de administrador pueden acceder a todos los objetos administrados por el servicio.

Cuando se asigna la función de administrador a un usuario o grupo para el dominio, el servicio de integración de datos o el servicio de repositorio de modelos, al usuario o grupo en cuestión se le conceden todos los privilegios para el servicio. La función de administrador omite la comprobación de permisos. Los usuarios con la función de administrador pueden acceder a todos los objetos administrados por el servicio.

Cuando asigne la función de administrador a un usuario o grupo para el dominio o servicio de Ultra Messaging, al usuario o grupo en cuestión se le conceden todos los privilegios para el servicio. La función de administrador omite la comprobación de permisos. Los usuarios con la función de administrador pueden acceder a todos los objetos administrados por el servicio.

## Función de administrador

Al asignar la función de administrador a un usuario o grupo para el dominio, el servicio de integración de datos o el servicio de repositorio de PowerCenter, el usuario o el grupo podrán realizar algunas tareas determinadas por la función de administrador y no por privilegios ni permisos.

Al asignar la función de administrador a un usuario o grupo para el dominio o el servicio de integración de datos, el usuario o el grupo podrán realizar algunas tareas determinadas por la función de administrador y no por privilegios ni permisos.

Al asignar la función de administrador a un usuario o grupo para el dominio o el servicio de Ultra Messaging, el usuario o el grupo podrán realizar algunas tareas determinadas por la función de administrador y no por privilegios ni permisos.

Puede asignar a un usuario o grupo todos los privilegios para el dominio, el servicio de integración de datos o el servicio de repositorio de PowerCenter y, a continuación, conceder al usuario o al grupo todos los permisos sobre todos los objetos del dominio o del repositorio de PowerCenter. Sin embargo, dicho usuario o grupo no puede realizar las tareas determinadas por la función de administrador.

Puede asignar a un usuario o grupo todos los privilegios para el dominio o el servicio de integración de datos y, a continuación, conceder al usuario o al grupo todos los permisos sobre todos los objetos del dominio. Sin embargo, dicho usuario o grupo no puede realizar las tareas determinadas por la función de administrador.

Puede asignar a un usuario o grupo todos los privilegios para el dominio o el servicio de Ultra Messaging y, a continuación, conceder al usuario o al grupo todos los permisos sobre todos los objetos del dominio. Sin embargo, dicho usuario o grupo no puede realizar las tareas determinadas por la función de administrador.

Por ejemplo, un usuario al que se le haya asignado la función de administrador para el dominio puede configurar las propiedades de dicho dominio en la herramienta Administrator. Sin embargo, un usuario al que se le hayan asignado todos los privilegios y permisos de dominio sobre dicho dominio no puede configurar las propiedades del mismo.

En la siguiente tabla, se enumeran las tareas determinadas por la función del administrador para el dominio, el servicio de integración de datos y el servicio de repositorio de PowerCenter:

En la siguiente tabla, se enumeran las tareas determinadas por la función del administrador para el dominio o el servicio de integración de datos:

En la siguiente tabla, se enumeran las tareas determinadas por la función del administrador para el dominio o el servicio de Ultra Messaging:

Servicio	Tareas
Dominio	<ul style="list-style-type: none"> <li>- Configurar las propiedades del dominio.</li> <li>- Crear los perfiles del sistema operativo.</li> <li>- Eliminar los perfiles del sistema operativo.</li> <li>- Conceder permiso sobre el dominio y los perfiles del sistema operativo.</li> <li>- Administrar y purgar eventos de registro.</li> <li>- Recibir alertas del dominio.</li> <li>- Ejecutar el informe de licencia.</li> <li>- Ver los eventos de registro de actividad del usuario.</li> <li>- Cerrar el dominio.</li> <li>- Acceder al asistente para actualización de servicios.</li> </ul>
Servicio de integración de datos	<ul style="list-style-type: none"> <li>- Actualizar el servicio de integración de datos mediante el menú Acciones.</li> </ul>
Servicio de repositorio de PowerCenter	<ul style="list-style-type: none"> <li>- Asignar perfiles del sistema operativo a carpetas del repositorio si el servicio de integración de PowerCenter utiliza perfiles de sistema operativo.</li> <li>- Cambiar el propietario de carpetas y objetos globales.*</li> <li>- Configurar permisos de carpeta y de objeto global.*</li> <li>- Conectarse al servicio de integración de PowerCenter desde el cliente de PowerCenter al ejecutar el servicio de integración de PowerCenter en modo seguro.</li> <li>- Eliminar un servicio de integración de PowerCenter desde el navegador del administrador de flujos de trabajo.</li> <li>- Eliminar carpetas y objetos globales.*</li> <li>- Designar carpetas para compartirlas.*</li> <li>- Editar el nombre y la descripción de las carpetas.*</li> </ul> <p>*El propietario del objeto global o de la carpeta del repositorio de PowerCenter también pueden realizar estas tareas.</p>

Servicio	Tareas
Dominio	<ul style="list-style-type: none"> <li>- Configurar las propiedades del dominio.</li> <li>- Conceder permiso para el dominio.</li> <li>- Administrar y purgar eventos de registro.</li> <li>- Recibir alertas del dominio.</li> <li>- Ver los eventos de registro de actividad del usuario.</li> </ul>

Servicio	Tareas
Dominio	<ul style="list-style-type: none"> <li>- Configurar las propiedades del dominio.</li> <li>- Conceder permiso para el dominio.</li> <li>- Administrar y purgar eventos de registro.</li> <li>- Recibir alertas del dominio.</li> <li>- Ver los eventos de registro de actividad del usuario.</li> </ul>

## Funciones personalizadas

Una función personalizada es una función que se puede editar o eliminar.

La Herramienta del administrador incluye de forma predeterminada las siguientes funciones personalizadas:

- Función personalizada del servicio del analista
- Funciones personalizadas del servicio de Metadata Manager
- Función personalizada del operador
- Funciones personalizadas del servicio de repositorio de PowerCenter
- Funciones personalizadas del servicio de Test Data Manager

Puede editar los privilegios de estas funciones o eliminar las funciones. También puede crear sus propias funciones personalizadas.

### Creación de funciones personalizadas

Cuando cree un rol personalizado, asignará privilegios al rol para el dominio o para un tipo de servicio de aplicación. Un rol puede incluir privilegios para uno o más servicios.

1. En la herramienta del administrador, haga clic en la ficha Seguridad.
2. En el menú Acciones de seguridad, haga clic en Crear función.  
Aparecerá el cuadro de diálogo Crear rol.
3. Especifique las siguientes propiedades de la función:

Propiedad	Descripción
Nombre	Nombre de la función. El nombre del rol no distingue mayúsculas de minúsculas y no puede superar los 128 caracteres. No puede incluir tabulaciones, caracteres de nueva línea o los siguientes caracteres especiales: , + " \ < > ; / * % ? El nombre puede incluir un carácter de espacio ASCII siempre y cuando no sea el primer y último carácter. No se permiten otros caracteres de espacio.
Descripción	Descripción de la función. La descripción no puede superar los 765 caracteres ni puede incluir tabulaciones, caracteres de nueva línea o los siguientes caracteres especiales: < > "

4. Haga clic en la ficha Privilegios.
5. Expanda el dominio o un tipo de servicio de aplicación.
6. Seleccione los privilegios que se asignarán a la función del dominio o el tipo de servicio de aplicación.
7. Haga clic en Aceptar.

### Cómo editar propiedades para funciones personalizadas

Cuando edite una función personalizada, podrá cambiar la descripción de la función. No puede modificar el nombre de la función.

1. En Administrator Tool, haga clic en la ficha Seguridad.
2. En la sección Funciones del navegador, seleccione una función.
3. Haga clic en Editar.
4. Cambie la descripción de la función y haga clic en Aceptar.



## Cómo editar privilegios asignados a funciones personalizadas

Puede modificar los privilegios asignados a una función personalizada para el dominio y para cada tipo de servicio de aplicación.

1. En la herramienta del administrador, haga clic en la ficha Seguridad.
2. Seleccione una función en la sección Funciones del navegador.
3. Haga clic en la ficha Privilegios.
4. Haga clic en Editar.  
Se abrirá el cuadro de diálogo Editar funciones y privilegios.
5. Expanda el dominio o un tipo de servicio de aplicación.
6. Para asignar privilegios a la función, seleccione los privilegios del dominio o el tipo de servicio de aplicación.
7. Para quitar privilegios a la función, elimine los privilegios del dominio o el tipo de servicio de aplicación.
8. Repita los pasos para cambiar los privilegios de cada tipo de servicio.
9. Haga clic en Aceptar.

## Cómo eliminar funciones personalizadas

Si elimina una función personalizada, la función personalizada y todos los privilegios que incluía se eliminarán de todo usuario o grupo asignado a la función.

Para eliminar una función personalizada, haga clic con el botón derecho sobre la función en la sección Funciones del navegador y seleccione Eliminar función. Confirme que desea eliminar la función.

# Cómo asignar privilegios y funciones a usuarios y grupos

Puede determinar las acciones que los usuarios pueden realizar; para ello, ha de asignar los siguientes elementos a los usuarios y grupos:

- Privilegios. Un privilegio determina las acciones que los usuarios pueden realizar en aplicaciones cliente.
- Funciones. Una función es una recopilación de privilegios. Cuando asigna una función a un usuario o grupo, asigna la recopilación de privilegios que pertenecen a la función.

Aplique las siguientes reglas y directrices al asignar privilegios y funciones a usuarios y grupos:

- Asigne privilegios y funciones a usuarios y grupos para el dominio y para cada servicio de aplicación que se ejecute en el dominio.  
No puede asignar privilegios ni funciones a usuarios ni grupos de un servicio de Metadata Manager o servicio de repositorio de PowerCenter en las situaciones siguientes:
  - El servicio de aplicación no está habilitado.
  - El servicio de repositorio de PowerCenter se está ejecutando en modo exclusivo.
- Puede asignar diferentes privilegios y funciones a un usuario o grupo para cada servicio de aplicación del mismo tipo.
- Una función puede incluir privilegios para el dominio y varios tipos de servicio de aplicación. Al asignar la función a un usuario o grupo para un servicio de aplicación, se asignan los privilegios para dicho tipo de servicio de aplicación al usuario o grupo.

Si cambia los privilegios o las funciones asignadas a un usuario, dicho cambio se aplicará la próxima vez que el usuario inicie sesión.

**Nota:** No obstante, no puede editar los privilegios ni las funciones asignadas a la cuenta de usuario del administrador predeterminado.

## Privilegios heredados

Un usuario o grupo puede heredar privilegios de los siguientes objetos:

- Grupo. Cuando se asignan privilegios a un grupo, todos los subgrupos y usuarios que pertenecen al grupo heredan los privilegios.
- Función. Cuando se asigna una función a un usuario, el usuario hereda los privilegios que pertenecen a la función. Cuando se asigna una función a un grupo, el grupo y todos los subgrupos y usuarios que pertenecen al grupo heredan los privilegios de la función. Los subgrupos y los usuarios no heredan la función.

No se pueden revocar los privilegios heredados de un grupo o función. Es posible asignar privilegios adicionales a un usuario o grupo que no se heredaron de un grupo o función.

En la ficha Privilegios de un usuario o grupo, se muestran todas las funciones y privilegios asignados al usuario o grupo para el dominio y para cada servicio de aplicación. Expanda el dominio o servicio de aplicación para ver las funciones y privilegios asignados para el dominio o servicio. Haga clic en los siguientes elementos para ver información adicional acerca de las funciones y privilegios asignados:

- Nombre de la función asignada. Muestra los detalles de la función en el panel de detalles.
- Icono Información para una función asignada. Destaca todos los privilegios heredados con esa función.

Los privilegios heredados de una función o grupo se muestran con un icono de herencia. La ayuda flotante de un privilegio heredado indica de qué función o grupo el usuario heredó el privilegio.

## Asignación de privilegios y funciones a un usuario o grupo mediante navegación

1. En Administrator Tool, haga clic en la ficha Seguridad.
2. En el navegador, seleccione un usuario o grupo.
3. Haga clic en la ficha Privilegios.
4. Haga clic en Editar.  
Aparecerá el cuadro de diálogo Editar funciones y privilegios.
5. Para asignar funciones, expanda el dominio o un servicio de aplicación en la ficha Funciones.
6. Para conceder funciones, seleccione las funciones que desee asignar al usuario o grupo para el dominio o servicio de aplicación.  
Puede seleccionar cualquier función que incluya privilegios para el tipo de dominio o servicio de aplicación seleccionado.
7. Para revocar funciones, anule la selección de las funciones asignadas al usuario o grupo.
8. Repita los pasos del [5](#) al [7](#) si desea asignar funciones para otro servicio.
9. Para asignar privilegios, haga clic en la ficha Privilegios.
10. Expanda el dominio o un servicio de aplicación.
11. Para conceder privilegios, seleccione los privilegios que desee asignar al usuario o grupo para el dominio o servicio de aplicación.

12. Para revocar privilegios, anule la selección de los privilegios asignados al usuario o grupo.  
No se pueden revocar los privilegios heredados de una función o grupo.
13. Repita los pasos del [10](#) al [12](#) si desea asignar privilegios para otro servicio.
14. Haga clic en Aceptar.

## Visualización de usuarios con privilegios para un servicio

Puede visualizar todos los usuarios que tienen privilegios para el dominio o para un servicio de aplicación.

1. En la herramienta Administrator, haga clic en la ficha Seguridad.
2. En el menú Acciones de seguridad, haga clic en Privilegios del usuario de servicio.  
Se abre el cuadro de diálogo Servicios.
3. Seleccione el dominio o un servicio de aplicación.  
El panel de detalle muestra todos los usuarios que tienen privilegios para el dominio o servicio de aplicación.
4. Haga clic con el botón derecho en un nombre de usuario y haga clic en Navegar al elemento para navegar hasta el usuario.

## Solucionar problemas de privilegios y funciones

**No puedo asignar privilegios ni funciones a los usuarios de un servicio de Metadata Manager o servicio de repositorio de PowerCenter.**

No puede asignar privilegios ni funciones a usuarios ni grupos de un servicio de Metadata Manager o servicio de repositorio de PowerCenter en las situaciones siguientes:

- El servicio de aplicación no está habilitado.
- El servicio de repositorio de PowerCenter se está ejecutando en modo exclusivo.

**Quité un privilegio de un grupo. ¿Por qué algunos usuarios de dicho grupo todavía tienen ese privilegio?**

Puede usar uno de los siguientes métodos para asignar privilegios a un usuario:

- Asignar un privilegio directamente a un usuario.
- Asignar una función a un usuario.
- Asignar un privilegio o función a un grupo al que pertenezca el usuario.

Si quita un privilegio de un grupo, puede asignar directamente el privilegio a los usuarios que pertenecen a dicho grupo o los usuarios pueden heredar el privilegio de una función asignada.

**Tengo asignados todos los privilegios de dominio y permisos de todos los objetos de dominio, pero no puedo efectuar todas las tareas de Herramienta del administrador.**

Algunas de las funciones de la Herramienta del administrador están determinadas por la función de administrador, no por privilegios o permisos. Puede tener asignados todos los privilegios en el dominio y concedidos los permisos completos en todos los objetos del dominio y, aún así, no podrá completar las tareas que determina la función del administrador.

**Tengo asignada la función de administrador para un servicio de aplicación, pero no puedo configurar el servicio de aplicación en la Herramienta del administrador.**

Cuando dispone de la función de administrador para un servicio de aplicación, se trata en realidad de un administrador de la aplicación cliente. Un administrador de aplicación cliente tiene permisos y privilegios completos en una aplicación cliente,

pero no tiene permisos o privilegios en el dominio de Informatica. Un administrador de aplicación cliente no puede iniciar una sesión en la Herramienta del administrador para administrar el servicio de la aplicación cliente para el que tenga privilegios de administrador.

Para administrar un servicio de aplicación en la Herramienta del administrador, debe tener los permisos y los privilegios de dominio adecuados.

**Tengo asignada la función de administrador para el servicio de repositorio de PowerCenter, pero no puedo usar el Repository Manager para efectuar una depuración avanzada de los objetos o para crear extensiones de metadatos reutilizables.**

Debe tener el privilegio de dominio Administrar servicios y el permiso para el servicio de repositorio de PowerCenter en la Herramienta del administrador para efectuar las siguientes acciones en el Repository Manager:

- Efectuar una purga avanzada de las versiones de objeto en el nivel del repositorio de PowerCenter.
- Crear, editar y eliminar extensiones de metadatos reutilizables.

**Mis privilegios indican que debo poder editar objetos en una aplicación cliente, pero no puedo editar ningún metadato.**

Es posible que no tenga los permisos de objeto necesarios en la aplicación cliente. Aunque tenga el privilegio para efectuar determinadas acciones, es posible que necesite permiso para efectuar una determinada acción en el objeto en cuestión.

**No puedo usar pmrep para conectarme a un nuevo servicio de repositorio de PowerCenter que se ejecuta en modo exclusivo.**

Es posible que el Administrador de servicios no haya sincronizado la lista de usuarios y grupos del repositorio de PowerCenter con la lista de la base de datos de configuración del dominio. Para sincronizar la lista de usuarios y grupos, reinicie el Servicio de repositorio de PowerCenter.

**Tengo asignados todos los privilegios del grupo de privilegios Carpetas para el servicio de repositorio de PowerCenter y tengo permiso de lectura, escritura y ejecución en una carpeta y, sin embargo, no puedo configurar los permisos para dicha carpeta.**

Sólo el propietario de la carpeta o un usuario con la función de administrador para el servicio de repositorio de PowerCenter puede completar las siguientes tareas de administración de carpetas:

- Asignar perfiles de sistema operativo a las carpetas si el servicio de integración de PowerCenter usa perfiles de sistema operativo. Necesita permiso en el perfil de sistema operativo.
- Cambiar el propietario de la carpeta.

- Configurar los permisos de la carpeta.
- Eliminar la carpeta.
- Designar la carpeta que se debe compartir.
- Editar el nombre de la carpeta y la descripción.

Tengo asignada la función de administrador para el servicio de Metadata Manager, pero no puedo crear ni restaurar el repositorio de Metadata Manager.

Para crear o restaurar el repositorio de Metadata Manager, debe estar en el grupo Administrador predeterminado. Los usuarios del grupo Administrador predeterminado tienen más privilegios que los usuarios a los que se les ha asignado la función de administrador para un servicio de aplicación.

He asignado el privilegio Cargar recursos al servicio de Metadata Manager, pero recibo un error informando de que no hay privilegios suficientes cuando intento cargar recursos de Business Glossary.

Para cargar recursos de Business Glossary, son necesarios los privilegios Cargar recurso, Administrar recursos y Ver modelo. También se necesita permiso de escritura en cualquier recurso del glosario empresarial que desee cargar.

# CAPÍTULO 10

## Permisos

Este capítulo incluye los siguientes temas:

- [Resumen de permisos, 190](#)
- [Permisos del objeto de dominio, 193](#)
- [Permisos de conexión, 198](#)
- [Permisos de aplicación y de objeto de aplicación, 200](#)
- [Permisos del servicio de datos SQL, 202](#)
- [Permisos del servicio web, 207](#)

## Resumen de permisos

La seguridad del usuario se administra mediante privilegios y permisos. Los permisos definen el nivel de acceso que los usuarios y los grupos tienen respecto de un objeto.

Aunque un usuario posea el privilegio para realizar determinadas acciones, puede que el usuario también necesite permiso para realizar la acción en un objeto concreto.

Por ejemplo, un usuario tiene privilegio del dominio para administrar servicios y permiso sobre el servicio de repositorio de PowerCenter de desarrollo, pero no sobre el servicio de repositorio de PowerCenter de producción. El usuario puede editar o quitar el servicio de repositorio de PowerCenter de desarrollo, pero no el servicio de repositorio de PowerCenter de producción. Para administrar un servicio de aplicación, un usuario debe tener privilegio del dominio para administrar servicios y permiso sobre el servicio de aplicación.

Se usan diferentes herramientas para configurar permisos sobre los siguientes objetos:

Se usan diferentes herramientas para configurar permisos sobre los siguientes objetos:

Tipo de objeto	Herramienta	Descripción
Aplicaciones y objetos de aplicación	Herramienta del administrador	Puede asignar permisos sobre aplicaciones y objetos de aplicación como asignaciones y flujos de trabajo.
Objetos de conexión	Herramienta del administrador Herramienta del analista Developer tool	Puede asignar permisos sobre conexiones definidas en la Herramienta del administrador, la Herramienta del analista o Developer tool. Estas herramientas comparten los permisos de conexión.

Tipo de objeto	Herramienta	Descripción
Objetos de dominio	Herramienta del administrador	Puede asignar permisos sobre los siguientes objetos de dominio: dominio, carpetas, nodos, mallas, licencias, servicios de aplicación y perfiles del sistema operativo.
Objetos de catálogo de Metadata Manager	Metadata Manager	Puede asignar permisos sobre carpetas y objetos de catálogo de Metadata Manager.
Proyectos del repositorio de modelos	Herramienta del analista Developer tool	Puede asignar permisos sobre proyectos definidos en la Herramienta del analista y en Developer tool. Estas herramientas comparten los permisos de proyecto.
Objetos del repositorio de PowerCenter	Cliente de PowerCenter	Puede asignar permisos sobre grupos de implementación, etiquetas, consultas, objetos de conexión y carpetas de PowerCenter.
Objetos del servicio de datos SQL	Herramienta del administrador	Puede asignar permisos sobre objetos de datos SQL, tales como servicios de datos SQL, esquemas virtuales, tablas virtuales y procedimientos virtuales almacenados.
Objetos de servicio web	Herramienta del administrador	Puede asignar permisos sobre servicios web u operaciones de servicio web.

Tipo de objeto	Herramienta	Descripción
Objetos de conexión	Herramienta del administrador Developer tool	Puede asignar permisos sobre conexiones definidas en la Herramienta del administrador o en Developer tool. Estas herramientas comparten los permisos de conexión.
Objetos de dominio	Herramienta del administrador	Puede asignar permisos en los siguientes objetos de dominio: dominio, carpetas, el nodo y los servicios de aplicación.
Proyectos del repositorio de modelos	Developer tool	Puede asignar permisos sobre proyectos definidos en Developer tool.

Puede utilizar la Herramienta del administrador para configurar permisos en un objeto de dominio. Puede asignar permisos para los objetos de dominio siguientes:

- dominio
- nodo
- servicios de aplicación

## Tipos de permisos

Los usuarios y grupos pueden tener los tipos de permisos de dominio siguientes:

### Permisos directos

Permisos asignados directamente a un usuario o grupo. Cuando los usuarios y grupos tienen permiso sobre un objeto, pueden realizar tareas administrativas con ese objeto si también disponen del privilegio adecuado. Los permisos directos pueden editarse.

### Permisos heredados

Permisos que los usuarios heredan. Cuando los usuarios tienen permiso sobre un dominio o carpeta, heredan el permiso para todos los objetos del dominio o la carpeta. Cuando los grupos tienen permisos sobre un objeto del dominio, todos los subgrupos y usuarios que pertenecen al grupo heredan el permiso sobre el objeto del dominio. Por ejemplo, un dominio tiene una carpeta llamada Nodes que contiene diversos nodos. Si asigna permisos a un grupo sobre la carpeta, todos los subgrupos y usuarios que pertenezcan al grupo heredarán el permiso sobre la carpeta y sobre todos los nodos en ella.

Permisos que los usuarios heredan. Si los usuarios tienen permiso en un dominio, heredan el permiso en todos los objetos de dominio. Cuando los grupos tienen permisos sobre un objeto del dominio, todos los subgrupos y usuarios que pertenecen al grupo heredan el permiso sobre el objeto del dominio.

Permisos que los usuarios heredan. Si los usuarios tienen permiso en un dominio, heredan el permiso en todos los objetos de dominio. Cuando los grupos tienen permisos sobre un objeto del dominio, todos los subgrupos y usuarios que pertenecen al grupo heredan el permiso sobre el objeto del dominio.

Los permisos heredados no se pueden revocar. Tampoco se pueden revocar los permisos de usuarios o grupos que tengan asignada la función de administrador. La función de administrador omite la comprobación de permisos. Los usuarios con función de administrador pueden acceder a todos los objetos.

Es posible denegar permisos heredados a algunos tipos de objetos. Al denegarse permisos, se configuran excepciones para los permisos que los usuarios y grupos puede que ya tengan.

### Permisos efectivos

Superconjunto de todos los permisos de un usuario o grupo. Incluye los permisos directos y heredados.

Cuando visualice los detalles de los permisos, puede ver el origen de los permisos efectivos. Los detalles de los permisos muestran los permisos directos asignados a un usuario o grupo, permisos directos asignados a grupos primarios y permisos heredados de objetos primarios. Además, los detalles de los permisos muestran si un usuario o grupo tiene asignada la función de administrador, la cual pasa por alto la comprobación de permisos.

## Filtros de búsqueda para el trabajo con permisos

Para asignar permisos, ver detalles de permisos o editar permisos para un usuario o grupo, puede utilizar filtros de búsqueda para buscar un grupo o usuario.

Durante la administración de permisos para usuarios o grupos, puede utilizar los siguientes filtros de búsqueda:

### Dominio de seguridad

Seleccione el dominio de seguridad en el que se buscarán los usuarios o grupos.

### Cadena patrón

Especifique una cadena para buscar usuarios o grupos. Administrator Tool devuelve todos los nombres que contengan dicha cadena de búsqueda. La cadena no distingue mayúsculas de minúsculas. Por ejemplo, la cadena "DA" puede devolver "iasdaemon", "daphne" y "DA\_AdminGroup".

También es posible ordenar la lista de usuarios o grupos. Haga clic con el botón derecho en un nombre de columna para ordenar la columna en orden ascendente o descendente.



# Permisos del objeto de dominio

Debe configurar privilegios y permisos para administrar la seguridad del usuario en el dominio. Los permisos definen el nivel de acceso de un usuario a un objeto de dominio. Para iniciar sesión en la Herramienta del administrador, el usuario debe tener permiso en un objeto de dominio como mínimo. Si el usuario tiene permiso en un objeto, pero no tiene el privilegio de dominio que permite modificar el tipo de objeto, solamente puede ver el objeto.

Por ejemplo, si un usuario tiene permiso en un nodo, pero no tiene el privilegio Administrar nodos y mallas, puede ver las propiedades del nodo, pero no puede configurar, cerrar ni quitar el nodo.

Puede configurar permisos en los siguientes tipos de objetos de dominio:

Tipo de objeto de dominio	Descripción del permiso
Dominio	Permite a los usuarios de la Herramienta del administrador acceder a todos los objetos de dominio. Si los usuarios tienen permiso en un dominio, heredan el permiso en todos los objetos del dominio.
Carpeta	Permite a los usuarios de la Herramienta del administrador acceder a todos los objetos de la carpeta en la Herramienta del administrador. Si los usuarios tienen permiso en una carpeta, heredan el permiso en todos los objetos de la carpeta.
Nodo	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades del nodo. Sin permiso, un usuario no puede usar el nodo para definir un servicio de aplicación o crear una malla.
Malla	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades de la malla. Sin permiso, un usuario no puede asignar la malla a un servicio de integración de datos o a un servicio de integración de PowerCenter.
Licencia	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades de la licencia. Sin permiso, un usuario no puede usar la licencia para crear un servicio de aplicación.
Servicio de aplicación	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades del servicio de aplicación.
Perfil de sistema operativo	Permite a los desarrolladores, analistas y operadores de Informática asociados con el perfil de sistema operativo, ejecutar asignaciones, perfiles y flujos de trabajo. Permite a los usuarios de PowerCenter ejecutar flujos de trabajo asociados al perfil de sistema operativo. Si el usuario que ejecuta un flujo de trabajo no tiene permiso en el perfil de sistema operativo asignado al flujo de trabajo, el flujo de trabajo genera un error.

Tipo de objeto de dominio	Descripción del permiso
Dominio	Permite a los usuarios de la Herramienta del administrador acceder a todos los objetos de dominio. Si los usuarios tienen permiso en un dominio, heredan el permiso en todos los objetos del dominio.
Nodo	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades del nodo.

Tipo de objeto de dominio	Descripción del permiso
Servicio de aplicación	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades del servicio de aplicación.
Licencia	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades de la licencia.

Tipo de objeto de dominio	Descripción del permiso
Dominio	Permite a los usuarios de la Herramienta del administrador acceder a todos los objetos de dominio. Si los usuarios tienen permiso en un dominio, heredan el permiso en todos los objetos del dominio.
Nodo	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades del nodo.
Servicio de aplicación	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades del servicio de aplicación.
Licencia	Permite a los usuarios de la Herramienta del administrador ver y editar las propiedades de la licencia.

Puede usar los siguientes métodos para administrar los permisos del objeto de dominio:

- Administración de permisos por objeto de dominio. Use la vista de permisos de un objeto de dominio para asignar y editar permisos en el objeto para varios usuarios o grupos.
- Administración de permisos por usuario o grupo. Use el cuadro de diálogo Administrar permisos para asignar y editar permisos en los objetos de dominio para un usuario o grupo específicos.

**Nota:** La configuración de permisos en un perfil de sistema operativo debe ser distinta de la configuración de permisos en otros objetos de dominio.

## Permisos por objeto de dominio

Use la vista **Permisos** de un objeto de dominio para asignar, ver y editar permisos en el objeto de dominio para varios usuarios o grupos.

### Cómo asignar permisos sobre un objeto de dominio

Cuando asigna permisos sobre un objeto de dominio, está otorgando a usuarios y grupos acceso al objeto.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione el objeto de dominio.
3. En el panel de contenido, seleccione la vista **Permisos**.
4. Haga clic en la ficha **Grupos o Usuarios**.
5. Haga clic en **Acciones > Asignar permisos**.

El cuadro de diálogo **Asignar permisos** muestra todos los usuarios o grupos que no tienen permiso sobre el objeto.

6. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
7. Seleccione un usuario o un grupo y haga clic en **Siguiente**.
8. Seleccione **Permitir**, y haga clic en **Finalizar**.

## Visualización de detalles de permiso en un objeto de dominio

Cuando visualice los detalles de un permiso, puede ver el origen de los permisos efectivos.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione el objeto de dominio.
3. En el panel de contenido, seleccione la vista **Permisos**.
4. Haga clic en la ficha **Grupos o Usuarios**.
5. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
6. Seleccione un usuario o grupo y haga clic en **Acciones > Ver detalles del permiso**.

Se abre el cuadro de diálogo **Detalles del permiso**. El cuadro de diálogo muestra los permisos directos asignados al usuario o grupo, los permisos directos asignados a los grupos primarios y los permisos heredados de los objetos primarios. Los detalles del permiso muestran además si el usuario o grupo tiene asignada la función de administrador que omite la comprobación del permiso.

7. Haga clic en **Cerrar**
8. o haga clic en **Editar permisos** para editar los permisos directos.

## Edición de permisos en un objeto de dominio

Puede editar los permisos directos para un usuario o grupo en un objeto de dominio. No puede revocar permisos heredados ni sus propios permisos.

**Nota:** Si revoca un permiso directo en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione el objeto de dominio.
3. En el panel de contenido, seleccione la vista **Permisos**.
4. Haga clic en la ficha **Grupos o Usuarios**.
5. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
6. Seleccione un usuario o grupo y haga clic en **Acciones > Editar permisos directos**.

Aparecerá el cuadro de diálogo **Editar permisos directos**.

7. Para asignar permisos en el objeto, seleccione **Permitir**.
8. Para revocar permisos en el objeto, seleccione **Revocar**.

Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**.

9. Haga clic en **Aceptar**.

## Permisos por usuario o grupo

Use el cuadro de diálogo **Administrar permisos** para ver, asignar y editar los permisos del objeto de dominio para un usuario o grupo específico.

## Visualización de detalles de permiso para un usuario o grupo

Cuando visualice los detalles de un permiso, puede ver el origen de los permisos efectivos.

1. En el encabezado de Infomatica Administrator, haga clic en **Administrar > Permisos**.  
Se abre el cuadro de diálogo **Administrar permisos**.
2. Haga clic en la ficha **Grupos o Usuarios**.
3. Indique una cadena para buscar usuarios y grupos y haga clic en el botón **Filtro**.
4. Seleccione un usuario o grupo.
5. Seleccione un objeto de dominio y haga clic en el botón **Ver detalles del permiso**.  
Se abre el cuadro de diálogo **Detalles del permiso**. El cuadro de diálogo muestra los permisos directos asignados al usuario o grupo, los permisos directos asignados a los grupos primarios y los permisos heredados de los objetos primarios. Los detalles del permiso muestran además si el usuario o grupo tiene asignada la función de administrador que omite la comprobación del permiso.
6. Haga clic en **Cerrar**
7. o haga clic en **Editar permisos** para editar los permisos directos.

## Asignación y edición de permisos para un usuario o grupo

Cuando se editan los permisos de objeto de dominio para un usuario o grupo, se pueden asignar permisos y también editar los permisos directos existentes. No puede revocar permisos heredados ni sus propios permisos.

**Nota:** Si revoca un permiso directo en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

1. En el encabezado de Infomatica Administrator, haga clic en **Administrar > Permisos**.  
Aparecerá el cuadro de diálogo **Administrar permisos**.
2. Haga clic en la ficha **Grupos o Usuarios**.
3. Escriba una cadena para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
4. Seleccione un usuario o grupo.
5. Seleccione un objeto de dominio y haga clic en el botón **Editar permisos directos**.  
Aparecerá el cuadro de diálogo **Editar permisos directos**.
6. Para asignar permisos en el objeto, seleccione **Permitir**.
7. Para revocar permisos en el objeto, seleccione **Revocar**.  
Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**.
8. Haga clic en **Aceptar**.
9. Haga clic en **Cerrar**.

## Permisos de perfil de sistema operativo

Asigne, vea y edite permisos en los perfiles de sistema operativo en la página Seguridad de la Herramienta del administrador.

El grupo Administrador tiene permisos en todos los perfiles de sistema operativo.

## Asignación de permisos en un perfil de sistema operativo

Al asignar permisos en un perfil de sistema operativo, los usuarios de Informática ejecutan asignaciones, perfiles y flujos de trabajo con dicho perfil. Los usuarios de PowerCenter ejecutan los flujos de trabajo asignados al perfil de sistema operativo.

1. En la ficha **Seguridad**, seleccione la vista **Perfiles de sistema operativo**.
2. Seleccione el perfil de sistema operativo y haga clic en la ficha **Permisos**.
3. Seleccione la vista **Grupos** o **Usuarios** y haga clic en **Conceder permisos**.  
El cuadro de diálogo **Asignar usuarios o grupos al perfil de sistema operativo** muestra todos los usuarios o grupos que no tienen permiso sobre el perfil de sistema operativo.
4. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
5. Seleccione un usuario o un grupo y haga clic en **Siguiente**.
6. Seleccione **Permitir**, y haga clic en **Finalizar**.

## Visualización de detalles de permisos en un perfil de sistema operativo

Cuando visualice los detalles de un permiso, puede ver el origen de los permisos efectivos.

1. En la ficha **Seguridad**, seleccione la vista **Perfiles de sistema operativo**.
2. Seleccione el perfil de sistema operativo y haga clic en la ficha **Permisos**.
3. Seleccione la vista **Grupos** o **Usuarios**.
4. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
5. Seleccione un usuario o grupo y haga clic en **Ver detalles del permiso**.  
Se abre el cuadro de diálogo **Detalles del permiso**. El cuadro de diálogo muestra los permisos directos asignados al usuario o grupo, los permisos directos asignados a los grupos primarios y los permisos heredados de los objetos primarios. Los detalles del permiso muestran además si el usuario o grupo tiene asignada la función de administrador que omite la comprobación del permiso.
6. Haga clic en **Cerrar**
7. o haga clic en **Editar permisos** para editar los permisos directos.

## Edición de permisos en un perfil de sistema operativo

Puede editar los permisos directos para un usuario o grupo en un perfil de sistema operativo. No puede revocar permisos heredados ni sus propios permisos.

**Nota:** Si revoca un permiso directo en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

1. En la ficha **Seguridad**, seleccione la vista **Perfiles de sistema operativo**.
2. Seleccione el perfil de sistema operativo y haga clic en la ficha **Permisos**.
3. Seleccione la vista **Grupos** o **Usuarios**.
4. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
5. Seleccione un usuario o grupo y haga clic en **Editar permisos directos**.  
Aparecerá el cuadro de diálogo **Editar permisos directos**.
6. Para asignar permisos en el perfil de sistema operativo, seleccione **Permitir**.
7. Para revocar permisos en el perfil de sistema operativo, seleccione **Revocar**.  
Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**.

8. Haga clic en **Aceptar**.

## Permisos de conexión

Los permisos controlan el nivel de acceso que un usuario o grupo tiene en la conexión.

Los permisos de una conexión se pueden configurar en las herramientas Analyst, Developer o Administrator.

Los permisos de una conexión se pueden configurar en las herramientas Developer o Administrator.

Cualquier permiso de conexión que se asigne a un usuario o grupo en una herramienta también se aplica en las demás herramientas. Supongamos, por ejemplo, que concede a GroupA permiso en ConnectionA en la herramienta Developer. GroupA tendrá permiso en ConnectionA también en las herramientas Analyst y Administrator.

Cualquier permiso de conexión que se asigne a un usuario o grupo en una herramienta también se aplica en las demás herramientas. Supongamos, por ejemplo, que concede a GroupA permiso en ConnectionA en la herramienta Developer. GroupA también tendrá permiso en ConnectionA en la herramienta Administrator.

Los siguientes componentes de Informatica usan permisos de conexión:

- Herramienta Administrator. Aplica permisos de lectura, escritura y ejecución en las conexiones.
- Herramienta Analyst. Aplica permisos de lectura, escritura y ejecución en las conexiones.
- Interfaz de línea de comandos de Informatica. Aplica permisos de lectura, escritura y concesión en las conexiones.
- Herramienta Developer. Aplica permisos de lectura, escritura y ejecución en las conexiones.  
Para los servicios de datos SQL, la herramienta Developer no aplica permisos de conexión. En su lugar, aplica seguridad de nivel de columna y exclusión de seguridad para restringir el acceso a los datos.
- Servicio de integración de datos. Aplica permisos de ejecución cuando un usuario intenta obtener la vista previa de los datos o ejecutar una asignación, cuadro de mando o perfil.
- Servicio de integración de datos. Aplica permisos de ejecución cuando un usuario intenta obtener la vista previa de los datos o ejecutar una asignación o perfil.

**Nota:** No puede asignar permisos en las conexiones del almacén de perfiles, de la base de datos de la memoria caché del objeto de datos o del repositorio de modelos.

## Tipos de permisos de conexión

Puede asignar diferentes tipos de permiso a los usuarios para que realicen las siguientes acciones:

Acción	Tipos de permiso
Ver todos los metadatos de las conexiones, excepto las contraseñas, como el nombre de la conexión, el tipo, la descripción, las cadenas de conexión y los nombres de usuario.	Lectura
Modifique todos los metadatos de conexión, incluidas las contraseñas. Elimine la conexión. Los usuarios con permiso de escritura heredan el permiso de lectura.	Escritura

Acción	Tipos de permiso
Acceder a los datos físicos en el origen de datos subyacente definido por la conexión. Los usuarios pueden previsualizar datos, ejecutar una asignación, ejecutar una asignación en una tarea de asignación de flujo de trabajo, ejecutar un cuadro de mando o ejecutar un perfil que utiliza la conexión. Acceder a los datos físicos en el origen de datos subyacente definido por la conexión. Los usuarios pueden previsualizar datos, ejecutar una asignación, ejecutar una asignación en una tarea de asignación de flujo de trabajo o ejecutar un perfil que utiliza la conexión.	Ejecución
Conceder y revocar permisos para las conexiones.	Concesión

## Permisos de conexión predeterminados

El administrador del dominio tiene todos los permisos para todas las conexiones. El usuario que crea una conexión tiene permiso para leer, escribir, ejecutar y otorgar permisos sobre esa conexión. De manera predeterminada, todos los usuarios tienen permiso para realizar las siguientes acciones o conexiones:

- Ver metadatos de conexión básicos, tales como nombre, tipo y descripción de la conexión.
- Usar la conexión en asignaciones en la herramienta Developer.
- Crear perfiles en la herramienta Analyst para objetos de la conexión.

## Cómo asignar permisos sobre una conexión

Cuando asigna permisos sobre una conexión, define el nivel de acceso que un usuario o grupo tiene sobre la conexión.

1. En la ficha Administrar, seleccione la vista **Conexiones**.
2. En el navegador, seleccione la conexión.
3. En el panel de contenido, seleccione la vista **Permisos**.
4. Haga clic en la ficha **Grupos** o **Usuarios**.
5. Haga clic en **Acciones** > **Asignar permisos**.

El cuadro de diálogo **Asignar permisos** muestra todos los usuarios o grupos que no tienen permiso sobre la conexión.

6. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
7. Seleccione un usuario o un grupo y haga clic en **Siguiente**.
8. Seleccione **Permitir** para cada tipo de permiso que desee asignar.
9. Haga clic en **Finalizar**.

## Visualización de detalles de permiso en una conexión

Cuando visualice los detalles de un permiso, puede ver el origen de los permisos efectivos.

1. En la ficha Administrar, seleccione la vista **Conexiones**.
2. En el navegador, seleccione la conexión.
3. En el panel de contenido, seleccione la vista **Permisos**.
4. Haga clic en la ficha **Grupos** o **Usuarios**.

5. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
6. Seleccione un usuario o grupo y haga clic en **Acciones > Ver detalles del permiso**.  
Se abre el cuadro de diálogo **Ver detalles del permiso**. El cuadro de diálogo muestra los permisos directos asignados al usuario o grupo y los permisos directos asignados a los grupos primarios. Los detalles del permiso muestran además si el usuario o grupo tiene asignada la función de administrador que omite la comprobación del permiso.
7. Haga clic en **Cerrar**
8. o haga clic en **Editar permisos** para editar los permisos directos.

## Edición de permisos en una conexión

Puede editar los permisos directos para un usuario o grupo en una conexión. No puede revocar permisos heredados ni sus propios permisos.

**Nota:** Si revoca un permiso directo en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

1. En la ficha Administrar, seleccione la vista **Conexiones**.
2. En el navegador, seleccione la conexión.
3. En el panel de contenido, seleccione la vista **Permisos**.
4. Haga clic en la ficha **Grupos o Usuarios**.
5. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
6. Seleccione un usuario o grupo y haga clic en **Acciones > Editar permisos directos**.  
Aparecerá el cuadro de diálogo **Editar permisos directos**.
7. Elija si desea permitir o revocar permisos.
  - Seleccione **Permitir** para asignar un permiso.
  - Desactive la opción **Permitir** para revocar un solo permiso.
  - Seleccione **Revocar** para revocar todos los permisos.

Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**.

8. Haga clic en **Aceptar**.

## Permisos de aplicación y de objeto de aplicación

Los permisos controlan el nivel de acceso que un usuario o grupo tienen en relación con las aplicaciones y los objetos de aplicación como, por ejemplo, asignaciones y flujos de trabajo.

Puede configurar los permisos de aplicación y de objeto de aplicación en la Herramienta del administrador o desde la línea de comandos.

## Tipos de permisos de aplicación y de objeto de aplicación

Puede asignar la visualización, concesión y ejecución de permisos a usuarios y grupos.

Puede asignar los siguientes permisos a usuarios y grupos:



### Ver permiso

Vea las aplicaciones y los objetos de aplicación.

### Conceder permiso

Conceda y revoque permisos en las aplicaciones y los objetos de aplicación.

### Ejecutar permiso

Ejecuta las aplicaciones y los objetos de aplicación.

**Nota:** Para realizar operaciones de aplicación como iniciar, detener o realizar una copia de seguridad en la Herramienta del administrador o desde la línea de comandos, el usuario debe tener permiso de ejecución y el privilegio Administrar aplicaciones en la aplicación.

## Asignar permisos en una aplicación u objeto de aplicación

Al asignar permisos en una aplicación u objeto de aplicación, debe definir el nivel de acceso que un usuario o grupo tiene con respecto a una aplicación u objeto de aplicación.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione una aplicación, una asignación o un flujo de trabajo.
5. En el panel de detalles, seleccione la vista **Permisos de grupo o Permisos de usuario**.
6. Haga clic en el botón **Asignar permiso**.

El cuadro de diálogo **Asignar permisos** muestra todos los usuarios o grupos que no tienen permiso sobre la aplicación ni sobre el objeto de aplicación.

7. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
8. Seleccione un usuario o un grupo y haga clic en **Siguiente**.
9. Seleccione **Permitir** para cada tipo de permiso que desee asignar.
10. Haga clic en **Finalizar**.

## Visualizar los detalles del permiso sobre una aplicación u objeto de aplicación

Cuando visualice los detalles de un permiso, puede ver el origen de los permisos efectivos.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione la aplicación, asignación o flujo de trabajo.
5. En el panel de detalles, seleccione la vista **Permisos de grupo o Permisos de usuario**.
6. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
7. Seleccione un usuario o grupo y haga clic en el botón **Ver detalles del permiso**.

Se abre el cuadro de diálogo **Detalles del permiso**. El cuadro de diálogo muestra los permisos directos asignados al usuario o grupo, los permisos directos asignados a los grupos primarios y los permisos heredados de los objetos primarios. Los detalles del permiso muestran además si el usuario o grupo tiene asignada la función de administrador que omite la comprobación del permiso.

8. Haga clic en **Cerrar**

- o haga clic en **Editar permisos** para editar los permisos directos.

## Editar permisos sobre una aplicación u objeto de aplicación

Puede editar los permisos directos sobre una aplicación u objeto de aplicación para un usuario o grupo. No puede revocar permisos heredados ni sus propios permisos.

**Nota:** Si revoca un permiso directo en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

- En la ficha Administrar, seleccione la vista **Servicios y nodos**.
- En el navegador, seleccione un servicio de integración de datos.
- En el panel de contenido, seleccione la vista **Aplicaciones**.
- Seleccione la aplicación u objeto de aplicación.
- En el panel de detalles, seleccione la vista **Permisos de grupo** o **Permisos de usuario**.
- Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
- Seleccione un usuario o grupo y haga clic en el botón **Editar permisos directos**.

Aparecerá el cuadro de diálogo **Editar permisos directos**.

- Elija si desea permitir o revocar permisos.
  - Seleccione **Permitir** para asignar un permiso.
  - Desactive la opción **Permitir** para revocar un solo permiso.
  - Seleccione **Revocar** para revocar todos los permisos.

Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**.

- Haga clic en **Aceptar**.

## Denegar permisos sobre una aplicación u objeto de aplicación

Puede denegar explícitamente permisos sobre aplicaciones y objetos de aplicación. Cuando deniega un permiso, está aplicando una excepción al permiso efectivo.

## Permisos del servicio de datos SQL

Los usuarios se pueden conectar a un servicio de datos SQL a través de una herramienta de cliente JDBC u ODBC. Tras conectarse, los usuarios pueden ejecutar consultas SQL sobre tablas virtuales en un servicio de datos SQL o ejecutar un procedimiento almacenado virtual en un servicio de datos SQL. Los permisos controlan el nivel de acceso que un usuario tiene a un servicio de datos SQL.

Puede asignar permisos a usuarios y grupos para los objetos de datos SQL siguientes:

- Servicio de datos SQL
- Tabla virtual
- Procedimiento almacenado virtual

Cuando asigne permisos en un objeto de servicio de datos SQL, el usuario o grupo heredará los mismos permisos para todos los objetos que pertenezcan al objeto de servicio de datos SQL. Por ejemplo, asigna a

un usuario permiso de selección para un servicio de datos SQL. Dicho usuario hereda el permiso de selección para todas las tablas virtuales del servicio de datos SQL.

Puede denegar permisos a usuarios y grupos para algunos objetos de datos SQL. Al denegar permisos, configura excepciones para los permisos que los usuarios y grupos puede que ya tengan. Por ejemplo, no puede asignar permisos a una columna en una tabla virtual, pero puede denegar a un usuario que ejecute una instrucción SQL SELECT que incluya dicha columna.

## Tipos de permiso del servicio de datos SQL

Puede asignar los siguientes permisos a usuarios y grupos:

- Permiso de concesión. Los usuarios pueden conceder y revocar permisos para los objetos del servicio de datos de SQL con Administrator Tool o empleando el programa de línea de comandos *infacmd*.
- Permiso de ejecución. Los usuarios pueden ejecutar en el servicio de datos de SQL los procedimientos virtuales almacenados mediante una herramienta cliente JDBC u ODBC.
- Permiso de selección. Los usuarios pueden ejecutar instrucciones SQL SELECT en tablas virtuales del servicio de datos de SQL mediante una herramienta cliente JDBC u ODBC.

Algunos permisos no son aplicables a todos los objetos del servicio de datos SQL.

La tabla siguiente describe los permisos para cada objeto del servicio de datos SQL:

Objeto	Permiso de concesión	Permiso de ejecución	Permiso de selección
Servicio de datos SQL	Conceder y revocar permisos para el servicio de datos de SQL y todos objetos del mismo.	Ejecutar todos los procedimientos almacenados virtuales del servicio de datos SQL.	Ejecutar instrucciones SQL SELECT en todas las tablas virtuales del servicio de datos de SQL.
Tabla virtual	Conceder y revocar permisos para la tabla virtual.	-	Ejecutar instrucciones SQL SELECT en la tabla virtual.
Proceso almacenado virtual	Conceder y revocar permisos para el procedimiento almacenado virtual.	Ejecutar el procedimiento almacenado virtual.	-

## Asignación de permisos en un servicio de datos SQL

Cuando se asignan permisos en un objeto de servicio de datos SQL, se define el nivel de acceso que tiene un usuario o grupo al objeto.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione el objeto de servicio de datos SQL.
5. En el panel de detalles, seleccione la vista **Permisos de grupo** o **Permisos de usuario**.
6. Haga clic en el botón **Asignar permiso**.

El cuadro de diálogo **Asignar permisos** muestra todos los usuarios o grupos que no tienen permisos en el objeto de servicio de datos SQL.

7. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
8. Seleccione un usuario o un grupo y haga clic en **Siguiente**.

9. Seleccione **Permitir** para cada tipo de permiso que desee asignar.
10. Haga clic en **Finalizar**.

## Visualización de detalles de permisos en un servicio de datos SQL

Cuando visualice los detalles de un permiso, puede ver el origen de los permisos efectivos.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione el objeto de servicio de datos SQL.
5. En el panel de detalles, seleccione la vista **Permisos de grupo** o **Permisos de usuario**.
6. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
7. Seleccione un usuario o grupo y haga clic en el botón **Ver detalles del permiso**.

Se abre el cuadro de diálogo **Detalles del permiso**. El cuadro de diálogo muestra los permisos directos asignados al usuario o grupo, los permisos directos asignados a los grupos primarios y los permisos heredados de los objetos primarios. Los detalles del permiso muestran además si el usuario o grupo tiene asignada la función de administrador que omite la comprobación del permiso.

8. Haga clic en **Cerrar**
9. o haga clic en **Editar permisos** para editar los permisos directos.

## Edición de permisos en un servicio de datos SQL

Puede editar los permisos directos para un usuario o grupo en un servicio de datos SQL. No puede revocar permisos heredados ni sus propios permisos.

**Nota:** Si revoca un permiso directo en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione el objeto de servicio de datos SQL.
5. En el panel de detalles, seleccione la vista **Permisos de grupo** o **Permisos de usuario**.
6. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
7. Seleccione un usuario o grupo y haga clic en el botón **Editar permisos directos**.

Aparecerá el cuadro de diálogo **Editar permisos directos**.

8. Elija si desea permitir o revocar permisos.
  - Seleccione **Permitir** para asignar un permiso.
  - Desactive la opción **Permitir** para revocar un solo permiso.
  - Seleccione **Revocar** para revocar todos los permisos.

Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**.

9. Haga clic en **Aceptar**.

## Denegación de permisos en un servicio de datos SQL

Puede denegar explícitamente los permisos en algunos objetos de servicio de datos SQL. Cuando se deniega un permiso en un objeto en un servicio de datos SQL, se está aplicando una excepción al permiso efectivo.

Para denegar permisos, se usa uno de los siguientes comandos de infacmd:

- `infacmd sql SetStoredProcedurePermissions`. Deniega los permisos de ejecución o concesión en el nivel de procedimiento almacenado.
- `infacmd sql SetTablePermissions`. Deniega los permisos de selección y concesión en el nivel de tabla virtual.
- `infacmd sql SetColumnPermissions`. Deniega el permiso de selección en el nivel de columna.

Cada comando tiene opciones para aplicar permisos (-ap) y denegar permisos (-dp). El comando `SetColumnPermissions` no incluye la opción de aplicar permisos.

**Nota:** No se pueden denegar permisos desde Administrator Tool.

El servicio de integración de datos comprueba los permisos antes de ejecutar procedimientos almacenados y consultas SQL en la base de datos virtual. El servicio de integración de datos valida los permisos para los usuarios o grupos a partir del nivel de servicio de datos SQL. Cuando los permisos se aplican a un objeto primario en un servicio de datos SQL, los objetos secundarios heredan el permiso. El servicio de integración de datos comprueba si hay permisos denegados en el nivel de columna.

## Seguridad de nivel de columna

Un administrador puede denegar el acceso a las columnas de una tabla virtual de un objeto de datos SQL. El administrador puede configurar el comportamiento del servicio de integración de datos para que las consultas se realicen en una columna restringida.

Cuando el usuario consulta una columna para la que no tiene permisos, puede ocurrir lo siguiente:

- La consulta devuelve un valor de sustitución en lugar de los datos. La consulta devuelve un valor de sustitución en cada fila que devuelve. El valor de sustitución reemplaza el valor de la columna a través de la consulta. Si la consulta incluye filtros o uniones, el valor de sustitución del resultado aparece en los resultados.
- La consulta falla por un error de permisos no suficientes.

Para obtener más información sobre la configuración de la seguridad para los servicios de datos SQL, consulte el artículo "How to Configure Security for SQL Data Services" en la biblioteca de procedimientos de Informática (Informatica How-To Library):

[https://kb.informatica.com/h2l/HowTo%20Library/1/0266\\_ConfiguringSecurityForSQLDataServices.pdf](https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf).

## Columnas restringidas

Cuando configure la seguridad a nivel de columna, debe establecer una opción de columna que determine qué ocurrirá si un usuario selecciona la columna restringida en una consulta. Los datos restringidos se pueden sustituir con un valor predeterminado. Otra posibilidad es hacer que la consulta falle si el usuario selecciona la columna restringida.

Por ejemplo, un administrador deniega al usuario acceso a la columna de salario de la tabla Empleado. El administrador configura un valor sustituto de 100.000 para la columna de salario. Cuando el usuario selecciona la columna de salario en una consulta SQL, el servicio de integración de datos devuelve 100.000 como salario en todas las filas.

Ejecute el comando `infacmd sql UpdateColumnOptions` para configurar las opciones de columna. No puede establecer opciones de columna desde Administrator Tool.

Cuando ejecute `infacmd sql UpdateColumnOptions`, especifique las siguientes opciones:

**ColumnOptions.DenyWith=opción**

Determina si se sustituye el valor de la columna restringida o si se hace fallar a la consulta. Si sustituye el valor de la columna, puede hacerlo por NULL o por un valor constante. Especifique una de las siguientes opciones:

- **ERROR.** Hace fallar a la consulta y devuelve un error cuando una consulta SQL selecciona una columna restringida.
- **NULL.** Devuelve valores nulos para una columna restringida en cada fila.
- **VALUE.** Devuelve un valor constante en lugar de una columna restringida en cada fila. Configure el valor constante en la opción `ColumnOptions.InsufficientPermissionValue`.

**ColumnOptions.InsufficientPermissionValue=valor**

Sustituye el valor de la columna restringida con una constante. El valor predeterminado es una cadena vacía. Si el servicio de integración de datos sustituye la columna con una cadena vacía, pero la columna incluye números o fechas, la consulta devolverá errores. Si no configura un valor para la opción `DenyWith`, el servicio de integración de datos ignora la opción `InsufficientPermissionValue`.

Para configurar un valor de sustitución para una columna, especifique un comando con la siguiente sintaxis:

```
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
```

Si no configura ninguna opción para una columna restringida, la opción predeterminada no hará fallar la consulta. En tal caso, se ejecutará la consulta y el servicio de integración de datos sustituirá la columna con NULL.

## Cómo añadir seguridad a nivel de columna

Configure la seguridad a nivel de columna con el comando `infacmd sql SetColumnPermissions`. No puede establecer la seguridad a nivel de columna desde Administrator Tool.

Una tabla de empleados contiene las columnas `FirstName`, `LastName`, `Dept` y `Salary`. Puede habilitar a un usuario para que acceda a la tabla de empleados, pero impedir que tenga acceso a la columna `Salary`.

Para restringir el acceso del usuario a la columna `Salary`, deshabilite el servicio de integración de datos e introduzca un `infacmd` similar al comando siguiente:

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd
Adminpass -sqlds employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

Las siguientes instrucciones SQL devuelven NULL en la columna `Salary`:

```
Select * from Employee
Select LastName, Salary from Employee
```

La conducta predeterminada es devolver valores NULL.

# Permisos del servicio web

Los usuarios finales pueden enviar solicitudes de servicio web y recibir respuestas del servicio web mediante un cliente de servicio web. Los permisos controlan el nivel de acceso que tiene un usuario en un determinado servicio web.

Puede asignar permisos a usuarios y grupos en los siguientes objetos del servicio web:

- Servicio web
- Recurso de servicio web REST
- Operación del servicio web SOAP

Cuando asigna permisos a un objeto del servicio web, el usuario o el grupo hereda los mismos permisos en todos los objetos que pertenecen al objeto del servicio web en cuestión. Supongamos, por ejemplo, que asigna un permiso de ejecución a un usuario del servicio web. Este usuario hereda el permiso de ejecución para las operaciones del servicio web.

Puede denegar permisos para una operación del servicio web. Cuando deniega permisos, se configuran excepciones sobre los permisos que los usuarios y los grupos ya tenían. Un usuario, por ejemplo, tiene permisos de ejecución para un servicio web que tiene tres operaciones. Puede denegarle el permiso para ejecutar una de las operaciones del servicio web.

## Tipos de permiso para los servicios web

Un administrador asigna los permisos de servicio web a los siguientes tipos de usuarios y grupos:

- Consumidor de servicio web. Un usuario del dominio nativo que envía una solicitud al servicio web y recibe una respuesta del servicio web. El usuario debe tener el permiso de ejecución en el servicio web.
- Administrador de servicio web. Un usuario que puede iniciar sesión en la Herramienta del administrador, editar las propiedades del servicio web y conceder permisos a otros usuarios.
- Operador del servicio web. Un usuario que puede iniciar sesión en la Herramienta del administrador, supervisar un servicio web e iniciar o detener un servicio web.

Un administrador puede asignar los siguientes permisos a los usuarios y grupos:

- Conceder permisos. Los usuarios pueden administrar los permisos de los objetos del servicio web mediante Administrator Tool o con el programa de línea de comandos *infacmd*.
- Ejecutar permisos. Los usuarios pueden enviar solicitudes de servicio web y recibir respuestas del servicio web.

La tabla siguiente describe los permisos de cada objeto del servicio web SOAP:

Objeto	Permiso de concesión	Permiso de ejecución
Servicio web SOAP	Conceder y revocar permisos en el servicio web y todas las operaciones de servicio web dentro de este.	Enviar solicitudes de servicio web y recibir respuestas de este desde todas las operaciones de servicio web dentro del mismo.
Operación del servicio web SOAP	Conceder, revocar y denegar permisos en la operación de servicio web.	Enviar solicitudes de servicio web y recibir respuestas de este desde la operación de servicio web.

La tabla siguiente describe los permisos de cada objeto del servicio web REST:

Objeto	Permiso de concesión	Permiso de ejecución
Servicio web REST	Conceder y revocar permisos en el servicio web REST y todos los recursos de servicio web dentro de este.	Enviar solicitudes de servicio web y recibir respuestas de este desde todos los recursos de servicio web dentro del servicio web REST.
Recurso de REST	Conceder, revocar y denegar permisos en el recurso de servicio web REST.	Enviar solicitudes de servicio web y recibir respuestas de este desde el recurso de servicio web REST.

## Asignación de permisos en un servicio web

Cuando se asignan permisos en un objeto de servicio web, se define el nivel de acceso que tiene un usuario o grupo al objeto.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione el objeto de servicio web.
5. En el panel de detalles, seleccione la vista **Permisos de grupo** o **Permisos de usuario**.
6. Haga clic en el botón **Asignar permiso**.  
El cuadro de diálogo **Asignar permisos** muestra todos los usuarios o grupos que no tienen permisos en el objeto de servicio de datos SQL.
7. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
8. Seleccione un usuario o un grupo y haga clic en **Siguiente**.
9. Seleccione **Permitir** para cada tipo de permiso que desee asignar.
10. Haga clic en **Finalizar**.

## Visualización de detalles de permiso en un servicio web

Cuando visualice los detalles de un permiso, puede ver el origen de los permisos efectivos.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione el objeto de servicio web.
5. En el panel de detalles, seleccione la vista **Permisos de grupo** o **Permisos de usuario**.
6. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
7. Seleccione un usuario o grupo y haga clic en el botón **Ver detalles del permiso**.

Se abre el cuadro de diálogo **Detalles del permiso**. El cuadro de diálogo muestra los permisos directos asignados al usuario o grupo, los permisos directos asignados a los grupos primarios y los permisos heredados de los objetos primarios. Los detalles del permiso muestran además si el usuario o grupo tiene asignada la función de administrador que omite la comprobación del permiso.

8. Haga clic en **Cerrar**
9. o haga clic en **Editar permisos** para editar los permisos directos.



## Edición de permisos en un servicio web

Puede editar los permisos directos para un usuario o grupo en un servicio web. Cuando edite los permisos en un objeto de servicio web, podrá denegar permisos en el objeto. No puede revocar permisos heredados ni sus propios permisos.

**Nota:** Si revoca un permiso directo en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

1. En la ficha Administrar, seleccione la vista **Servicios y nodos**.
2. En el navegador, seleccione un servicio de integración de datos.
3. En el panel de contenido, seleccione la vista **Aplicaciones**.
4. Seleccione el objeto de servicio web.
5. En el panel de detalles, seleccione la vista **Permisos de grupo** o **Permisos de usuario**.
6. Introduzca las condiciones de filtro para buscar usuarios y grupos y haga clic en el botón **Filtrar**.
7. Seleccione un usuario o grupo y haga clic en el botón **Editar permisos directos**.

Aparecerá el cuadro de diálogo **Editar permisos directos**.

8. Elija si desea permitir o revocar permisos.
  - Seleccione **Permitir** para asignar un permiso.
  - Seleccione **Denegar** para denegar un permiso en un objeto de servicio web.
  - Desactive la opción **Permitir** para revocar un solo permiso.
  - Seleccione **Revocar** para revocar todos los permisos.

Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**.

9. Haga clic en **Aceptar**.

## CAPÍTULO 11

# Informes de auditoría

Este capítulo incluye los siguientes temas:

- [Resumen de informes de auditoría, 210](#)
- [Información personal del usuario, 211](#)
- [Asociación de grupos de usuarios, 211](#)
- [Privilegios, 213](#)
- [Asociación de funciones, 213](#)
- [Permiso del objeto de dominio, 214](#)
- [Seleccionar usuarios para un informe de auditoría, 214](#)
- [Seleccionar grupos para un informe de auditoría, 215](#)
- [Seleccionar funciones para un informe de auditoría, 215](#)

## Resumen de informes de auditoría

Utilice los informes de auditoría para ver información sobre los usuarios y los grupos del dominio de Informática, así como los privilegios y los permisos asignados a ellos.

Puede generar los siguientes informes de auditoría:

### **Información personal del usuario**

Muestra información sobre las cuentas de usuario del dominio, incluido el estado del usuario. Puede seleccionar los usuarios o los grupos para los que desea generar el informe.

### **Asociación de grupos de usuarios**

Muestra información acerca de los usuarios y los grupos a los que pertenecen. Puede seleccionar los usuarios o los grupos para los que desea generar el informe.

### **Privilegios**

Muestra información sobre los privilegios asignados a los usuarios y los grupos del dominio. Puede seleccionar los usuarios o los grupos para los que desea generar el informe.

### **Funciones**

Muestra información sobre las funciones asignadas a los usuarios y los grupos del dominio. Puede seleccionar las funciones para las que desea generar el informe.

### **Permisos de objeto de dominio**

Muestra información sobre los objetos de dominio para los que los usuarios y grupos tienen permisos. Puede seleccionar los usuarios o los grupos para los que desea generar el informe.

Puede generar los informes de auditoría en formatos diferentes; entre ellos, archivos CSV, de texto o PDF. También puede ver el informe en la pantalla.

Puede generar los informes de auditoría desde la herramienta Administrator o desde la línea de comandos. Para ejecutar los informes de auditoría desde la línea de comandos, ejecute el programa de la línea de comandos `infacmd aud`.

## Información personal del usuario

El informe de información personal del usuario muestra la información de contacto y el estado de las cuentas de usuario del dominio.

Si ejecuta el informe para grupos, este organiza la lista de usuarios por grupo y muestra el nombre del grupo y el dominio de seguridad de cada grupo. El informe muestra los grupos anidados por separado.

El informe de información personal del usuario muestra la información siguiente:

**Nombre de inicio de sesión**

Nombre de inicio de sesión de la cuenta de usuario.

**Nombre completo**

Nombre completo de la cuenta de usuario.

**Dominio de seguridad**

Dominio de seguridad al que pertenece el usuario.

**Descripción**

Descripción de la cuenta de usuario.

**ID de correo electrónico**

Dirección de correo electrónico de la cuenta de usuario.

**Teléfono**

Número de teléfono de la cuenta de usuario.

**Cuenta bloqueada**

Indica si la cuenta está bloqueada o no. El informe muestra Sí si la cuenta está bloqueada y No, si no lo está.

**Cuenta deshabilitada**

Indica si la cuenta está deshabilitada o no. El informe muestra Sí si la cuenta está deshabilitada y No, si está habilitada.

## Asociación de grupos de usuarios

El informe de asociación de grupos de usuarios muestra información sobre los usuarios y sus grupos asociados.

Si ejecuta el informe para usuarios, el informe muestra la lista de usuarios y los grupos a los que pertenecen.

El informe de asociación de grupos de usuarios muestra la siguiente información:

**Nombre de inicio de sesión**

Nombre de inicio de sesión de la cuenta de usuario.

**Nombre completo**

Nombre completo de la cuenta de usuario.

**Dominio de seguridad**

Dominio de seguridad al que pertenece la cuenta de usuario.

**Nombre de grupo**

Nombre del grupo al que pertenece el usuario.

**Ruta de grupo**

Si el grupo es un grupo simple, la ruta de grupo muestra el nombre del grupo. Si el grupo es un grupo anidado, la ruta de grupo muestra la posición del grupo dentro de la jerarquía de los grupos anidados.

**Dominio de seguridad de grupo**

Dominio de seguridad del grupo al que pertenece el usuario.

Si ejecuta el informe para grupos, este organiza la lista de usuarios por grupo y muestra el nombre del grupo y el dominio de seguridad de cada grupo. El informe muestra los grupos anidados por separado. Para cada grupo, el informe muestra la lista de usuarios y grupos secundarios que pertenecen al grupo.

El informe de asociación de grupos de usuarios muestra la siguiente información de los usuarios que pertenecen al grupo:

**Nombre de inicio de sesión**

Nombre de inicio de sesión de la cuenta de usuario.

**Nombre completo**

Nombre completo de la cuenta de usuario.

**Dominio de seguridad**

Dominio de seguridad al que pertenece la cuenta de usuario.

El informe de asociación de grupos de usuarios muestra la siguiente información de los grupos secundarios que pertenecen al grupo:

**Nombre de grupo**

Nombre del grupo.

**Dominio de seguridad**

Dominio de seguridad al que pertenece el grupo.

**Ruta de grupo**

Si el grupo es un grupo simple, la ruta de grupo muestra el nombre del grupo. Si el grupo es un grupo anidado, la ruta de grupo muestra la posición del grupo dentro de la jerarquía de los grupos anidados.

# Privilegios

El informe de privilegios muestra los usuarios y los grupos, así como los privilegios asignados a los usuarios y los grupos.

Si ejecuta el informe para usuarios, este muestra la lista de usuarios y los privilegios asignados a cada usuario. Si ejecuta el informe para grupos, este muestra la lista de grupos y los privilegios asignados a cada grupo.

El informe de privilegios muestra la información siguiente:

**Nombre del privilegio**

Nombre del privilegio.

**Ruta del privilegio**

La jerarquía del grupo de privilegios que contiene el privilegio.

**Nombre de objeto**

Nombre del objeto en el que está permitido el privilegio.

**Tipo de objeto**

Tipo de objeto en el que está permitido el privilegio.

## Asociación de funciones

El informe de asociación de funciones muestra una lista de las funciones y los usuarios y grupos a los que se asignan las funciones.

El informe de asociación de funciones muestra la siguiente información:

**Nombre de inicio de sesión**

Nombre de inicio de sesión para la cuenta de usuario a la que la función está asignada. Se muestra para la lista de usuarios.

**Nombre completo**

Nombre completo de la cuenta de usuario a la que la función está asignada. Se muestra para la lista de usuarios.

**Nombre de grupo**

Nombre del grupo al que la función está asignada. Se muestra para la lista de grupos.

**Dominio de seguridad**

Dominio de seguridad al que pertenece el usuario o el grupo.

**Nombre de objeto**

Nombre del objeto en el que está permitido el conjunto de privilegios de la función.

**Tipo de objeto**

Tipo de objeto en el que está permitido el conjunto de privilegios de la función.

# Permiso del objeto de dominio

El informe Permiso del objeto de dominio muestra los usuarios y los grupos, así como los objetos para los que los usuarios y los grupos tienen permisos.

Si ejecuta el informe para los usuarios, el informe muestra la lista de usuarios y los objetos para los que los usuarios tienen permisos. Si ejecuta el informe para grupos, el informe muestra la lista de grupos y los objetos para los que los grupos tienen permisos.

El informe Permiso del objeto de dominio muestra la siguiente información:

## Nombre de objeto

Nombre del objeto para el que el usuario o grupo tiene permiso.

## Tipo de objeto

Tipo de objeto para el que el usuario o grupo tiene permiso.

## Ruta de acceso al objeto

Ubicación del objeto en el repositorio.

# Seleccionar usuarios para un informe de auditoría

Los informes de auditoría se pueden generar para varios usuarios.

1. En la herramienta Administrator, haga clic en **Seguridad > Informes de auditoría**.
2. En la lista **Seleccionar tipo de informe**, seleccione el tipo de informe de auditoría que desea ejecutar.
3. En la lista **Generar informe para**, seleccione **Usuarios** y haga clic en **Ir**.

Se abre el cuadro de diálogo **Seleccionar usuarios**. De forma predeterminada, el icono **Usuarios** está seleccionado y se muestra la lista de todos los usuarios disponibles. La lista muestra el nombre completo del usuario y el dominio de seguridad al que este pertenece.

4. En la lista **Usuarios disponibles**, seleccione los usuarios para los que desea ejecutar el informe.

Utilice las teclas Mayús o Ctrl para seleccionar varios usuarios.

5. Para seleccionar usuarios por grupo, haga clic en el icono **Grupos**.

La lista **Grupos disponibles** muestra todos los grupos del dominio y la lista **Miembros** muestra los usuarios que son miembros de los grupos. En la lista **Miembros**, seleccione los usuarios para los que desea ejecutar el informe. Puede seleccionar usuarios de varios grupos.

6. Haga clic en **Añadir**.

Para ejecutar el informe para todos los usuarios, haga clic en el icono **Usuarios** y, después, haga clic en **Añadir todo** sin seleccionar un usuario.

Para ejecutar el informe para todos los usuarios de un grupo, haga clic en el icono **Grupos**. Seleccione un grupo y haga clic en **Añadir todo** sin seleccionar un usuario de la lista **Miembros**.

Los usuarios seleccionados pasan a la lista **Usuarios seleccionados**.

7. En la lista **Formato de salida del informe**, seleccione el formato en el que desea ver el informe.

De forma predeterminada, el informe se muestra en la pantalla.

También puede ver un informe de auditoría en uno de los siguientes formatos:

- Texto. Genera el informe de auditoría como un archivo de texto con valores en columnas.
- CSV. Genera el informe de auditoría como un archivo de texto con valores separados por comas.
- PDF. Genera el informe de auditoría en formato .pdf. Debe instalar Acrobat Reader para ver el informe.

8. Haga clic en **Generar informe**.

## Seleccionar grupos para un informe de auditoría

Puede ejecutar informes de auditoría para varios grupos.

1. En la herramienta Administrator, haga clic en **Seguridad > Informes de auditoría**.
2. En la lista **Seleccionar tipo de informe**, seleccione el tipo de informe de auditoría que desea ejecutar.
3. En la lista **Generar informe para**, seleccione **Grupos** y haga clic en **Ir**.  
Aparece el cuadro de diálogo **Seleccionar grupos**. La lista de grupos se organiza según el dominio de seguridad.
4. En la lista **Grupos disponibles**, seleccione los grupos para los que desea ejecutar el informe.  
Utilice las teclas Mayús o Ctrl para seleccionar varios grupos.
5. Haga clic en **Añadir**.  
Para ejecutar el informe para todos los grupos, no seleccione ninguno y haga clic en **Añadir todo**.  
Los grupos seleccionados pasan a la lista **Grupos seleccionados**.
6. En la lista **Formato de salida del informe**, seleccione el formato en el que desea ver el informe.  
De forma predeterminada, los informes se muestran en la pantalla.  
También puede ejecutar un informe de auditoría en uno de los siguientes formatos:
  - Texto. Genera el informe de auditoría como un archivo de texto con valores en columnas.
  - CSV. Genera el informe de auditoría como un archivo de texto con valores separados por comas.
  - PDF. Genera el informe de auditoría en formato .pdf. Debe instalar Acrobat Reader para ver el informe.
7. Haga clic en **Generar informe**.

## Seleccionar funciones para un informe de auditoría

Cuando ejecute el informe de asociación de funciones, debe seleccionar las funciones para las que desea ejecutar el informe.

1. En la herramienta Administrator, haga clic en **Seguridad > Informes de auditoría**.
2. En la lista **Seleccionar tipo de informe**, seleccione el informe **Asociación de funciones**.
3. En la lista **Generar informe para**, seleccione **Funciones** y haga clic en **Ir**.

Aparecerá el cuadro de diálogo **Seleccionar funciones**. La lista de funciones definidas por el sistema se muestra por separado de la lista de funciones personalizadas.

4. En la lista **Funciones disponibles**, seleccione las funciones para las que desea ejecutar el informe. Utilice las teclas Mayús o Ctrl para seleccionar varias funciones.

5. Haga clic en **Añadir**.

Para ejecutar el informe para todas las funciones, no seleccione ninguna y haga clic en **Añadir todo**.

Las funciones seleccionadas pasan a la lista **Funciones seleccionadas**.

6. En la lista **Formato de salida del informe**, seleccione el formato en el que desea ver el informe.

De forma predeterminada, los informes se muestran en la pantalla.

También puede ejecutar un informe de auditoría en uno de los siguientes formatos:

- Texto. Genera el informe de auditoría como un archivo de texto con valores en columnas.
- CSV. Genera el informe de auditoría como un archivo de texto con valores separados por comas.
- PDF. Genera el informe de auditoría en formato .pdf. Debe instalar Acrobat Reader para ver el informe.

7. Haga clic en **Generar informe**.



## APÉNDICE A

# Permisos y privilegios de la línea de comandos

Este apéndice incluye los siguientes temas:

- [Comandos de infacmd as, 217](#)
- [Comandos infacmd dis, 218](#)
- [comandos infacmd es, 220](#)
- [Comandos infacmd ipc, 220](#)
- [Comandos infacmd isp, 220](#)
- [Comandos infacmd mrs, 232](#)
- [Comandos infacmd ms, 235](#)
- [Comandos infacmd oie, 235](#)
- [Comandos infacmd ps, 235](#)
- [Comandos infacmd pwx, 236](#)
- [Comandos infacmd rms, 237](#)
- [Comandos infacmd rtm, 238](#)
- [Comandos infacmd sch, 238](#)
- [Comandos infacmd sql, 239](#)
- [Comandos infacmd wfs, 240](#)
- [Comandos pmcmd, 240](#)
- [Comandos pmrep, 243](#)

## Comandos de infacmd as

Para ejecutar los comandos de *infacmd as*, los usuarios deben tener uno de los conjuntos de privilegios de dominio, privilegios de servicio del analista y permisos del objeto de dominio indicados.

En la tabla siguiente, se indican los privilegios y permisos necesarios para los comandos *infacmd as*:

Comando de <i>infacmd as</i>	Grupo de privilegios	Nombre de privilegio	Permiso de...
CreateAuditTables	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio del analista
CreateService	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio del analista
DeleteAuditTables	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio del analista
ListServiceOptions	-	-	Servicio del analista
ListServiceProcessOptions	-	-	Servicio del analista
UpdateServiceOptions	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio del analista
UpdateServiceProcessOptions	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio del analista

## Comandos *infacmd dis*

Para ejecutar los comandos de *infacmd dis*, los usuarios deben tener uno de los conjuntos de privilegios de dominio indicados, los privilegios del servicio de integración de datos y permisos de objeto de dominio.

En la tabla siguiente, se indican los privilegios y permisos necesarios para los comandos de *infacmd dis*:

Comando de <i>infacmd dis</i>	Grupo de privilegios	Nombre de privilegio	Permiso de...
BackupApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
CancelDataObjectCacheRefresh	-	-	-
CreateService	Administración de dominios	Gestionar servicios	Dominio o nodo donde se ejecuta el servicio de integración de datos
DeployApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
ListApplicationObjects	-	-	-
ListApplications	-	-	-

Comando de infacmd dis	Grupo de privilegios	Nombre de privilegio	Permiso de...
ListComputeOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos
ListDataObjectOptions	-	-	-
ListServiceOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos
ListServiceProcessOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos
PurgeDataObjectCache	-	-	-
RefreshDataObjectCache	-	-	-
RenameApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
RestoreApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
StartApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
StopApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
stopBlazeService	Administración de la aplicación	Administrar aplicaciones	Aplicación
UndeployApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
UpdateApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
UpdateApplicationOptions	Administración de la aplicación	Administrar aplicaciones	Aplicación
UpdateDataObjectOptions	Administración de la aplicación	Administrar aplicaciones	-
UpdateComputeOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos
UpdateServiceOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos
UpdateServiceProcessOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos

## comandos infacmd es

Los usuarios deben tener asignada la función de administrador del dominio para poder ejecutar los siguientes comandos infacmd es:

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

## Comandos infacmd ipc

Para ejecutar comandos *infacmd ipc*, los usuarios deben poseer uno de los permisos de objeto del repositorio de modelos que se enumeran.

La siguiente tabla enumera los privilegios y los permisos necesarios para los comandos *infacmd ipc*:

Comando infacmd ipc	Grupo de privilegios	Nombre de privilegio	Permiso de...
ExportToPC	-	-	Lectura en la carpeta que crea las tablas de referencia que se exportarán
genReuseReportFromPC	Herramientas	Acceder a Repository Manager	-

## Comandos infacmd isp

Para ejecutar los comandos *infacmd isp*, los usuarios deben tener uno de los conjuntos de privilegios de dominio, privilegios de servicio, permisos del objeto de dominio o permisos de conexión listados.

A los usuarios se les debe haber asignado la función de administrador para el dominio para que ejecuten los siguientes comandos:

- AddDomainLink
- AssignGroupPermission (en dominio)
- AssignGroupPermission (en perfiles del sistema operativo)
- AddServiceLevel
- AssignUserPermission (en dominio)
- AssignUserPermission (en perfiles del sistema operativo)
- CreateConnection
- CreateOSProfile
- PurgeLog
- RemoveDomainLink

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

A los usuarios se les debe haber asignado la función de administrador del dominio para que ejecuten el comando UpdateGatewayInfo.

En la siguiente tabla, se enumeran los privilegios y permisos requeridos para los comandos *infacmd isp*

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
GetNodeName	-	-	Nodo
UpdateGatewayInfo	-	-	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
AddAlertUser (para su cuenta de usuario)	-	-	-
AddAlertUser (para otros usuarios)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
AddConnectionPermissions	-	-	Conceder al conectar
AddDomainLink	-	-	-
AddDomainNode	Administración de dominios	Administrar nodos y mallas	Dominio y nodo
AssignGroupPermission (en servicios de aplicación u objetos de licencia)	Administración de dominios	Gestionar servicios	Servicio de aplicación u objeto de licencia
AssignGroupPermission (en dominio)	-	-	-
AssignGroupPermission (en carpetas)	Administración de dominios	Administrar carpetas del dominio	Carpeta
AssignGroupPermission (en nodos y mallas)	Administración de dominios	Administrar nodos y mallas	Nodo o malla
AssignGroupPermission (en perfiles del sistema operativo)	-	-	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
AddGroupPrivilege	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
AddLicense	Administración de dominios	Gestionar servicios	Dominio o carpeta primaria
AddNodeResource	Administración de dominios	Administrar nodos y mallas	Nodo
AddRolePrivilege	Administración de seguridad	Gestionar usuarios, grupos y roles	-
AddServiceLevel	-	-	-
AssignUserPermission (en servicios de aplicación u objetos de licencia)	Administración de dominios	Gestionar servicios	Servicio de aplicación u objeto de licencia
AssignUserPermission (en dominio)	-	-	-
AssignUserPermission (en carpetas)	Administración de dominios	Administrar carpetas del dominio	Carpeta
AssignUserPermission (en nodos o mallas)	Administración de dominios	Administrar nodos y mallas	Nodo o malla
AssignUserPermission (en perfiles del sistema operativo)	-	-	-
AssignUserPrivilege	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
AssignUserToGroup	Administración de seguridad	Gestionar usuarios, grupos y roles	-
AssignedToLicense	Administración de dominios	Gestionar servicios	Objeto de licencia y servicio de aplicación
AssignISTOMMSservice	Administración de dominios	Gestionar servicios	Servicio de Metadata Manager

<b>Comando infacmd isp</b>	<b>Grupo de privilegios</b>	<b>Nombre del privilegio</b>	<b>Permiso en</b>
AssignLicense	Administración de dominios	Gestionar servicios	Objeto de licencia y servicio de aplicación
AssignRoleToGroup	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
AssignRoleToUser	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
AssignRSToWSHubService	Administración de dominios	Gestionar servicios	Servicio de repositorio de PowerCenter y concentrador de servicios web
ConvertLogFile	-	-	Servicio de aplicación o dominio
CreateFolder	Administración de dominios	Administrar carpetas del dominio	Dominio o carpeta primaria
CreateConnection	-	-	-
CreateGrid	Administración de dominios	Administrar nodos y mallas	Dominio o carpeta primaria y nodos asignados a la malla
CreateGroup	Administración de seguridad	Gestionar usuarios, grupos y roles	-
CreateIntegrationService	Administración de dominios	Gestionar servicios	Dominio o carpeta, nodo o malla primario donde se ejecuta el servicio de integración de PowerCenter, objeto de licencia y servicio de repositorio de PowerCenter asociado

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
CreateMMService	Administración de dominios	Gestionar servicios	Dominio, carpeta o nodo primario donde se ejecuta el servicio de Metadata Manager, objeto de licencia, servicio de integración de PowerCenter y servicio de repositorio de PowerCenter asociados
CreateOSProfile	-	-	-
CreateRepositoryService	Administración de dominios	Gestionar servicios	Dominio, carpeta o nodo donde se ejecuta el servicio de repositorio de PowerCenter y objeto de licencia
CreateRole	Administración de seguridad	Gestionar usuarios, grupos y roles	-
CreateSAPBWService	Administración de dominios	Gestionar servicios	Dominio, malla, carpeta o nodo primario donde se ejecuta el servicio SAP BW, objeto de licencia y servicio de integración de PowerCenter asociado
CreateUser	Administración de seguridad	Gestionar usuarios, grupos y roles	-
CreateWSHubService	Administración de dominios	Gestionar servicios	Dominio, malla, carpeta o nodo donde se ejecuta el Concentrador de servicios web, objeto de licencia y servicio de repositorio de PowerCenter asociado
DisableNodeResource	Administración de dominios	Administrar nodos y mallas	Nodo



Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
DisableService (para el servicio de Metadata Manager)	Administración de dominios	Administrar ejecución de servicio	Servicio de Metadata Manager, servicio de integración de PowerCenter asociado y servicio de repositorio de PowerCenter
DisableService (para el resto de servicios de aplicación)	Administración de dominios	Administrar ejecución de servicio	Servicio de aplicación
DisableServiceProcess	Administración de dominios	Administrar ejecución de servicio	Servicio de aplicación
DisableUser	Administración de seguridad	Gestionar usuarios, grupos y roles	-
EditUser	Administración de seguridad	Gestionar usuarios, grupos y roles	-
EnableNodeResource	Administración de dominios	Administrar nodos y mallas	Nodo
EnableService (para el servicio de Metadata Manager)	Administración de dominios	Administrar ejecución de servicio	Servicio de Metadata Manager, servicio de integración de PowerCenter asociado y servicio de repositorio de PowerCenter
EnableService (para el resto de servicios de aplicación)	Administración de dominios	Administrar ejecución de servicio	Servicio de aplicación
EnableServiceProcess	Administración de dominios	Administrar ejecución de servicio	Servicio de aplicación
EnableUser	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ExportDomainObjects (para usuarios, grupos y funciones)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ExportDomainObjects (para conexiones)	Administración de dominios	Administrar conexiones	Leer al conectar

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
ExportUsersAndGroups	Administración de seguridad	Gestionar usuarios, grupos y roles	-
generateHadoopConnectionFromHiveConection	-	-	-
GetFolderInfo	-	-	Carpeta
GetLastError	-	-	Servicio de aplicación
GetLog	-	-	Servicio de aplicación o dominio
GetNodeName	-	-	Nodo
GetServiceOption	-	-	Servicio de aplicación
GetServiceProcessOption	-	-	Servicio de aplicación
GetServiceProcessStatus	-	-	Servicio de aplicación
GetServiceStatus	-	-	Servicio de aplicación
GetSessionLog	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta de repositorio
GetWorkflowLog	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta de repositorio
Ayuda	-	-	-
ImportDomainObjects (para usuarios, grupos y funciones)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ImportDomainObjects (para conexiones)	Administración de dominios	Administrar conexiones	Escribir al conectar
ImportUsersAndGroups	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ListAlertUsers	-	-	Dominio
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
ListConnectionOptions	-	-	Leer al conectar
ListConnections	-	-	-
ListConnectionPermissions	-	-	-
ListConnectionPermissions por grupo	-	-	-
ListConnectionPermissions por usuario	-	-	-
ListDomainLinks	-	-	Dominio
ListDomainOptions	-	-	Dominio
ListFolders	-	-	Carpetas
ListGridNodes	-	-	-
ListGroupsForUser	-	-	Dominio
ListGroupPermissions	-	-	-
ListGroupPrivilege	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
ListLDAPConnectivity	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ListLicenses	-	-	Objetos de licencia
listMonitoringOptions	Supervisión	Configuración de supervisión	Dominio
ListNodeOptions	-	-	Nodo
ListNodes	-	-	-
ListNodeResources	-	-	Nodo
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Dominio
ListRolePrivileges	-	-	-
ListSecurityDomains	Administración de seguridad	Gestionar usuarios, grupos y roles	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
ListServiceLevels	-	-	Dominio
ListServiceNodes	-	-	Servicio de aplicación
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListSMTPOptions	-	-	Dominio
ListUserPermissions	-	-	-
ListUserPrivilege	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
MoveFolder	Administración de dominios	Administrar carpetas del dominio	Carpetas originales y de destino
MoveObject (en servicios de aplicación u objetos de licencia)	Administración de dominios	Gestionar servicios	Carpetas originales y de destino
MoveObject (en nodos o mallas)	Administración de dominios	Administrar nodos y mallas	Carpetas originales y de destino
Ping	-	-	-
PurgeLog	-	-	-
purgeMonitoringData	Supervisión	Configuración de supervisión	Dominio
RemoveAlertUser (para su cuenta de usuario)	-	-	-
RemoveAlertUser (para otros usuarios)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RemoveConnection	-	-	Escribir al conectar
RemoveConnectionPermissions	-	-	Conceder al conectar
RemoveDomainLink	-	-	-
RemoveFolder	Administración de dominios	Administrar carpetas del dominio	Dominio o carpeta primaria y carpeta que se va a quitar

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
RemoveGrid	Administración de dominios	Administrar nodos y mallas	Dominio o carpeta y malla primaria
RemoveGroup	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RemoveGroupPrivilege	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
RemoveLicense	Administración de dominios	Gestionar servicios	Dominio o carpeta primario y objeto de licencia
RemoveNode	Administración de dominios	Administrar nodos y mallas	Dominio o carpeta y nodo primario
RemoveNodeResource	Administración de dominios	Administrar nodos y mallas	Nodo
RemoveOSProfile	-	-	-
RemoveRole	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RemoveRolePrivilege	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RemoveService	Administración de dominios	Gestionar servicios	Dominio o carpeta primaria y servicio de aplicación
RemoveServiceLevel	-	-	-
RemoveUser	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RemoveUserFromGroup	Administración de seguridad	Gestionar usuarios, grupos y roles	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
RemoveUserPrivilege	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
RenameConnection	-	-	Escribir al conectar
ResetPassword (para su cuenta de usuario)	-	-	-
ResetPassword (para otros usuarios)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RunCPUProfile	Administración de dominios	Administrar nodos y mallas	Nodo
SetConnectionPermission	-	-	Conceder al conectar
SetLDAPConnectivity	Administración de seguridad	Gestionar usuarios, grupos y roles	-
SetRepositoryLDAPConfiguration	-	-	Dominio
ShowLicense	-	-	Objeto de licencia
ShutdownNode	Administración de dominios	Administrar nodos y mallas	Nodo
SwitchToGatewayNode	-	-	-
SwitchToWorkerNode	-	-	-
UnAssignISMMService	Administración de dominios	Gestionar servicios	Servicio de integración de PowerCenter y servicio de Metadata Manager
UnassignLicense	Administración de dominios	Gestionar servicios	Objeto de licencia y servicio de aplicación
UnAssignRoleFromGroup	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
UnAssignRoleFromUser	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
UnassignRSWHubService	Administración de dominios	Gestionar servicios	Servicio de repositorio de PowerCenter y concentrador de servicios web
UnassociateDomainNode	Administración de dominios	Administrar nodos y mallas	Nodo
UpdateConnection	-	-	Escribir al conectar
UpdateDomainOptions	-	-	-
UpdateFolder	Administración de dominios	Administrar carpetas del dominio	Carpeta
UpdateGatewayInfo	-	-	-
UpdateGrid	Administración de dominios	Administrar nodos y mallas	Malla y nodos
UpdateIntegrationService	Administración de dominios	Gestionar servicios	Servicio de integración de PowerCenter
UpdateLicense	Administración de dominios	Gestionar servicios	Objeto de licencia
UpdateMMService	Administración de dominios	Gestionar servicios	Servicio de Metadata Manager
updateMonitoringOptions	Supervisión	Configuración de supervisión	Dominio
UpdateNodeOptions	Administración de dominios	Administrar nodos y mallas	Nodo
UpdateNodeRole	Administración de dominios	Administrar nodos y mallas	Nodo
UpdateOSPProfile	Administración de seguridad	Gestionar usuarios, grupos y roles	Perfil del sistema operativo

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
UpdateRepositoryService	Administración de dominios	Gestionar servicios	Servicio de repositorio de PowerCenter
UpdateSAPBWService	Administración de dominios	Gestionar servicios	Servicio SAP BW
UpdateServiceLevel	-	-	-
UpdateServiceProcess	Administración de dominios	Gestionar servicios	Servicio de integración de PowerCenter Cada nodo añadido al servicio de integración de PowerCenter
UpdateSMTPOptions	-	-	-
UpdateWSHubService	Administración de dominios	Gestionar servicios	concentrador de servicios web

## Comandos infacmd mrs

Para ejecutar comandos *infacmd mrs*, los usuarios deben tener uno de los conjuntos enumerados de privilegios del dominio, privilegios del servicio de repositorio de modelos y permisos de objetos del repositorio de modelos.

Los usuarios pueden ejecutar los siguientes comandos, que están relacionados con las operaciones de bloqueo y de control de versiones, en los objetos de los que sean propietarios. La ejecución de los comandos en objetos que sean propiedad de otros usuarios requiere el privilegio Administrar desarrollo basado en equipos:

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout
- UnlockObject



En la siguiente tabla, se enumeran los privilegios y permisos necesarios para los comandos *infacmd mrs*

Comando <i>infacmd mrs</i>	Grupo de privilegios	Nombre de privilegio	Permiso de...
BackupContents	Administración de dominios	Servicio de administración	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos
CheckInObject	Administración de dominios	Administrar desarrollo basado en equipos	El servicio de repositorio de modelos
CreateContents	Administración de dominios	Servicio de administración	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos
CreateFolder	Administración de dominios	Para Developer tool: - Acceder con el desarrollador  Para la Herramienta del analista: - Acceder con el analista - Acceder al espacio de trabajo Detección	El servicio de repositorio de modelos
CreateProject	Administración de dominios	Crear, editar y eliminar proyectos	El servicio de repositorio de modelos
CreateService	Administración de dominios	Servicio de administración	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos
DeleteContents	Administración de dominios	Servicio de administración	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos
DeleteFolder	Administración de dominios	Para Developer tool: - Acceder con el desarrollador  Para la Herramienta del analista: - Acceder con el analista - Acceder al espacio de trabajo Detección	El servicio de repositorio de modelos
DeleteProject	Administración de dominios	Crear, editar y eliminar proyectos	El servicio de repositorio de modelos
ListBackupFiles	Administración de dominios	Servicio de administración	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos
ListCheckedOutObjects	Administración de dominios	Administrar desarrollo basado en equipos	El servicio de repositorio de modelos
ListFolders	Administración de dominios	Servicio de administración	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos

Comando infacmd mrs	Grupo de privilegios	Nombre de privilegio	Permiso de...
ListLockedObjects	Administración de dominios	Administrar desarrollo basado en equipos	El servicio de repositorio de modelos
ListProjects	Administración de dominios	Para Developer tool: - Acceder con el desarrollador  Para la Herramienta del analista: - Acceder con el analista - Acceder al espacio de trabajo Detección	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos
ListServiceOptions	-	-	El servicio de repositorio de modelos
ListServiceProcessOptions	-	-	El servicio de repositorio de modelos
PopulateVCS	Administración de dominios	Administrar desarrollo basado en equipos	El servicio de repositorio de modelos
ReassignCheckedOutObject	Administración de dominios	Administrar desarrollo basado en equipos	El servicio de repositorio de modelos
RebuildDependencyGraph	-	-	El servicio de repositorio de modelos
RenameFolder	Administración de dominios	Para Developer tool: - Acceder con el desarrollador  Para la Herramienta del analista: - Acceder con el analista - Acceder al espacio de trabajo Detección	El servicio de repositorio de modelos
RestoreContents	Administración de dominios	Servicio de administración	El dominio o el nodo en el que se ejecuta el servicio de repositorio de modelos
UndoCheckout	Administración de dominios	Administrar desarrollo basado en equipos	El servicio de repositorio de modelos
UnlockObject	Administración de dominios	Administrar desarrollo basado en equipos	El servicio de repositorio de modelos
UpdateServiceOptions	Administración de dominios	Servicio de administración	El servicio de repositorio de modelos
UpdateServiceProcessOptions	Administración de dominios	Servicio de administración	El servicio de repositorio de modelos
UpgradeContents	Administración del servicio de repositorio de modelos	Servicio de administración	El servicio de repositorio de modelos

## Comandos infacmd ms

Para ejecutar comandos *infacmd ms*, los usuarios deben poseer uno de los conjuntos de permisos del objeto de dominio que se enumeran.

La siguiente tabla enumera los privilegios y los permisos necesarios para los comandos *infacmd ms*:

Comando infacmd ms	Grupo de privilegios	Nombre de privilegio	Permiso de...
GetRequestLog	-	-	-
ListMappings	-	-	-
ListMappingParams	-	-	-
RunMapping	-	-	Ejecución de objetos de conexión usados por la asignación

## Comandos infacmd oie

Para ejecutar comandos *infacmd oie*, los usuarios deben poseer uno de los permisos de objeto del repositorio de modelos que se enumeran.

La siguiente tabla enumera los permisos necesarios para los comandos *infacmd oie*:

Comando infacmd oie	Grupo de privilegios	Nombre de privilegio	Permiso de...
ExportObjects	-	-	Lectura en proyecto
ImportObjects	-	-	Escritura en proyecto

## Comandos infacmd ps

Para ejecutar comandos *infacmd ps*, los usuarios deben poseer uno de los conjuntos de privilegios de creación de perfiles y permisos del objeto de dominio que se enumeran.

La siguiente tabla enumera los privilegios y los permisos necesarios para los comandos *infacmd ps*:

Comando infacmd ps	Grupo de privilegios	Nombre de privilegio	Permiso de...
CreateWH	-	-	-
DropWH	-	-	-

Comando infacmd ps	Grupo de privilegios	Nombre de privilegio	Permiso de...
Ejecución	-	-	Lectura en proyecto Ejecución en el objeto de conexión de origen
List	-	-	Lectura en proyecto
Purge	-	-	Lectura y escritura en proyecto

Comando infacmd ps	Grupo de privilegios	Nombre de privilegio	Permiso de...
CreateWH	-	-	-
DropWH	-	-	-

## Comandos infacmd pwx

Para ejecutar comandos *infacmd pwx*, los usuarios deben tener uno de los conjuntos enumerados de permisos y privilegios del servicio de aplicaciones de PowerExchange.

La siguiente tabla enumera los privilegios y permisos necesarios para los comandos *infacmd pwx*:

Comando infacmd pwx	Grupo de privilegios	Nombre de privilegio	Permiso de...
CloseForceListener	Comandos de administración	closeforce	-
CloseListener	Comandos de administración	cerrar	-
CondenseLogger	Comandos de administración	condensar	-
CreateListenerService	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio de aplicación de PowerExchange
CreateLoggerService	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio de aplicación de PowerExchange
DisplayAllLogger	Comandos informativos	displayall	-
DisplayCPULogger	Comandos informativos	displaycpu	-

Comando infacmd pwx	Grupo de privilegios	Nombre de privilegio	Permiso de...
DisplayEventsLogger	Comandos informativos	displayevents	-
DisplayMemoryLogger	Comandos informativos	displaymemory	-
DisplayRecordsLogger	Comandos informativos	displayrecords	-
DisplayStatusLogger	Comandos informativos	displaystatus	-
FileSwitchLogger	Comandos de administración	fileswitch	-
ListTaskListener	Comandos informativos	listtask	-
ShutDownLogger	Comandos de administración	apagar	-
StopTaskListener	Comandos de administración	stoptask	-
UpdateListenerService	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio de aplicación de PowerExchange
UpdateLoggerService	Administración de dominios	Servicio de administración	Dominio o nodo donde se ejecuta el servicio de aplicación de PowerExchange

## Comandos infacmd rms

Para poder ejecutar comandos *infacmd rms*, los usuarios deben tener uno de los conjuntos de privilegios y permisos de dominio enumerados.

En la siguiente tabla, se enumeran los privilegios y permisos requeridos para los comandos *infacmd rms*:

Comando infacmd rms	Grupo de privilegios	Nombre de privilegio	Permiso para
ListComputeNodeAttributes	Administración de dominios	-	Servicio de administrador de recursos
ListServiceOptions	Administración de dominios	-	Servicio de administrador de recursos

Comando infacmd rms	Grupo de privilegios	Nombre de privilegio	Permiso para
SetComputeNodeAttributes	Administración de dominios	Gestionar servicios	Servicio de administrador de recursos
UpdateServiceOptions	Administración de dominios	Gestionar servicios	Servicio de administrador de recursos

## Comandos infacmd rtm

Para ejecutar comandos *infacmd rtm*, los usuarios deben poseer uno de los conjuntos de privilegios del servicio de repositorio de modelos y permisos del objeto de dominio que se enumeran.

La siguiente tabla enumera los privilegios y los permisos necesarios para los comandos *infacmd rtm*:

Comando infacmd rtm	Grupo de privilegios	Nombre de privilegio	Permiso de...
Deployimport	-	-	-
Exportar	-	-	Lectura en el proyecto que contiene las tablas de referencia que se exportarán
Importar	-	-	Lectura y escritura en el proyecto donde se importarán las tablas de referencia

## Comandos infacmd sch

Para poder ejecutar comandos *infacmd sch*, los usuarios deben tener uno de los conjuntos de privilegios y permisos de dominio enumerados.

En la siguiente tabla, se enumeran los privilegios y permisos requeridos para los comandos *infacmd sch*:

Comando infacmd sch	Grupo de privilegios	Nombre del privilegio	Permiso en
CreateSchedule	Privilegios de programador	Crear programa	Servicio de programador
DeleteSchedule	Privilegios de programador	Eliminar programa	Servicio de programador
ListSchedule	Privilegios de programador	Ver programas	Servicio de programador
ListServiceOptions	Privilegios del dominio	Gestionar servicios	Servicio de programador
ListServiceProcessOptions	Privilegios del dominio	Gestionar servicios	Servicio de programador

Comando infacmd sch	Grupo de privilegios	Nombre del privilegio	Permiso en
PauseAll	Privilegios de programador	Editar programa	Servicio de programador
PauseSchedule	Privilegios de programador	Editar programa	Servicio de programador
ResumeAll	Privilegios de programador	Editar programa	Servicio de programador
ResumeSchedule	Privilegios de programador	Editar programa	Servicio de programador
UpdateSchedule	Privilegios de programador	Editar programa	Servicio de programador
UpdateService	Privilegios del dominio	Gestionar servicios	Servicio de programador
UpdateServiceProcess	Privilegios del dominio	Gestionar servicios	Servicio de programador
Actualizar	Privilegios del dominio	Gestionar servicios	Servicio de programador

## Comandos infacmd sql

Para ejecutar comandos *infacmd sql*, los usuarios deben tener uno de los conjuntos enumerados de permisos, privilegios para el servicio de integración de datos y permisos para los objetos de dominio.

La siguiente tabla enumera los privilegios y permisos necesarios para los comandos *infacmd sql*:

Comando infacmd sql	Grupo de privilegios	Nombre de privilegio	Permiso de...
ExecuteSQL	-	-	Basado en objetos a los que se vaya a acceder en las instrucciones SQL.
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-

Comando infacmd sql	Grupo de privilegios	Nombre de privilegio	Permiso de...
RenameSQLDataService	Administración de aplicaciones	Administrar aplicaciones	-
SetColumnPermissions	-	-	Concedido para el objeto
SetSQLDataServicePermissions	-	-	Concedido para el objeto
SetStoredProcedurePermissions	-	-	Concedido para el objeto
SetTablePermissions	-	-	Concedido para el objeto
StartSQLDataService	Administración de aplicaciones	Administrar aplicaciones	-
StopSQLDataService	Administración de aplicaciones	Administrar aplicaciones	-
UpdateColumnOptions	Administración de aplicaciones	Administrar aplicaciones	-
UpdateSQLDataServiceOptions	Administración de aplicaciones	Administrar aplicaciones	-
UpdateTableOptions	Administración de aplicaciones	Administrar aplicaciones	-

## Comandos infacmd wfs

Para ejecutar comandos infacmd wfs, los usuarios no requieren privilegios ni permisos.

## Comandos pmcmd

Para ejecutar los comandos *pmcmd*, los usuarios deben tener los conjuntos de privilegios del Servicio de repositorio de PowerCenter y los permisos de objeto del repositorio de PowerCenter que se indican a continuación.

Cuando el Servicio de integración de PowerCenter se ejecuta en modo seguro, los usuarios deben tener la función de administrador para el Servicio de repositorio de PowerCenter asociado para ejecutar los siguientes comandos:

- aborttask
- abortworkflow
- getrunningsessionsdetails



- getservicedetails
- getsessionstatistics
- gettaskdetails
- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow
- unscheduleworkflow

En la siguiente tabla se enumeran los privilegios y permisos necesarios para los comandos *pmcmd* :

Comando pmcmd	Grupo de privilegios	Nombre de privilegio	Permiso
aborttask (cuando lo inicia la cuenta del usuario)	-	-	Lectura y ejecución en carpeta
aborttask (cuando lo inician otros usuarios)	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta
abortworkflow (cuando lo inicia la cuenta del usuario)	-	-	Lectura y ejecución en carpeta
abortworkflow (cuando lo inician otros usuarios)	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta
connect	-	-	-
disconnect	-	-	-
exit	-	-	-
getrunningsessionsdetails	Objetos en tiempo de ejecución	Supervisar	-
getservicedetails	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta
getserviceproperties	-	-	-
getsessionstatistics	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta
gettaskdetails	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta
getworkflowdetails	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta
help	-	-	-

Comando pmcmd	Grupo de privilegios	Nombre de privilegio	Permiso
pingservice	-	-	-
recoverworkflow (cuando lo inicia la cuenta de usuario)	Objetos en tiempo de ejecución	Ejecutar	Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión Permisos del perfil del sistema operativo (cuando sea aplicable)
recoverworkflow (cuando lo inician otros usuarios)	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión Permisos del perfil del sistema operativo (cuando sea aplicable)
scheduleworkflow	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión Permisos del perfil del sistema operativo (cuando sea aplicable)
setfolder	-	-	Lectura en carpeta
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	Objetos en tiempo de ejecución	Ejecutar	Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión Permisos del perfil del sistema operativo (cuando sea aplicable)
startworkflow	Objetos en tiempo de ejecución	Ejecutar	Lectura y ejecución en carpeta Lectura y ejecución en objeto de conexión Permisos del perfil del sistema operativo (cuando sea aplicable)
stoptask (cuando lo inicia la cuenta de usuario)	-	-	Lectura y ejecución en carpeta
stoptask (cuando lo inician otros usuarios)	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta
stopworkflow (cuando lo inicia la cuenta de usuario)	-	-	Lectura y ejecución en carpeta
stopworkflow (cuando lo inician otros usuarios)	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta

Comando pmcmd	Grupo de privilegios	Nombre de privilegio	Permiso
unscheduleworkflow	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta
unsetfolder	-	-	Lectura en carpeta
version	-	-	-
waittask	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta
waitworkflow	Objetos en tiempo de ejecución	Supervisar	Lectura en carpeta

## Comandos pmrep

Los usuarios deben tener el privilegio de acceso al administrador de repositorios para poder ejecutar todos los comandos *pmrep*, a excepción de los siguientes:

- Run
- Crear
- Restore
- Upgrade
- Version
- Ayuda

Para ejecutar los comandos *pmrep*, los usuarios deben tener uno de los conjuntos enumerados de privilegios del dominio, privilegios del servicio de repositorio de modelos, permisos de objetos de dominio y permisos de objetos del repositorio de PowerCenter.

Los usuarios deben ser el propietario del objeto o tener la función de administrador para que el servicio del repositorio de PowerCenter ejecute los siguientes comandos:

- AssignPermission
- ChangeOwner
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- ModifyFolder (para cambiar propietario, configurar permisos, designar la carpeta como compartida o editar el nombre o descripción de la carpeta)

En la siguiente tabla, se enumeran los privilegios y permisos requeridos para los comandos *pmrep*:

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
AddToDeploymentGroup	Objetos globales	Administración de grupos de implementación	Lectura en carpeta original Lectura y escritura en grupo de implementación
ApplyLabel	-	-	Lectura en carpeta Lectura y ejecución en etiqueta
AssignPermission	-	-	-
BackUp	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
ChangeOwner	-	-	-
CheckIn (para las desprotecciones propias)	Objetos de diseño	Creación, edición y eliminación	Lectura y escritura en carpeta
CheckIn (para las desprotecciones propias)	Orígenes y destinos	Creación, edición y eliminación	Lectura y escritura en carpeta
CheckIn (para las desprotecciones propias)	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta
CheckIn (para las desprotecciones de otros)	Objetos de diseño	Administración de versiones	Lectura y escritura en carpeta
CheckIn (para las desprotecciones de otros)	Orígenes y destinos	Administración de versiones	Lectura y escritura en carpeta
CheckIn (para las desprotecciones de otros)	Objetos de tiempo de ejecución	Administración de versiones	Lectura y escritura en carpeta
CleanUp	-	-	-
ClearDeploymentGroup	Objetos globales	Administración de grupos de implementación	Lectura y escritura en grupo de implementación
Connect	-	-	-
Crear	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
CreateConnection	Objetos globales	Creación de conexiones	-
CreateDeploymentGroup	Objetos globales	Administración de grupos de implementación	-
CreateFolder	Carpetas	Crear	-
CreateLabel	Objetos globales	Creación de etiquetas	-

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
Eliminar	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	Objetos de diseño	Creación, edición y eliminación	Lectura y escritura en carpeta
DeleteObject	Orígenes y destinos	Creación, edición y eliminación	Lectura y escritura en carpeta
DeleteObject	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta
DeployDeploymentGroup	Objetos globales	Administración de grupos de implementación	Lectura en carpeta original Lectura y escritura en carpeta de destino Lectura y ejecución en grupo de implementación
DeployFolder	Carpetas	Copia en repositorio original Creación en repositorio de destino	Lectura en carpeta
ExecuteQuery	-	-	Lectura y ejecución en consulta
Exit	-	-	-
FindCheckout	-	-	Lectura en carpeta
GetConnectionDetails	-	-	Lectura en objeto de conexión
Ayuda	-	-	-
KillUserConnection	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
ListConnections	-	-	Lectura en objeto de conexión
ListObjectDependencies	-	-	Lectura en carpeta
ListObjects	-	-	Lectura en carpeta
ListTablesBySess	-	-	Lectura en carpeta
ListUserConnections	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
ModifyFolder (para cambiar propietario, configurar permisos, designar la carpeta como compartida o editar el nombre o descripción de la carpeta)	-	-	-
ModifyFolder (para modificar el estado)	Carpetas	Administración de versiones	Lectura y escritura en carpeta
Notify	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
ObjectExport	-	-	Lectura en carpeta
ObjectImport	Objetos de diseño	Creación, edición y eliminación	Lectura y escritura en carpeta
ObjectImport	Orígenes y destinos	Creación, edición y eliminación	Lectura y escritura en carpeta
ObjectImport	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta
PurgeVersion	Objetos de diseño	Administración de versiones	Lectura y escritura en carpeta Lectura, escritura y ejecución en consulta si se especifica un nombre de consulta
PurgeVersion	Orígenes y destinos	Administración de versiones	Lectura y escritura en carpeta Lectura, escritura y ejecución en consulta si se especifica un nombre de consulta
PurgeVersion	Objetos de tiempo de ejecución	Administración de versiones	Lectura y escritura en carpeta Lectura, escritura y ejecución en consulta si se especifica un nombre de consulta
PurgeVersion (para purgar objetos en el nivel de la carpeta)	Carpetas	Administración de versiones	Lectura y escritura en carpeta
PurgeVersion (para purgar objetos en el nivel del repositorio)	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
Register	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
RegisterPlugin	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
Restore	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
RollbackDeployment	Objetos globales	Administración de grupos de implementación	Lectura y escritura en carpeta de destino
Run	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta Lectura en objeto de conexión
TruncateLog	Objetos de tiempo de ejecución	Administración de ejecución	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones propias)	Objetos de diseño	Creación, edición y eliminación	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones propias)	Orígenes y destinos	Creación, edición y eliminación	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones propias)	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones de otros)	Objetos de diseño	Administración de versiones	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones de otros)	Orígenes y destinos	Administración de versiones	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones de otros)	Objetos de tiempo de ejecución	Administración de versiones	Lectura y escritura en carpeta
Unregister	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
UnregisterPlugin	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
UpdateConnection	-	-	Lectura y escritura en objeto de conexión
UpdateEmailAddr	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta
UpdateSeqGenVals	Objetos de diseño	Creación, edición y eliminación	Lectura y escritura en carpeta
UpdateSrcPrefix	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta
UpdateStatistics	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
UpdateTargPrefix	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
Upgrade	Administración de dominios	Administración de servicios	Permiso para el servicio de repositorio de PowerCenter
Validate	Objetos de diseño	Creación, edición y eliminación	Lectura y escritura en carpeta
Validate	Objetos de tiempo de ejecución	Creación, edición y eliminación	Lectura y escritura en carpeta
Version	-	-	-



## APÉNDICE B

# Funciones personalizadas

Este apéndice incluye los siguientes temas:

- [Función personalizada del Servicio del analista, 249](#)
- [Funciones personalizadas del Servicio de Metadata Manager, 250](#)
- [Función personalizada del operador, 252](#)
- [Funciones personalizadas del Servicio de repositorio de PowerCenter, 253](#)
- [Funciones personalizadas de Test Data Manager, 254](#)

## Función personalizada del Servicio del analista

El Consumidor de glosario empresarial del Servicio del analista es una función personalizada del Servicio del analista.

La siguiente tabla muestra el privilegio predeterminado asignado a la función personalizada Consumidor de glosario empresarial del Servicio del analista:

Grupo de privilegios	Nombre del privilegio
Acceso al espacio de trabajo	Espacio de trabajo de glosario

# Funciones personalizadas del Servicio de Metadata Manager

Las funciones personalizadas del Servicio de Metadata Manager incluyen las funciones de usuario avanzado de Metadata Manager, usuario básico de Metadata Manager y usuario intermedio de Metadata Manager.

## Usuario avanzado de Metadata Manager

La tabla siguiente enumera los privilegios predeterminados asignados a la función personalizada del usuario avanzado de Metadata Manager:

Grupo de privilegios	Nombre del privilegio
Catálogo	<ul style="list-style-type: none"><li>- Compartir accesos directos</li><li>- Ver linaje</li><li>- Ver catálogos relacionados</li><li>- Ver informes</li><li>- Ver resultados de perfil</li><li>- Ver catálogo</li><li>- Ver relaciones</li><li>- Administrar relaciones</li><li>- Ver comentarios</li><li>- Insertar comentarios</li><li>- Eliminar comentarios</li><li>- Ver vínculos</li><li>- Administrar vínculos</li><li>- Ver glosario</li><li>- Administrar objetos</li></ul>
Cargar	<ul style="list-style-type: none"><li>- Ver recurso</li><li>- Cargar recurso</li><li>- Administrar programas</li><li>- Purgar metadatos</li><li>- Administrar recursos</li></ul>
Modelo	<ul style="list-style-type: none"><li>- Ver modelo</li><li>- Administrar modelo</li><li>- Exportar/Importar modelos</li></ul>
Seguridad	Administrar permisos de catálogo

### Usuario básico de Metadata Manager

En la tabla siguiente se enumeran los privilegios predeterminados asignados a la función personalizada del usuario básico de Metadata Manager:

Grupo de privilegios	Nombre del privilegio
Catálogo	<ul style="list-style-type: none"><li>- Ver linaje</li><li>- Ver catálogos relacionados</li><li>- Ver catálogo</li><li>- Ver relaciones</li><li>- Ver comentarios</li><li>- Ver vínculos</li></ul>
Modelo	Ver modelo

### Usuario intermedio de Metadata Manager

En la tabla siguiente se enumeran los privilegios predeterminados asignados a la función personalizada del usuario intermedio de Metadata Manager:

Grupo de privilegios	Nombre del privilegio
Catálogo	<ul style="list-style-type: none"><li>- Ver linaje</li><li>- Ver catálogos relacionados</li><li>- Ver informes</li><li>- Ver resultados de perfil</li><li>- Ver catálogo</li><li>- Ver relaciones</li><li>- Ver comentarios</li><li>- Insertar comentarios</li><li>- Eliminar comentarios</li><li>- Ver vínculos</li><li>- Administrar vínculos</li><li>- Ver glosario</li></ul>
Cargar	<ul style="list-style-type: none"><li>- Ver recurso</li><li>- Cargar recurso</li></ul>
Modelo	Ver modelo

# Función personalizada del operador

La función personalizada del operador incluye privilegios para administrar, programar y supervisar servicios de aplicación.

La tabla siguiente enumera los privilegios predeterminados asignados a la función personalizada Operador:

Grupo de privilegios	Nombre del privilegio
Administración de la aplicación	Administrar aplicaciones
Administración de dominios	Administrar ejecución de servicio
Administración del servicio de repositorio de modelos	Administrar desarrollo basado en equipos
Supervisión	<p>El grupo de privilegios Supervisión incluye los siguientes privilegios:</p> <ul style="list-style-type: none"><li>- Ver: Ver trabajos de otros usuarios</li><li>- Ver: Ver estadísticas</li><li>- Ver: Ver informes</li><li>- Acceder a la supervisión: Acceso desde la Herramienta del analista</li><li>- Acceder a la supervisión: Acceso desde Developer tool</li><li>- Acceder a la supervisión: Acceso desde la herramienta Administrator</li><li>- Realizar acciones en tareas</li></ul> <p><b>Nota:</b> En un dominio que utiliza la autenticación Kerberos, los usuarios deben tener también la función de administrador del servicio de repositorio de modelos que se ha configurado para supervisar.</p>
Programador	<p>El grupo de privilegios Programador incluye los siguientes privilegios:</p> <ul style="list-style-type: none"><li>- Administrar trabajos programados: Crear programa</li><li>- Administrar trabajos programados: Eliminar programa</li><li>- Administrar trabajos programados: Editar programa</li><li>- Administrar los trabajos programados: Ver programas</li></ul>
Herramientas	Acceder a Informatica Administrator

# Funciones personalizadas del Servicio de repositorio de PowerCenter

Las funciones personalizadas del Servicio de repositorio de PowerCenter incluyen Administrador de conexiones de PowerCenter, Desarrollador de PowerCenter, Operador de PowerCenter y Administrador de carpetas del repositorio de PowerCenter.

## Administrador de conexiones de PowerCenter

La tabla siguiente enumera los privilegios predeterminados asignados a la función personalizada del administrador de conexiones de PowerCenter:

Grupo de privilegios	Nombre del privilegio
Herramientas	Acceso al administrador de flujos de trabajo
Objetos globales	Crear conexiones

## Desarrollador de PowerCenter

En la siguiente tabla se enumeran los privilegios predeterminados asignados a la función personalizada de Desarrollador de PowerCenter:

Grupo de privilegios	Nombre del privilegio
Herramientas	<ul style="list-style-type: none"><li>- Acceso a Designer</li><li>- Acceso al administrador de flujos de trabajo</li><li>- Acceso al supervisor de flujos de trabajo</li></ul>
Objetos de diseño	<ul style="list-style-type: none"><li>- Crear, editar y eliminar</li><li>- Administrar versiones</li></ul>
Orígenes y destinos	<ul style="list-style-type: none"><li>- Crear, editar y eliminar</li><li>- Administrar versiones</li></ul>
Objetos en tiempo de ejecución	<ul style="list-style-type: none"><li>- Crear, editar y eliminar</li><li>- Ejecutar</li><li>- Administrar versiones</li><li>- Supervisar</li></ul>

## Operador de PowerCenter

La tabla siguiente enumera los privilegios predeterminados asignados a la función personalizada de Operador de PowerCenter:

Grupo de privilegios	Nombre del privilegio
Herramientas	Acceso al supervisor de flujos de trabajo
Objetos en tiempo de ejecución	<ul style="list-style-type: none"><li>- Ejecutar</li><li>- Administrar ejecución</li><li>- Supervisar</li></ul>

## Administrador de carpetas del repositorio de PowerCenter

La tabla siguiente enumera los privilegios predeterminados asignados a la función personalizada de Administrador de carpetas del repositorio de PowerCenter:

Grupo de privilegios	Nombre del privilegio
Herramientas	Acceder al Repository Manager
Carpetas	<ul style="list-style-type: none"><li>- Copiar</li><li>- Crear</li><li>- Administrar versiones</li></ul>
Objetos globales	<ul style="list-style-type: none"><li>- Administrar grupos de implementación</li><li>- Ejecutar grupos de implementación</li><li>- Crear etiquetas</li><li>- Crear consultas</li></ul>

# Funciones personalizadas de Test Data Manager

Las funciones personalizadas del servicio de Test Data Manager incluyen el administrador de datos de prueba, el desarrollador de datos de prueba, el DBA de proyecto de datos de prueba, el desarrollador del

proyecto de datos de prueba, el propietario del proyecto de datos de prueba, el administrador de riesgos de datos de prueba, el especialista de datos de prueba y el ingeniero de pruebas.

### Administrador de datos de prueba

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de administrador de datos de prueba:

Grupo de privilegios	Nombre del privilegio
Proyectos	Auditar proyecto
Administración	<ul style="list-style-type: none"><li>- Ver conexiones</li><li>- Administrar conexiones</li><li>- Administrar preferencias</li></ul>

### Desarrollador de datos de prueba

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de desarrollador de datos de prueba:

Grupo de privilegios	Nombre del privilegio
Directivas	<ul style="list-style-type: none"><li>- Ver directivas</li><li>- Administrar directivas</li></ul>
Dominios de datos	<ul style="list-style-type: none"><li>- Ver dominios de datos</li><li>- Administrar dominios de datos</li></ul>
Reglas	<ul style="list-style-type: none"><li>- Ver reglas de enmascaramiento</li><li>- Administrar reglas de enmascaramiento</li><li>- Ver reglas de generación</li><li>- Administrar reglas de generación</li></ul>
Proyectos	Auditar proyecto

### DBA de proyecto de datos de prueba

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de DBA del proyecto de datos de prueba:

Grupo de privilegios	Nombre del privilegio
Proyectos	<ul style="list-style-type: none"><li>- Ver proyecto</li><li>- Ejecutar proyecto</li><li>- Supervisar proyecto</li><li>- Auditar proyecto</li></ul>
Administración	<ul style="list-style-type: none"><li>- Ver conexiones</li><li>- Administrar conexiones</li></ul>
Conjuntos de datos	<ul style="list-style-type: none"><li>- Ver un conjunto de datos</li><li>- Ver datos en un conjunto de datos</li></ul>

### Desarrollador de proyecto de datos de prueba

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de desarrollador del proyecto de datos de prueba:

Grupo de privilegios	Nombre del privilegio
Directivas	Ver directivas
Reglas	<ul style="list-style-type: none"><li>- Ver reglas de enmascaramiento</li><li>- Ver reglas de generación</li><li>- Administrar reglas de generación</li></ul>
Dominios de datos	Ver dominios de datos
Proyectos	<ul style="list-style-type: none"><li>- Ver proyecto</li><li>- Detectar proyecto</li><li>- Ejecutar proyecto</li><li>- Supervisar proyecto</li><li>- Auditar proyecto</li><li>- Importar metadatos</li></ul>
Enmascaramiento de datos	<ul style="list-style-type: none"><li>- Ver enmascaramiento de datos</li><li>- Administrar enmascaramiento de datos</li></ul>
Subconjunto de datos	<ul style="list-style-type: none"><li>- Ver subconjuntos de datos</li><li>- Administrar subconjuntos de datos</li></ul>
Generación de datos	<ul style="list-style-type: none"><li>- Ver la generación de datos</li><li>- Administrar la generación de datos</li></ul>
Administración	<ul style="list-style-type: none"><li>- Ver conexiones</li><li>- Administrar conexiones</li></ul>
Conjuntos de datos	<ul style="list-style-type: none"><li>- Ver un conjunto de datos</li><li>- Ver datos en un conjunto de datos</li></ul>

### Propietario de proyecto de datos de prueba

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de propietario del proyecto de datos de prueba:

Grupo de privilegios	Nombre del privilegio
Directivas	Ver directivas
Reglas	<ul style="list-style-type: none"><li>- Ver reglas de enmascaramiento</li><li>- Ver reglas de generación</li><li>- Administrar reglas de generación</li></ul>
Dominios de datos	Ver dominios de datos



Grupo de privilegios	Nombre del privilegio
Proyectos	<ul style="list-style-type: none"> <li>- Ver proyecto</li> <li>- Administrar proyectos</li> <li>- Detectar proyecto</li> <li>- Ejecutar proyecto</li> <li>- Supervisar proyecto</li> <li>- Auditar proyecto</li> <li>- Importar metadatos</li> </ul>
Enmascaramiento de datos	<ul style="list-style-type: none"> <li>- Ver enmascaramiento de datos</li> <li>- Administrar enmascaramiento de datos</li> </ul>
Subconjunto de datos	<ul style="list-style-type: none"> <li>- Ver subconjuntos de datos</li> <li>- Administrar subconjuntos de datos</li> </ul>
Generación de datos	<ul style="list-style-type: none"> <li>- Ver la generación de datos</li> <li>- Administrar la generación de datos</li> </ul>
Administración	<ul style="list-style-type: none"> <li>- Ver conexiones</li> <li>- Administrar conexiones</li> </ul>
Conjuntos de datos	<ul style="list-style-type: none"> <li>- Ver un conjunto de datos</li> <li>- Ver datos en un conjunto de datos</li> <li>- Administrar un conjunto de datos</li> <li>- Administrar datos en un conjunto de datos</li> <li>- Restablecer un conjunto de datos</li> </ul>

### Administrador de riesgos de datos de prueba

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de administrador de riesgos de datos de prueba:

Grupo de privilegios	Nombre del privilegio
Directivas	Ver directivas
Reglas	<ul style="list-style-type: none"> <li>- Ver reglas de enmascaramiento</li> <li>- Ver reglas de generación</li> </ul>
Dominios de datos	Ver dominios de datos
Proyectos	Auditar proyecto

## Especialista de datos de prueba

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de especialista de Test Data:

Grupo de privilegios	Nombre del privilegio
Directivas	Ver directivas
Reglas	<ul style="list-style-type: none"><li>- Ver reglas de enmascaramiento</li><li>- Administrar reglas de enmascaramiento</li><li>- Ver reglas de generación</li><li>- Administrar reglas de generación</li></ul>
Dominios de datos	<ul style="list-style-type: none"><li>- Ver dominios de datos</li><li>- Administrar dominios de datos</li></ul>
Proyectos	<ul style="list-style-type: none"><li>- Ver proyecto</li><li>- Administrar proyecto</li><li>- Detectar proyecto</li><li>- Ejecutar proyecto</li><li>- Supervisar proyecto</li><li>- Auditar proyecto</li><li>- Importar metadatos</li></ul>
Enmascaramiento de datos	<ul style="list-style-type: none"><li>- Ver enmascaramiento de datos</li><li>- Administrar enmascaramiento de datos</li></ul>
Subconjunto de datos	<ul style="list-style-type: none"><li>- Ver subconjuntos de datos</li><li>- Administrar subconjuntos de datos</li></ul>
Generación de datos	<ul style="list-style-type: none"><li>- Ver la generación de datos</li><li>- Administrar la generación de datos</li></ul>
Administración	<ul style="list-style-type: none"><li>- Ver conexiones</li><li>- Administrar conexiones</li></ul>
Conjuntos de datos	<ul style="list-style-type: none"><li>- Ver un conjunto de datos</li><li>- Ver datos en un conjunto de datos</li><li>- Administrar un conjunto de datos</li><li>- Administrar datos en un conjunto de datos</li><li>- Restablecer un conjunto de datos</li></ul>

## Ingeniero de pruebas

En la siguiente tabla, se enumeran los privilegios predeterminados asignados a la función personalizada de ingeniero de pruebas:

Grupo de privilegios	Nombre del privilegio
Proyectos	<ul style="list-style-type: none"><li>- Ver proyecto</li><li>- Supervisar proyecto</li></ul>
Conjuntos de datos	<ul style="list-style-type: none"><li>- Ver un conjunto de datos</li><li>- Administrar un conjunto de datos</li><li>- Restablecer un conjunto de datos</li><li>- Ver datos en un conjunto de datos</li><li>- Administrar datos en un conjunto de datos</li></ul>

## APÉNDICE C

# Lista predeterminada de conjuntos de cifrado

De forma predeterminada, el dominio de Informática emplea los siguientes conjuntos de cifrado para la comunicación segura en el dominio y las conexiones de cliente seguras:

- 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

# INDICE

## A

- Administrador
  - función [181](#)
- Administrador de servicios
  - autenticación [103](#)
  - autorización [104](#)
  - inicio de sesión único [103](#)
- administrador del dominio
  - descripción [113](#)
- administrador predeterminado
  - contraseñas, cambiar [113](#)
  - descripción [113](#)
  - modificar [113](#)
- administradores
  - aplicación cliente [113](#)
  - dominio [113](#)
  - predeterminadas [113](#)
- aplicación
  - permisos [200](#)
- archivo de truststore cacerts [28](#)
- archivos de migración de usuario
  - migrateUsers [32](#)
- as
  - permisos por comando [217](#)
  - privilegios por comando [217](#)
- asignación
  - permisos [200](#)
  - permisos heredados [200](#)
- autenticación
  - Administrador de servicios [103](#)
  - Kerberos [20](#)
  - LDAP [19](#), [23](#), [103](#)
  - nativa [19](#), [103](#)
- autenticación de LDAP
  - horas de sincronización [27](#)
- Autenticación de LDAP
  - certificado SSL autofirmado [28](#)
  - configuración [23](#)
  - descripción [19](#), [103](#)
  - grupos anidados [28](#)
  - servicios de directorio [23](#)
- autenticación Kerberos
  - descripción [20](#)
- Autenticación Kerberos
  - usar bibliotecas personalizadas [50](#)
- autenticación nativa
  - descripción [19](#), [103](#)
- autorización
  - Administrador de servicios [104](#)
  - Servicio de integración de datos [104](#)
  - Servicio de Metadata Manager [104](#)
  - Servicio de repositorio de modelos [104](#)
  - Servicio de repositorio de PowerCenter [104](#)
  - servicios de aplicación [104](#)

## C

- cambiar
  - contraseña de cuenta de usuario [108](#)
- carpetas
  - permisos [193](#)
  - privilegios [156](#)
- certificado SSL
  - Autenticación de LDAP [28](#)
  - Autenticación de usuario de LDAP [23](#)
- Cliente de PowerCenter
  - administrador [113](#)
- conexiones
  - permisos [198](#)
  - permisos predeterminados [199](#)
- Conexiones
  - Tipos de permiso [198](#)
- configuración del cliente
  - dominio seguro [60](#)
- consultas de objetos
  - privilegios para PowerCenter [166](#)
- contraseña
  - cambiar para una cuenta de usuario [108](#)
- contraseñas
  - cambiar para administrador predeterminado [113](#)
  - requisitos [115](#)
  - usuarios nativos [115](#)
- convertUserActivityLog
  - registros de actividad del usuario [120](#)
- Crear tablas de referencia
  - privilegio [148](#)
- cuentas
  - cambiar la contraseña [108](#)
- cuentas de usuario
  - cambiar la contraseña [108](#)
  - creadas durante la instalación [113](#)
  - habilitar [117](#)
  - predeterminadas [113](#)
  - resumen [112](#)

## D

- descripción del grupo
  - caracteres no válidos [123](#)
- descripción del usuario
  - caracteres no válidos [115](#)
- destinos
  - privilegios [160](#)
- dis
  - permisos por comando [218](#)
  - privilegios por comando [218](#)
- dominio
  - administrador [113](#)
  - Función de administrador [181](#)
  - privilegios [138](#)

- dominio (*continuado*)
  - privilegios de administración [140](#)
  - privilegios de administración de seguridad [139](#)
  - seguridad del usuario [109](#)
  - sincronización de usuarios [104](#)
  - usuarios con privilegios [187](#)
- dominio de Informática
  - permisos [109](#)
  - privilegios [109](#)
  - seguridad del usuario [109](#)
  - usuarios, administración [115](#)
- dominio de seguridad de LDAP
  - descripción [19](#), [20](#)
- dominio de seguridad nativo
  - descripción [19](#)
- dominio seguro
  - configuración del cliente [60](#)
- dominios de seguridad
  - configuración de LDAP [25](#)
  - eliminar LDAP [29](#)
  - LDAP [19](#), [20](#), [22](#)
  - nativa [19](#)
- dominios de seguridad de LDAP
  - configuración [25](#)
  - descripción [22](#)
- dominios de seguridad LDAP
  - eliminar [29](#)

## E

- Editar metadatos de tabla de referencia
  - privilegio [148](#)
- es
  - permisos por comando [220](#)
  - privilegios por comando [220](#)
- esquema virtual
  - permisos [202](#)
  - permisos heredados [202](#)
- etiquetas
  - privilegios para PowerCenter [166](#)

## F

- filtros
  - getUserActivityLog [120](#)
- filtros de búsqueda
  - permisos [192](#)
- flujo de trabajo
  - permisos [200](#)
  - permisos heredados [200](#)
- funciones
  - administración [180](#)
  - Administrador [181](#)
  - asignación [185](#)
  - descripción [137](#)
  - personalizadas [184](#)
  - resumen [107](#)
  - solución de problemas [187](#)
- funciones definidas por el sistema
  - Administrador [181](#)
  - asignación a usuarios y grupos [185](#)
  - descripción [180](#)
- funciones personalizadas
  - asignación a usuarios y grupos [185](#)
  - cómo editar [184](#)
  - cómo eliminar [185](#)

- funciones personalizadas (*continuado*)
  - crear [184](#)
  - descripción [180](#), [184](#)
  - Operador [252](#)
  - privilegios, cómo asignar [185](#)
  - Servicio de Metadata Manager [250](#)
  - Servicio de repositorio de PowerCenter [253](#)
  - Servicio del analista [249](#)

## G

- getUserActivityLog
  - filtros [120](#)
  - registros de actividad del usuario [120](#)
- grupo de privilegios Administración de dominios
  - descripción [140](#)
- Grupo de privilegios Administración de seguridad
  - descripción [139](#)
- Grupo de privilegios Administración en la nube
  - dominio [146](#)
- grupo de privilegios Carga
  - descripción [151](#)
- grupo de privilegios Carpetas
  - descripción [156](#)
- Grupo de privilegios Examinar
  - descripción [150](#)
- Grupo de privilegios Herramientas
  - dominio [146](#)
  - Servicio de repositorio de PowerCenter [155](#)
- grupo de privilegios Modelo
  - descripción [152](#)
- grupo de privilegios Objetos de diseño
  - descripción [158](#)
- Grupo de privilegios Objetos de tiempo de ejecución
  - descripción [162](#)
- Grupo de privilegios Objetos globales
  - descripción [166](#)
- Grupo de privilegios Orígenes y destinos
  - descripción [160](#)
- grupo de privilegios Seguridad
  - descripción [152](#)
- grupo de privilegios Supervisión
  - dominio [145](#)
- Grupo Todos
  - descripción [112](#)
- grupos
  - administración [123](#)
  - caracteres no válidos [123](#)
  - funciones, asignación [185](#)
  - grupo primario [123](#)
  - nombre válido [123](#)
  - privilegios, asignación [185](#)
  - resumen [106](#)
  - sincronización [104](#)
  - Todos predeterminado [112](#)
- grupos anidados
  - Autenticación de LDAP [28](#)
  - servicio de directorio LDAP [28](#)
- grupos de implementación
  - privilegios para PowerCenter [166](#)
- grupos de LDAP
  - administración [123](#)
  - importación [23](#)
- grupos de privilegio
  - Objetos globales [166](#)
- grupos de privilegios
  - Administración de dominios [140](#)

- grupos de privilegios (*continuado*)
  - Administración de Informatica Cloud [146](#)
  - Administración de seguridad [139](#)
  - Carga [151](#)
  - Carpetas [156](#)
  - Descripción [137](#)
  - Examinar [150](#)
  - Herramientas [146](#), [155](#)
  - Modelo [152](#)
  - Objetos de diseño [158](#)
  - Objetos en tiempo de ejecución [162](#)
  - Orígenes y destinos [160](#)
  - Seguridad [152](#)
  - Supervisión [145](#)
- grupos nativos
  - administración [123](#)
  - cómo añadir [123](#)
  - cómo eliminar [125](#)
  - edición [124](#)
  - usuarios, asignar [116](#)
- Grupos nativos
  - Movimiento a otro grupo [124](#)
- grupos primarios
  - descripción [123](#)

## H

- herramienta keytool [28](#)

## I

- IBM Tivoli Directory Server
  - Autenticación de LDAP [23](#)
- infacmd isp
  - migrateUsers [33](#)
- Informatica Administrator
  - buscar [105](#)
  - fichas, visualización [101](#)
  - Navegador [105](#)
  - Página Seguridad [105](#)
  - resumen [101](#)
- Informatica Analyst
  - administrador [113](#)
- Informatica Developer
  - administrador [113](#)
- informes de auditoría
  - descripción [210](#)
  - para grupos [215](#)
  - para usuarios [214](#), [215](#)
- inicio de sesión único
  - configuración [81](#)
  - descripción [103](#)
  - resumen [80](#)
- ipc
  - permisos por comando [220](#)
  - privilegios por comando [220](#)
- isp
  - permisos por comando [220](#)
  - privilegios por comando [220](#)

## L

- Lenguaje de marcado de aserción de seguridad (SAML)
  - compatibilidad con [80](#)

- licencias
  - permisos [193](#)

## M

- mallas
  - permisos [193](#)
- memoria del sistema
  - cómo aumentar [119](#)
- Metadata Manager
  - administrador [113](#)
- Microsoft Active Directory
  - Autenticación de LDAP [23](#)
- migrateUsers
  - archivos de migración de usuario [32](#)
  - infacmd isp [33](#)
- mrs
  - permisos por comando [232](#)
  - privilegios por comando [232](#)
- ms
  - permisos por comando [235](#)
  - privilegios por comando [235](#)

## N

- Navegador
  - Página Seguridad [105](#)
- nodos
  - permisos [193](#)
- nombre válido
  - cuenta de usuario [115](#)
  - grupos [123](#)
- Novell eDirectory
  - Autenticación de LDAP [23](#)

## O

- objetos de conexión
  - privilegios para PowerCenter [166](#)
- objetos de diseño
  - descripción [158](#)
  - privilegios [158](#)
- objetos de dominio
  - permisos [193](#)
- objetos en tiempo de ejecución
  - descripción [162](#)
  - privilegios [162](#)
- objetos globales
  - privilegios para PowerCenter [166](#)
- oie
  - permisos por comando [235](#)
  - privilegios por comando [235](#)
- OpenLDAP
  - Autenticación de LDAP [23](#)
- operación del servicio web
  - Permisos [207](#)
- Operador
  - funciones personalizadas [252](#)
- Orígenes
  - privilegios [160](#)



## P

Página Seguridad  
Informatica Administrator [105](#)  
Navegador [105](#)

perfil de sistema operativo  
administración [125](#)  
crear [129](#)  
edición [125](#)  
eliminar [132](#)  
predeterminadas [131](#)  
propiedades, servicio de integración de datos [125](#), [127](#)  
propiedades, servicio de integración de PowerCenter [125](#)

perfiles de sistema operativo  
permisos [193](#)

Perfiles de sistema operativo  
Permisos [196](#)

permiso directo  
descripción [191](#)

permiso efectivo  
descripción [191](#)

permiso heredado  
descripción [191](#)

permisos  
aplicación [200](#)  
as, comandos [217](#)  
asignación [200](#)  
carpetas [193](#)  
comandos dis [218](#)  
comandos es [220](#)  
Comandos ipc [220](#)  
comandos isp [220](#)  
comandos mrs [232](#)  
Comandos ms [235](#)  
comandos oie [235](#)  
comandos pmcmd [240](#)  
comandos pmrep [243](#)  
comandos ps [235](#)  
comandos pwx [236](#)  
comandos rms [237](#)  
comandos rtm [238](#)  
comandos sch [238](#)  
comandos sql [239](#)  
Comandos wfs [240](#)  
conexiones [198](#)  
descripción [190](#)  
directo [191](#)  
efectivo [191](#)  
esquema virtual [202](#)  
filtros de búsqueda [192](#)  
flujo de trabajo [200](#)  
heredado [191](#)  
licencias [193](#)  
mallas [193](#)  
nodos [193](#)  
objetos de dominio [193](#)  
operación del servicio web [207](#)  
perfiles de sistema operativo [193](#)  
procedimiento almacenado virtual [202](#)  
servicio de datos SQL [202](#)  
servicio web [207](#)  
servicios de aplicación [193](#)  
tabla virtual [202](#)  
tipos [191](#)  
trabajo con privilegios [190](#)

Permisos  
perfiles de sistema operativo [196](#)

permisos del dominio

directo [191](#)  
efectivo [191](#)  
heredado [191](#)

pmcmd  
permisos por comando [240](#)  
privilegios por comando [240](#)

pmrep  
permisos por comando [243](#)  
privilegios por comando [243](#)

privilegios  
administración de dominios [140](#)  
Administración de Informatica Cloud [146](#)  
administración de seguridad [139](#)  
as, comandos [217](#)  
asignación [185](#)  
carpetas [156](#)  
comandos dis [218](#)  
comandos es [220](#)  
Comandos ipc [220](#)  
comandos isp [220](#)  
comandos mrs [232](#)  
Comandos ms [235](#)  
comandos oie [235](#)  
comandos pmcmd [240](#)  
comandos pmrep [243](#)  
comandos ps [235](#)  
comandos pwx [236](#)  
comandos rms [237](#)  
comandos rtm [238](#)  
comandos sch [238](#)  
comandos sql [239](#)  
Comandos wfs [240](#)  
descripción [135](#)  
destinos [160](#)  
dominio [138](#)  
heredados [186](#)  
herramientas de dominio [146](#)  
Herramientas del servicio de repositorio de PowerCenter [155](#)  
objetos de diseño [158](#)  
objetos en tiempo de ejecución [162](#)  
objetos globales de PowerCenter [166](#)  
Orígenes [160](#)  
programas de la línea de comandos [217](#)  
Servicio de administración del contenido [148](#)  
Servicio de escucha PowerExchange [169](#)  
Servicio de integración de datos [148](#)  
Servicio de Metadata Manager [149](#)  
Servicio de programador [170](#)  
Servicio de registrador de PowerExchange [169](#)  
Servicio de repositorio de modelos [152](#)  
Servicio de repositorio de PowerCenter [154](#)  
Servicio del analista [146](#)  
solución de problemas [187](#)  
supervisión [145](#)  
trabajo con permisos [190](#)  
privilegios del servicio de Metadata Manager  
grupo de privilegios Carga [151](#)  
grupo de privilegios Modelo [152](#)  
grupo de privilegios Seguridad [152](#)  
Privilegios del servicio de Metadata Manager  
Grupo de privilegios Examinar [150](#)  
privilegios heredados  
descripción [186](#)  
procedimiento almacenado virtual  
permisos [202](#)  
permisos heredados [202](#)

programas de la línea de comandos  
privilegios [217](#)

ps  
permisos por comando [235](#)  
privilegios por comando [235](#)

powx  
permisos por comando [236](#)  
privilegios por comando [236](#)

## R

recurso de servicio web  
permisos [207](#)  
registros de actividad del usuario  
convertUserActivityLog [120](#)  
formatos de salida [120](#)  
getUserActivityLog [120](#)  
rms  
permisos por comando [237](#)  
privilegios por comando [237](#)  
rtm  
permisos por comando [238](#)  
privilegios por comando [238](#)

## S

sch  
permisos por comando [238](#)  
privilegios por comando [238](#)  
sección Buscar  
Informatica Administrator [105](#)  
seguridad  
contraseñas [115](#)  
funciones [137](#)  
permisos [109](#)  
privilegios [109](#), [135](#), [139](#)  
seguridad a nivel de columna  
restricción de columnas [205](#)  
Seguridad de PowerCenter  
administrar [105](#)  
seguridad del usuario  
descripción [102](#)  
Servicio de administración del contenido  
privilegios [148](#)  
servicio de datos SQL  
permisos [202](#)  
permisos heredados [202](#)  
tipos de permiso [203](#)  
Servicio de directorio de LDAP  
cómo conectar con [23](#)  
servicio de directorio LDAP  
grupos anidados [28](#)  
Servicio de escucha PowerExchange  
privilegios [169](#)  
Servicio de integración de datos  
autorización [104](#)  
privilegios [148](#)  
Servicio de Metadata Manager  
autorización [104](#)  
funciones personalizadas [250](#)  
privilegios [149](#)  
sincronización de usuarios [104](#)  
usuarios con privilegios [187](#)  
Servicio de programador  
privilegios [170](#)

Servicio de registrador de PowerExchange  
privilegios [169](#)  
Servicio de repositorio de modelos  
autorización [104](#)  
privilegios [152](#)  
sincronización de usuarios [104](#)  
usuarios con privilegios [187](#)  
Servicio de repositorio de PowerCenter  
autorización [104](#)  
Función de administrador [181](#)  
funciones personalizadas [253](#)  
privilegios [154](#)  
sincronización de usuarios [104](#)  
usuarios con privilegios [187](#)  
Servicio del analista  
funciones personalizadas [249](#)  
privilegios [146](#)  
servicio web  
Permisos [207](#)  
tipos de permiso [207](#)  
servicios de aplicación  
autorización [104](#)  
permisos [193](#)  
sincronización de usuarios [104](#)  
Servicios de Federación de Active Directory  
configuración para el inicio de sesión único [89](#)  
sincronización  
horas para el servicio de directorio LDAP [27](#)  
usuarios [104](#)  
Usuarios de LDAP [23](#)  
sql  
permisos por comando [239](#)  
privilegios por comando [239](#)  
suites de cifrado  
avanzadas [69](#)  
configuración [69](#)  
Java Cryptography Extension (JCE) [69](#)  
Sun Java System Directory Server  
Autenticación de LDAP [23](#)

## T

tabla virtual  
permisos [202](#)  
permisos heredados [202](#)  
Test Data Manager  
administrador [113](#)

## U

UpdateColumnOptions  
sustitución de valores de columna [205](#)  
usuarios  
administración [115](#)  
asignar a grupos [116](#)  
caracteres no válidos [115](#)  
funciones, asignación [185](#)  
gran número de [119](#)  
memoria del sistema [119](#)  
nombre válido [115](#)  
privilegios, asignación [185](#)  
resumen [107](#)  
sincronización [104](#)  
Usuarios de LDAP  
asignar a grupos [117](#)  
importación [23](#)

- usuarios LDAP
  - administración [115](#)
  - habilitar [117](#)
- usuarios nativos
  - administración [115](#)
  - asignar a grupos [116](#)
  - cómo añadir [115](#)
  - cómo editar [116](#)
  - cómo eliminar [117](#)
  - contraseñas [115](#)
  - habilitar [117](#)

## V

- variables de entorno
  - INFA\_TRUSTSTORE [60](#)
  - INFA\_TRUSTSTORE\_PASSWORD [60](#)

## W

- wfs
  - permisos por comando [240](#)
  - privilegios por comando [240](#)